informática Y DERECHO
23-26
24-25
REVISTA IBEROAMERICANA DE DERECHO INFORMÁTICO

JORNADAS

MARCO LEGAL Y DEONTOLÓGICO DE LA INFORMÁTICA

ACTAS
(VOLUMEN II)

UNED
Centro Regional de Extremadura

REVISTA IBEROAMERICANA DE DERECHO INFORMÁTICO

DIRECTOR

Valentín Carrascosa López
Director C.A. de la U.N.E.D. Mérida (ESPAÑA)
Presidente de la Federación Iberoamericana de Asociaciones de Derecho e Informática (FIADI)

SECRETARIO

Eduardo Pedro Rodríguez de Castro
Profesor-Tutor U.N.E.D Mérida (ESPAÑA). Abogado

CONSEJO ASESOR

Yarina Amoroso Fernández
Presidenta Sociedad Cubana de Derecho e Informática (CUBA)

Juan Diego Castro Fernández
Universidad Escuela Libre de Derecho (COSTA RICA)

Carlos E. Delpiazzo
Universidad Mayor de la República Oriental (URUGUAY)

Maria Fernanda Guerrero
Universidad del Rosario (COLOMBIA)

Pedro Patrón Bedoya
Universidad de Lima (PERU)

Enrique Pérez Luño
Universidad de Sevilla (ESPAÑA)

Julio Téllez Valdés
Universidad Nacional Autónoma (MEXICO)

Antonio Vittorino
Universidad de Lisboa (PORTUGAL)

informática Y DERECHO
23-26
24-25
REVISTA IBEROAMERICANA DE DERECHO INFORMÁTICO

SOBRE LA EDICIÓN DIGITAL 2012

La presente edición es el resultado de un acuerdo de colaboración entre la *Federación Iberoamericana de Asociaciones de Derecho e Informática* (FIADI) y el *Instituto Chileno de Derecho y Tecnologías* (ICDT), formalizado en octubre de 2011 en la ciudad de Buenos Aires, en que se decidió re-editar digitalmente la que es la primera publicación periódica de habla castellana en Derecho Informático: **Informática y Derecho**, **Revista Iberoamericana de Derecho Informático**, que vio la luz en el año 1992 en el Centro Regional de Extremadura de la UNED de la ciudad de Mérida (España) bajo la dirección del Prof. Dr. Valentín Carrascosa López, y que dejó de publicarse tras una década de fructífera labor.

El objetivo final de esta nueva edición digital, ahora a cargo del *Instituto Chileno de Derecho y Tecnologías*, es rescatar los trabajos, investigaciones e ideas aparecidos en las páginas de esta revista académica para su libre consulta por futuras generaciones de docentes, investigadores y estudiantes, como modo de contribuir no solo con la preservación de la cultura jurídica, sino también aportar conocimiento a la historia de las ideas y rescatar la labor de los pioneros en temas de Derecho y Tecnologías en Iberoamérica.

informática Y DERECHO
23-26
24-25
REVISTA IBEROAMERICANA DE DERECHO INFORMÁTICO

JORNADAS

MARCO LEGAL
Y DEONTOLÓGICO DE LA
INFORMÁTICA

Año 1998

UNIVERSIDAD NACIONAL
DE EDUCACIÓN A DISTANCIA
Centro Regional de Extremadura - Mérida

EDICION ORIGINAL IMPRESA

Universidad Nacional de Educación a Distancia
Centro Regional de Extremadura en Mérida
c/ Moreno de Vargas, 10
06800 MÉRIDA (BADAJOZ)
Tfno. (924) 315050/11 Fax. (924) 302556
ISBN: 84-88861-62-1

EDICIÓN DIGITAL 2012

Instituto Chileno de Derecho y Tecnologías
c/ Melchor Concha y Toro 187
7520312 Providencia,
Santiago de Chile
Web: http://www.icdt.cl

ACTAS (VOLUMEN II)

El contenido de este volúmen es continuación del Volumen I, con lo que tenemos recogido las actas de las Jornadas sobre MARCO LEGAL Y DEONTOLOGICO DE LA INFORMATICA, celebradas en Mérida (ESPAÑA), del 16 a 20 de septiembre de 1997.

El sumario de ambos volúmenes figura al comienzo del Volúmen I sin prejuicio de expresar alfabéticamente los autores al final del presente volúmen.

El Acceso Judicial a los Datos de Carácter Personal contenidos en los Ficheros Automatizados de la Administración Tributaria

LUIS GOMEZ LOECHES

Licenciado en Derecho

PREFACIO

La declaración legal del carácter reservado de toda la información personal incluida en los ficheros automatizados de la Administración Tributaria, ha provocado cierta controversia sobre si es o no obligatorio atender aquellos requerimientos de cesión de datos, procedentes de la Administración de Justicia, cuyo objeto no está exceptuado de la reserva.

Ello es debido a que la prevalencia entre dos bienes constitucionalmente protegidos, como la intimidad informática y la tutela judicial efectiva, no puede resolverse en abstracto, mediante disposiciones generales, sino caso por caso por aquellos a quienes el ordenamiento jurídico designa como sus garantes, es decir, por los Jueces y Tribunales.

INTRODUCCION

Para adecuar la normativa tributaria al resto del ordenamiento jurídico la Ley 25/1995, de 20 de julio, de modificación parcial de la Ley General Tributaria, a través de la nueva redacción dada a su artículo 113, estableció, mediante la declaración de reservado de los datos de carácter personal incluidos en los ficheros informáticos creados por la Administración Tributaria, un régimen de uso y tratamiento distinto y especial respecto del que ya dispensaba para tales datos la Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal (LORTAD).

La declaración legal del carácter reservado de estos datos impide su utilización para otros fines que no sean los que legitiman - *ex* artículo 31.1 de la Constitución - su obtención, esto es, la efectiva aplicación de los tributos o recursos cuya gestión tenga encomendada la Administración Tributaria, sin que puedan ser cedidos o comunicados a terceros, salvo que la cesión tenga por objeto atender los deberes de colaboración entre Administraciones Públicas y que taxativamente se señalan en el apartado 1 del citado artículo 113.

En un primer momento, el ámbito de colaboración con la Administración de Justicia sufrió una extrema restricción, puesto que las únicas cesiones de datos permitidas a los órganos jurisdiccionales o al Ministerio Público, eran aquellas que tuvieran por objeto la investigación o persecución de delitos públicos (artículo 113.1.a de la LGT). La citada limitación legal generó cierta controversia y discrepancia de criterios entre los operadores jurídicos implicados (cedente y cesionarios), motivando importantes pronunciamientos [1].

La situación descrita experimentó una modificación con la Ley 13/1996, de 30 de diciembre, de Medidas Fiscales, Administrativas y del Orden Social, (Ley de "acompañamiento" a la de Presupuestos Generales del Estado para 1997) cuyo artículo 47 dispone la incorporación de una nueva letra f) en el apartado 1 del artículo 113 de la LGT que permite las cesiones de datos cuyo objeto sea la

[1] Vid. El Informe del Servicio Jurídico de la Agencia Tributaria de 15 de diciembre de 1995 y la Sentencia del Tribunal de Conflictos de Jurisdicción de 25 de junio de 1996 (BOE 2-agosto-1996).

protección de los derechos o intereses de los menores e incapacitados por los órganos jurisdiccionales o por el Ministerio Fiscal.

A pesar de que este cambio pueda ser considerado plausible, por cuanto supone ensanchar el angosto cauce de información tributaria cedible a la Administración de Justicia, a nuestro juicio, el actual régimen de cesiones exceptuadas de la reserva todavía resulta insuficiente e inadecuado al ordenamiento jurídico.

Dicha falta de acomodo se fundamenta en las consideraciones que se expondrán más adelante en un intento de analizar cuestiones como las colisiones de la nueva regulación de las condiciones de licitud de las cesiones de datos respecto de los principios contenidos en la LORTAD, la legitimidad del poder judicial en la tutela de los derechos, la prevalencia entre las obligaciones del responsable del fichero de colaboración con la Administración de Justicia y de secreto profesional, o si esta cuestión ha de situarse en el plano de las relaciones individuo-Estado o se trata de un problema de cooperación entre los poderes públicos implicados [2].

I. EL ACCESO JUDICIAL A LAS INFORMACIONES RESERVADAS.

En el tema del acceso judicial a los documentos [3] reservados confluyen algunas cuestiones, íntimamente relacionadas con la protección de los datos de carácter personal, como las necesidades democráticas de control de la información y del tratamiento de estos datos por parte de los órganos jurisdiccionales para el desempeño de las funciones que legítimamente tienen atribuidas.

■[2] Vid. El epígrafe de este trabajo referido a las dudas sobre la justificación del nuevo régimen (de cesión de datos tributarios).

■[3] Se utiliza aquí el término documento con una significación tan amplia como la dada al mismo en el artículo 26 de la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal (CP/1995), que establece: " A los efectos de este Código se considera documento todo soporte que exprese o incorpore datos, hechos o narraciones con eficacia probatoria o cualquier otro tipo de relevancia jurídica.", es decir, en el sentido de soporte de información.

A) EL CARACTER RESERVADO DE LOS DATOS TRIBUTARIOS NOMINATIVOS.

Resulta evidente, en la sociedad en que vivimos, cada día más computerizada, que todos los ciudadanos se hallan expuestos a ver vulnerada su privacidad por determinados usos de la informática y la telemática, haciéndose *cada vez más* [4] extendida la injerencia del ordenador electrónico en las distintas esferas y relaciones que configuran la vida cotidiana.

De hecho, las exigencias de un progresivo intervencionismo estatal para la más o menos satisfactoria realización de las libertades públicas en un Estado social y democrático de Derecho, producen una merma paulatina de la esfera personal, poniendo en primer plano, en detrimento del derecho a la vida privada, a la legitimidad de la captación progresiva por las Administraciones Públicas de información sobre aspectos más o menos reservados de los ciudadanos, con el fin de realizar sus funciones y prestar de forma más eficaz [5] sus servicios.

Respecto de la protección de datos, es constatable, a través de su reiterada jurisprudencia, [6] que el Tribunal Constitucional defiende una concepción del

■[4] Esta nota de progresividad, característica del fenómeno informático, es destacada en el considerando (4) de la Directiva 95/46 /CE del Parlamento Europeo y del Consejo, (DOCE nº L281, de 23 de noviembre de 1995, p.31), así como por CARRASCOSA LOPEZ, Valentín, y otros en "La LORTAD: una necesidad en el panorama legislativo español", en Informática y Derecho 6-7. UNED Mérida, 1994, quien, además, adjetiva la injerencia informática, como difusa e implacable.

■[5] Una muestra reciente del constante esfuerzo por mejorar la eficacia de los servicios públicos puede encontrarse en el acuerdo del Consejo de Ministros de 4 de abril de 1997, publicado en el BOE de 14 de abril de 1997, para la progresiva implantación de un sistema intercomunicado de registros en soporte informático entre la Administración General del Estado, las Administraciones de las Comunidades Autónomas y las entidades que integran la Administración Local, como un paso más en el proyecto denominado de "ventanilla única", cuyo fundamento se encuentra en el art. 38 de la Ley 30/1992, y enmarcado en el cumplimiento del mandato de constitucional de la cooperación entre poderes públicos.

■[6] Desde bien pronto lo recordó el Tribunal Constitucional, así su STC 91/1983, de 7 de noviembre, declara en el FJ3º que: "Los derechos fundamentales reconocidos en la Constitución... no son derechos ilimitados, sino que encuentran sus límites en el derecho de los demás (art. 10

derecho a la intimidad como un derecho a ser dejado en paz, como un instrumento a través del cual oponerse a intromisiones ilegítimas, por no deseadas, en su vida privada, siempre y cuando tales intromisiones no vengan exigidas por la necesidad de defender, de salvaguardar o de asegurar un interés que se entienda preponderante.

El derecho a la intimidad reconocido en el artículo 18.4 de la Constitución no constituye una cláusula o excepción oponible por el individuo contra cualquier tipo de injerencia,[7] pero tampoco cederá frente aquellas injerencias arbitrarias, o aquellas otras de menor relevancia constitucional, pues los derechos fundamentales del ciudadano, como expresión que son del derecho general del mismo a la libertad frente al Estado, sólo pueden ser restringidos por el poder público en cuanto esto sea indispensable (principio de proporcionalidad) [8] para la salvaguarda del interés general.[9]

La anterior constatación, nos reafirma en la idea [10] de que los derechos fundamentales suponen el despliegue de los valores que el ordenamiento jurídico establece como superiores (artículo 1.1 CE), y sirven de criterios racionalizadores del poder, así como de su estructura y funcionamiento democrático pero, no por ello se debe olvidar que todos los derechos fundamentales tienen carácter relativo.[11]

CE) y, en general, en otros bienes y derechos constitucionalmente protegidos" (BJC, nº 3, p. 1331).

■7 POMED SANCHEZ, L.A. "El derecho de acceso de los ciudadanos a los archivos y registros administrativos". Instituto Nacional de Administración Pública. Madrid, 1989, destaca la cita de la STC 110/1984, de 26 de noviembre (FJ3º).

■8 En este sentido, el artículo 4 de la LORTAD, Calidad de los datos, cuando exige que los datos sean adecuados, pertinentes y no excesivos en relación con el ámbito y finalidades legítimas para las que se hayan obtenido, está introduciendo parámetros de proporcionalidad.

■9 Vid. Sentencia del Tribunal Constitucional Federal alemán de 15 de diciembre de 1983, sobre inconstitucionalidad de la Ley del censo de población.

■10 PECES BARBA MARTINEZ, Gregorio, en Prólogo a la Constitución española de 1978. Centro de Estudios ADAMS. Ediciones Valbuena, S.A. Madrid, 1990.

■11 "...este derecho fundamental "a la intimidad" no es absoluto y limita con los demás derechos y los derechos de los demás..." (SSTC 50/1995 y las citadas en su FJ 5º 15/1993 y 170/1994).

En este sentido, resulta posible afirmar - tras una puesta en relación de los preceptos constitucionales en los cuales el derecho a la intimidad opera como límite [12], no sólo frente a los derechos de los individuos, sino frente a los propios poderes públicos- que el derecho a la intimidad, ocupa una posición preferencial o privilegiada en relación con el conjunto de los derechos fundamentales,[13] lo cual viene a significar que algunos derechos fundamentales son más prevalentes que otros. [14] Por todo ello el derecho a la intimidad puede aceptarse como corolario de la dignidad de la persona, reconocida en el artículo 10.1 CE.

B) EL EJERCICIO LEGITIMO DE LA POTESTAD JURISDICCIONAL.

Se dice que la Constitución, en general, regula el uso de la fuerza del poder [15], establece quien la puede ejercer, por qué cauces, con qué fines, contra qué destinatarios, con qué limites.

El principio de seguridad jurídica, que representa una de las funciones primordiales del Derecho, por constituir un eje o punto de referencia constante alrededor del cual giran los principios constitucionales, es, en palabras del propio Tribunal Constitucional (STC 227/1988, de 28 de mayo) "suma de certeza y legalidad, jerarquía y publicidad normativa, irretroactividad de lo no favorable, interdicción de la arbitrariedad, sin perjuicio del valor que por sí mismo tiene ese

■[12] Cabe citar el mismo artículo 18.4 - límite al uso de la informática, el artículo 20.4 -límite a la libertad de expresión-, el 105, b) -límite al acceso a los archivos y registros administrativos-, o el 120.1 -límite a la publicidad de las actuaciones judiciales- .

■[13] Y este parece haber sido también el criterio de la reforma del artículo 113 de la LGT que comentamos.

■[14] Sobre el concepto gradual de la fundamentalidad o resistencia de los derechos fundamentales, PRIETO SANCHIS, Luis, en " Estudios sobre derechos fundamentales," Ed. Debate Madrid, 1990.

■[15] En términos similares se inicia la E. de M. de la Ley Orgánica, 10/1995, de 23 de noviembre, del Código Penal (...Se ha llegado a definir el ordenamiento jurídico como el conjunto de normas que regulan el uso de la fuerza...).

principio", responde a la idea de la necesidad de conocer las consecuencias jurídicas de los actos de los individuos y de los poderes públicos, guardando estrecha relación con la necesidad de interpretar todo el ordenamiento jurídico desde la Constitución. [16]

Por la función de seguridad de la Constitución sabemos a qué atenernos, tenemos certeza sobre quién es competente para mandar y por qué procedimientos y cauces puede mandar. La tranquilidad de la vida social depende, en gran parte, de conocer previamente la contestación a estos interrogantes. [17]

Partiendo de que el ejercicio de la potestad jurisdiccional corresponde en exclusiva a los Juzgados y Tribunales determinados por las leyes, según las normas de competencia y procedimiento que las mismas establezcan "en todo tipo de procesos" (artículo 117.3 CE), en principio, cabe concluir que, tan legítimas han de ser las funciones ejercidas por los integrantes del Poder Judicial en uno como en otro orden jurisdiccional.

El hecho de que el carácter reservado de la información tributaria personal resulte oponible a un órgano judicial que la recaba en el ejercicio de sus funciones en todos aquellos procesos cuyo objeto está afectado por dicha reserva, conlleva cierta dosis de inseguridad jurídica, por su falta de congruencia; es tanto como negar la efectividad de la tutela judicial (art. 24 CE) a quienes -sin ser menores ni incapacitados, ni perseguir un delito público- hayan acudido al amparo de la jurisdicción en el ejercicio de sus derechos e intereses legítimos, y su defensa haga indispensable [18] acceder a dicha información.

■[16] Vid. PEREZ LUÑO, A.E. en "La interpretación de la Constitución", en Revista de las Cortes Generales, nº 1, Madrid, 1984.

■[17] Vid. PECES BARBA MARTINEZ, Gregorio. Ob. Cit.

■[18] No necesariamente han de ser siempre menores o incapacitados, ni perseguir delitos públicos, aquellos que se vean necesitados de tutela judicial en defensa de un derecho o interés legítimo, vg., las reclamaciones de alimentos entre parientes, donde para realizar el juicio de proporcionalidad previo a fijar su cuantía es preciso acreditar ante el Juez (art. 1609 LEC) el caudal o medios del alimentante y las necesidades del alimentista (art. 146 CC), o en los casos de la fijación de los alimentos (art. 93 CC) o de la pensión compensatoria a favor del cónyuge al que la separación o divorcio produzca desequilibrio económico (art. 97.8ª CC).

No puede prevalecer una interpretación de la Constitución excluyente frente a otra integradora,[19] pues la aplicación estricta del artículo 113.1 de la LGT, en defensa del derecho a la intimidad informática de la persona concernida por los datos tributarios, antepone un formalismo rígido a toda consideración o ponderación a realizar por el Juez en el caso concreto. Dándose la posibilidad de que estas medidas supongan un sacrificio excesivo o innecesario de los derechos de los demás ciudadanos, derivado de una desproporción entre el fin perseguido y los medios empleados.

El sistema de cesiones comentado no deja de provocar cierta desazón jurídica, máxime, teniendo en cuenta que, ni en la propia Carta Magna, ni en la Ley Orgánica 1/1985, de 1 de julio, del Poder Judicial (LOPJ), se discrimina con carácter abstracto entre los ordenes jurisdiccionales, ni entre clases de procesos, y mucho menos entre unos y otros justiciables, cuando se trata de los derechos y libertades reconocidos en el Capítulo Segundo del Título I de la Constitución.

Lo cierto es que, como establece la LOPJ en su Título preliminar, los derechos y libertades fundamentales vinculan en su integridad a todos los Jueces y Tribunales y están garantizados bajo la tutela judicial efectiva de los mismos (artículo 7.1) y, en especial, los derechos enunciados en el artículo 53.2 de la Constitución -artículos 14 al 29 y 30.2- que se reconocerán, "en todo caso", de conformidad con su contenido constitucionalmente declarado, sin que las resoluciones judiciales puedan restringir, menoscabar o inaplicar dicho contenido (artículo 7.2).

Siendo la *autorización judicial*, en paridad, en ciertas ocasiones, con el *consentimiento* del titular del bien jurídico protegido y, en otras, con la *finalidad* perseguida - por ejemplo, la entrada en domicilio en caso de flagrancia de delito- (artículo 18.2 de la Constitución), una de las causas ante las cuales la protección constitucional del derecho a la intimidad cede, precisamente a guisa de garantía - por ejemplo, la inviolabilidad del secreto de las comunicaciones, salvo resolución judicial- (artículo 18.3 de la Constitución), resulta desconcertante que en esta regulación se pueda, no sólo calificar de intromisión ilegítima, sino incluso vetar una actuación judicial que pretende obtener la información personal que resulte

■[19] STC de 21 de junio de 1990, FJ 7°. También PEREZ LUÑO opina que en materia de derechos fundamentales, en caso de oscuridad, es mejor decidir a favor de la libertad.

adecuada, pertinente y no excesiva en relación con el ámbito y las finalidades legítimamente atribuidas por el ordenamiento jurídico, por ser presupuesto indispensable para la adopción de su decisión jurisdiccional.

Desde una perspectiva de la organización y funcionamiento de los poderes públicos, *prima facie*, resulta paradójico que, siendo tan decisiva función de los integrantes del Poder Judicial, únicos que disponen de la extraordinaria potestad para decidir, con independencia e imparcialidad y conforme a Derecho, sobre la libertad y el patrimonio de las personas, precisen del concurso de otras instancias públicas para contar con los instrumentos necesarios para desempeñar su cometido.

Sin embargo, desde un análisis más detenido, debe aceptarse como lógica la necesidad de concurso de terceros, ya que ésta es asumida por el sistema jurídico que diseña la Constitución, como expresión de un principio superior de solidaridad y de cooperación entre los poderes públicos (art. 118 CE) para la eficacia plena del Derecho, que se basa en el cumplimiento de la obligación constitucional de obediencia (artículo 9.1 CE).

Este concurso de personas, tanto públicas como privadas, se hace esencial en materia de información, hasta tal punto que, hoy en día, una institución carente de información es una organización débil, caduca y reñida con el progreso, pues toda decisión requiere información.[20]

C) NECESIDADES DEMOCRÁTICAS DE INFORMACIÓN.

Comúnmente, la idea de información se asocia a la de poder. El control de la información ha sido considerado, aunque desde diferentes puntos de vista, como un instrumento básico en el ejercicio de poder [21]. En este sentido, se ha

■[20] ALVAREZ CIENFUEGOS, José María, en "Sistemas informáticos para la Administración de Justicia, en el ámbito de las Comunidades Autónomas" Plan Territorial de la Rioja. C.G.P.J., 1993. En este sentido, exponiendo los problemas de acomodación de la función de los jueces al Estado constitucional de fin de siglo, y resaltando el desfase del Poder Judicial en relación al protagonismo en el proceso de construcción y desarrollo del Estado democrático contemporáneo del Parlamento y el Ejecutivo, DELGADO BARRIO, Francisco Javier, en el discurso ya citado.

■[21] TIJERAS COZAR, Ramón: Llega a afirmar en su libro "Abogados de oro. El negocio de los bufetes" Ediciones Temas de hoy. Madrid, 1997, que la clave del poder se apoya ineludiblemente en tres pilares: la política, las finanzas y los medios de información

llegado a afirmar que, hoy en día, el poder y la soberanía -no sólo política, sino cultural- de los pueblos se mide por la calidad y cantidad de su información.

No obstante, si cierto es que el conocimiento es fuente de poder, no es menos cierto que ocultar conocimientos también lo es.[22] Baste recordar, que la ocultación de conocimientos puede estar amparada en una justa causa, valga como ejemplo lo que al respecto establece la Ley de Secretos Oficiales.[23] Desde otro punto de vista, el derecho del detenido a no ser obligado a declarar (art. 17.3 CE), o el derecho de todo ciudadano a no declarar contra sí mismo, a no confesarse culpable y a la presunción de inocencia, y a no declarar sobre hechos presuntamente delictivos por razones de parentesco o de secreto profesional (art. 24.2 CE) pueden considerase como supuestos de legítimo derecho al silencio.

La necesidad de contar con el soporte sólido de una completa información en la esfera del ejercicio de la potestad jurisdiccional permite ser contemplada desde dos vertientes, una formal o instrumental y otra más sustancial.

Por un lado, desde una perspectiva instrumental, para resolver a tiempo y eficazmente las demandas sociales, los Jueces y Tribunales deben disponer, no sólo de acceso a ficheros de informática jurídica que le ofrezcan, en un momento, los repertorios de legislación y jurisprudencia y la posible doctrina científica aplicable al caso concreto,[24] sino de una respuesta eficaz y leal a sus requerimientos de colaboración, tanto en el curso del proceso como en la ejecución de los resueltos.

■[22] SAINZ MORENO, Fernando, en "Principios éticos y responsabilidad en el ejercicio de la función pública" Ciclo de conferencias sobre "La Universidad y las profesiones jurídicas: Deontología, función social y responsabilidad", Organizado por el Consejo Social de la Universidad Complutense de Madrid. Enero, 1997.

■[23] El artículo 2 de la Ley 9/1968, de 5 de abril, de Secretos Oficiales, modificada por la Ley 48/1978, de 7 de octubre, (LSO) establece que podrán ser declaradas "materias clasificadas" los asuntos, actos, documentos, informaciones, datos y objetos cuyo conocimiento por personas no autorizadas pueda dañar o poner en peligro la seguridad y defensa del Estado.

■[24] ALVAREZ CIENFUEGOS, José María, Ob. Cit., insistiendo en la necesidad de cambiar los métodos operativos de la Administración de Justicia.

Pues el deber de impartir justicia sin dilaciones indebidas no constituye una obligación de la que estén absolutamente exentos las partes procesales y los demás Poderes del Estado, sino que, antes al contrario, ha de comprometer a todos los poderes públicos y a los propios justiciables, porque también es una obligación general, la que tienen de prestar su colaboración en el curso del proceso (Artículo 118 de la CE) y porque la Justicia es un valor superior que informa a todo nuestro ordenamiento (artículo 1.1 de la CE). [25]

Por otro lado, en un sentido más sustancial, el del ejercicio de su función jurisdiccional, juzgando y haciendo ejecutar lo juzgado, más genuino de su función decisoria, los Jueces y Tribunales para resolver con cierta probabilidad de acierto [26], necesitan la previa obtención de una información precisa sobre el hecho o hechos sometidos a su enjuiciamiento, pues la jurisdicción, *-iuris dictio-*, consiste en decir el Derecho, pero el Derecho se dice respecto de un hecho. La subsunción del hecho concreto bajo el supuesto abstractamente previsto en la norma aplicable es un *prius* para el despliegue de las consecuencias jurídicas que de ella pueden derivarse.

El conocimiento de los hechos que constituyen el caso concreto se adquiere en el proceso, normalmente, a través de las informaciones vertidas por las partes, pero dado que en la mayor parte de los casos tales informaciones discrepan en el modo como ocurrieron los hechos, los mismos se convierten en controvertidos, y se hace entonces necesaria la actividad probatoria encaminada a verificar la validez de la afirmación contradicha, una labor histórico-crítica para averiguar lo que en realidad sucedió. Sólo la prueba vivifica el derecho y lo hace útil, como se desprende del aforismo *-idem est non esse aut non probari-* ("tener un derecho y no poder probarlo equivale a no tenerlo"). De poco puede servir a una persona hallarse en posesión del derecho más claro e incontrovertible si en el momento procesal oportuno no consigue, demostrando los hechos que constituyen la hipótesis legal, convencer al Juez, es como si no tuviera o hubiese

■[25] GIMENO SENDRA, Vicente, en "Constitución y proceso". Ed. Tecnos Madrid, 1988.

■[26] En este sentido se ha dicho que el progreso del Derecho consiste, precisamente, en disminuir lo más posible el margen de incertidumbre, en acercar lo probable a lo real, lo verosímil a lo verdadero (LEVY-BRUHL). La verdad material pasa a ser el resultado "deseado" pero jamás "garantizado" (WACH). Por su parte SCHMIDT opina que la verdad material es la meta tendencial, pero nunca asequible, del juicio de hecho.

tenido nunca el derecho.

D) EL PROBLEMA DE LA DISPONIBILIDAD DE LA INFORMACION.

Uno de los primeros y grandes problemas de la prueba está en tender un "puente", que desde la afirmación de hecho conduzca a la verdad objetiva, a la certeza, para, de ese modo, poder trasladar los hechos a presencia del Juez. [27]

La experiencia demuestra que, cuando una decisión afecta favorablemente a una persona, ésta manifiesta una natural predisposición a facilitar la información en la que la decisión deba fundarse (p. ej. una beca, subvención, licencia, crédito, promociones comerciales, etc.). Hay una dación "voluntaria" de información en la medida en que es condición [28] para obtener un beneficio o ventaja, y ello es debido a que la información también es una "mercancía" de valor creciente, pues se enriquece con su uso.

Sin embargo, en algunos casos, la información pertinente no se facilita voluntariamente por quien dispone de ella.

Es habitual que sean las propias partes quienes disponen de los elementos de información o probatorios necesarios. En estos casos, quien dispone de documentos idóneos a los efectos de acreditar los hechos que sirven de base a las pretensiones de la parte contraria y conducentes por tanto al derecho de su adversario, lógicamente, no estará dispuesto a exhibirlos. [29]

■[27] Probar o sucumbir, como dice MUÑOZ SABATE, Luis, en "Técnica probatoria. Estudios sobre las dificultades de la prueba en el proceso". Editorial Praxis. Barcelona 3ª edición, 1993.

■[28] OROZCO PARDO, Guillermo, dando una perspectiva socio-jurídica del tema, en "Los derechos de las personas en la LORTAD", en Informática y Derecho 6-7, UNED. Mérida, 1994.

■[29] Vid. Sobre exhibición de documentos privados en poder de tercero: ORTIZ NAVACERRADA, Santiago, en "La prueba de documentos privados en el proceso civil", en Cuadernos de Derecho Judicial XXXIV Consejo General del Poder Judicial, 1993. También MUÑOZ SABATÉ, Luis, Ob. cit.

Siendo interesante a estos efectos lo que, en la fase pre-procesal, dispone la Ley de Enjuiciamiento Civil en los artículos 497 a 502, con respecto a las denominadas Diligencias preliminares (o de preparación de juicio), en ellas se prevé que el que se proponga demandar a otro puede pedir de este que declare (confiese) acerca de algún hecho relativo a su personalidad sin cuyo conocimiento no pueda entrarse en el juicio (497.1º) o que exhiba alguna cosa mueble, títulos o documentos que tenga en su poder (497, 2.º, 3.º, 4.º) o que presente cuentas de una sociedad o comunidad (497,5º).

Sobre estas pretensiones, el Juez realizará un juicio de admisibilidad, puesto que el segundo párrafo del artículo 497 establece que accederá el Juez si estima justa la causa en que se funde, rechazándola de oficio en otro caso. Esta norma debe ponerse en conexión con el artículo 11 de la LOPJ, cuyo apartado 2, otorga al Juez o Tribunal un facultad similar, pero válida para cualquier tipo de proceso, puesto que se ubica sistemáticamente en el Título preliminar de esta Ley, y que constituye un poderoso instrumento para la aplicación del principio de tutela efectiva que consagra el artículo 24 de la Constitución.

El Derecho sanciona la falta de respeto a las reglas de la buena fe, también vigentes en sede procesal. Por ejemplo, la negativa a exhibir sin justa causa en los casos 2.º, 3.º, 4.º y 5.º, se sanciona con los daños y perjuicios que se originen al actor, el cual los podrá reclamar juntamente con la demanda principal (art. 501 I de la LEC). No obstante, el párrafo 2º del artículo 501 prevé que el requerido pueda oponerse a la exhibición, pero ésta se substanciará y decidirá por los trámites establecidos para los incidentes.

Hay también, en el segundo inciso del apartado 1 del citado artículo 11 de la LOPJ, una muy importante sanción respecto de las pruebas obtenidas, directa o indirectamente, violentando los derechos o libertades fundamentales, al establecer que éstas no surtirán efecto, es decir, que son nulas las pruebas tan ilícitamente obtenidas. [30]

■[30] A este respecto, se ha desarrollado toda una doctrina en materia penal, denominada "el fruto del árbol envenenado", en el ámbito de la obtención de pruebas, sin las debidas garantías para el ejercicio y disfrute de los derechos fundamentales, principalmente del derecho a la intimidad, con motivo de la práctica de diligencias limitativas de este derecho fundamental como entradas y/o registros domiciliarios o de papeles, intervención de las comunicaciones.

Sin embargo, otras veces, no menos frecuentes, son los terceros quienes disponiendo de la información o los soportes de la misma, se niegan a suministrarla amparándose, como en el caso que nos ocupa, en el secreto profesional.

Este problema de disponibilidad de la información está conectado con el cumplimiento efectivo de la obligación de colaboración, el cual se procura a través del establecimiento de un deber jurídico o de una obligación legalmente exigibles, [31] o mediante una resolución judicial. [32]

II. LA PROTECCION DE LA INTIMIDAD FRENTE AL TRATAMIENTO DE LOS DATOS TRIBUTARIOS DE CARACTER PERSONAL.

A) DUDAS SOBRE LA JUSTIFICACIÓN DEL NUEVO RÉGIMEN.

En primer lugar, cabe considerar que esta regulación, lejos de lograr su confesado objetivo de adecuarse al resto del ordenamiento, más que adaptar aspectos de la LORTAD, entra en colisión con dicha norma, especialmente en relación con *la licitud de las cesiones de datos entre Administraciones Públicas.*

Ciertamente, del régimen que la LORTAD establece para que las cesiones de datos personales se efectúen en condiciones de licitud, no se desprende límite alguno para ceder datos a los órganos jurisdiccionales, siempre que la cesión cumpla el requisito de finalidad, exigido en función del principio del mismo nombre, que rige en materia de protección de datos. Esto es, que la cesión sea para el cumplimiento de fines directamente relacionados con las funciones

■31 HEREDERO HIGUERAS, Miguel, en "La Ley Orgánica 5/1992, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal. Comentarios y Textos" Editorial Tecnos. Madrid, 1996, cita como ejemplos los artículos 111 y 112 de la LGT.

■32 De la que constituyen ejemplos: el artículo 18.2 y 18.3 de la Constitución y los artículos 595, 597.2, 599, 603, 605, 1455 III y 2166 de la Ley de Enjuiciamiento Civil -LEC-.

legítimas del cedente y del cesionario (artículo 11.1 LORTAD), pues en atención a la relevante posición institucional ocupada por tan singulares cesionarios, no se exige el segundo de los requisitos de toda cesión lícita, esto es, el del consentimiento previo del afectado, privilegio igualmente dispensado por el legislador orgánico al Ministerio Fiscal y al Defensor del Pueblo, también incluidos en el artículo 11. 2. d) de la LORTAD.

En este orden de consideraciones, resulta inobjetable que *la Constitución atribuye al Juez,* con carácter general (artículo 24.1), *la tutela efectiva de los derechos e intereses legítimos* y, específicamente (artículo 53.2), le encomienda la tutela de las libertades y derechos fundamentales, por lo que el reconocimiento del carácter prioritario [33] de la tutela del juez ordinario en este campo, integra el mínimo ético indispensable para la legitimidad de su poder, ejercitable por éstos en todo tipo de procesos según las normas de competencia y procedimiento establecidas en las leyes (art. 117.3 CE).

Por otro lado, la consideración de falta de acomodo al orden constitucional del nuevo régimen del artículo 113 de la LGT, se sustenta en la confusión e inseguridad jurídicas producidas en la interpretación y aplicación práctica del citado precepto legal. Sin ser el artículo 113 de la LGT una norma de derecho procesal, niega la legitimidad a los titulares de la potestad jurisdiccional para acceder a los datos tributarios fuera de los supuestos en él expresamente indicados.

Así, desde la vigencia de este estricto sistema de cesiones, la Administración Tributaria, en el cumplimiento del correlativo deber de sigilo que exige la reserva (artículo 113.2 de la LGT), se ve obligada, en principio, a rechazar toda petición de cesión no expresamente permitida, puesto que si la atiende sería considerada una injerencia ilegítima en la esfera íntima del contribuyente concernido por tales datos, aunque, y aquí está el *quid* de la cuestión o la aporía, quien pretenda su conocimiento sea un órgano jurisdiccional en el ejercicio

■[33] Pues el recurso de amparo ante el Tribunal Constitucional opera con carácter subsidiario (arts. 43.2 y 441.1.a LOTC), según recordó el Excmo. Sr. Presidente del Tribunal Supremo y Presidente del Consejo General del Poder Judicial D. Francisco Javier DEGADO BARRIO en "La transparencia de la Justicia", discurso pronunciado en el Acto inaugural del Año Judicial, celebrado el 23 de septiembre de 1996. Imprenta Nacional del B.O.E., 1996.

legítimo de la funciones que tiene atribuidas.

Atendidas las anteriores consideraciones sobre la legitimidad reconocida al cesionario tanto por la Constitución como por la LORTAD, *se cuestiona si está obligado el responsable del fichero de datos fiscales a facilitar dicha información a los Jueces y Tribunales* que la requieran, en cumplimiento de la obligación constitucional de prestar la colaboración requerida por éstos (artículo 118 CE), *o si*, por el contrario, y en cumplimiento de la obligación de secreto profesional, *no está obligado a ello,* planteándose el debate sobre la prevalencia entre ambas obligaciones.

Cabe preguntarse, en último lugar, y desde una perspectiva diferente, si la cuestión se sitúa sólo en el plano de las relaciones individuo-Estado, tradicional en materia de derechos fundamentales, o si se trata de un problema mixto de organización y funcionamiento de los poderes públicos (cooperación) que, en definitiva, afecta a la eficacia y resistencia entre los dos derechos fundamentales enfrentados, el derecho a la intimidad informática y el derecho a la tutela judicial efectiva, reconocidos en la Constitución en los artículos 18.4 y 24, respectivamente, cuyo pleno ejercicio pretenden sus respectivos titulares.

Las anteriores consideraciones no empecen para apreciar la loable finalidad de la regulación comentada, materializada en el intento por parte del Estado de cumplir una obligación positiva, de promoción y remoción, en cuanto que tiende a limitar el poder respecto del derecho fundamental a la intimidad del artículo 18.4 CE y, si se quiere, de una obligación negativa, o de no interferencia, aún cuando no exista una pretensión subjetiva por parte del ciudadano.[34]

Las citadas obligaciones entrarían en colisión con la de respeto al ejercicio y disfrute de otros derechos también reconocidos como fundamentales en la

■[34] La STC 53/1985, de 11 de abril (BJC nº 49) declara que: "... los derechos fundamentales son los componentes estructurales básicos, tanto del conjunto del ordenamiento jurídico objetivo como de cada una de las ramas que lo integran, en razón a que son la expresión jurídica de un sistema de valores que, por decisión del constituyente, ha de informar el conjunto de la organización jurídica y política; son, en fin, como dice el artículo 10 de la Constitución, el "fundamento del orden jurídico y de la paz social". De la significación y finalidades de estos derechos dentro del orden constitucional, se desprende que la garantía de su vigencia no puede limitarse a la posibilidad del ejercicio de pretensiones por parte de los individuos, sino que ha de ser asumida también por el Estado..."

Constitución que, podrían estar siendo desconocidos o insuficientemente tutelados, en cuanto que la regulación comentada [35] debilita las facultades de actuación de sus principales garantes.

Esta obligación de respetar los derechos fundamentales puede entenderse como obligación superior, en conexión con los artículos 1.1, 9.1 y 9.2 de la Constitución, afectando en los dos primeros casos a los ciudadanos y a los poderes públicos, y en el último sólo a los poderes públicos y se convierte en derivación de la obligación jurídica de obediencia del artículo 9.1, de la obligación promocional del artículo 9.2 y de la configuración de España expresada en el artículo 1.1.[36]

Con la afirmación de un derecho de la era informática, el derecho a la protección de datos personales, [37] lo que los individuos afirman [38] es una parcela de su privacidad [39], una parcela del amplio y fundamental derecho a la intimidad individual, [40] que es donde aquel derecho encuentra su base jurídica.

■[35] A este respecto cabe citar la STC 129/1989, de 17 de julio (BJC nº 100/101) cuyo FJ.3º declara en relación con la significación de los derechos fundamentales que: "... especialmente obliga al legislador a proteger los valores positivados y formalizados en el ordenamiento a través de los derechos fundamentales, reconociendo, en su caso, las titularidades y obligaciones subjetivas que resulten a tal fin necesarias.

■[36] DE ASIS ROIG, Rafael, en "Deberes y Obligaciones en la Constitución". Centro de Estudios Constitucionales. Madrid, 1991.

■[37] Vid. ESTADELLA YUSTE, Olga, en "La protección de la intimidad frente a la transmisión internacional de datos personales". Editorial Tecnos, 1995, donde realiza algunas precisiones terminológicas respecto de la expresión derecho informático o derecho de protección de datos.

■[38] La garantía de la intimidad para la jurisprudencia constitucional "... adopta hoy un contenido positivo en forma de derecho de control sobre los datos relativos a la propia persona, este "derecho activo de control" ..." (STC 245/1993, de 20 de julio).

■[39] WESTIN, Alan F. en "Privacy and Freedom", Atheneum, Nueva York, 1970 (6ª reimpresión de la edición de 1967) definió el derecho a la privacidad como el derecho del individuo a determinar qué información acerca de sí mismo estaba dispuesto a compartir y con quién. Sobre diferencias conceptuales entre "intimidad" y "privacidad" vid. la propia Exposición de Motivos de la LORTAD, apartado 1.

■[40] POMED SANCHEZ, L.A. en "El derecho de acceso de los ciudadanos a los archivos y registros administrativos" Instituto Nacional de Administración Pública. Madrid, 1989, p. 256,

La protección del derecho a la intimidad respecto de los usos de la informática, reconocido en el artículo 18.4 de la Constitución y desarrollado por la Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal (LORTAD), encuentra a través de esta regulación un marco jurídico que, en principio, ofrece un nivel de protección que ha de entenderse suficiente, para que el tratamiento automatizado o no (artículo 2.1) de informaciones de carácter personal, *cuando resulte necesario*, [41] no menoscabe aquel derecho, ni el libre y pleno ejercicio de otros derechos civiles o políticos de las personas reconocidos por la Constitución Española.

Es obvio que el ordenamiento jurídico no ha previsto para los datos tributarios una especial protección, por no constituir la información patrimonial o económica personal con trascendencia tributaria, un aspecto de la esfera íntima de las personas especialmente sensible, a diferencia de aquellos otros datos que, por referirse a aspectos mucho más íntimos, han sido incluidos en el artículo 7 de la LORTAD.[42]

Estos datos al concernir a personas físicas identificadas o identificables, son de carácter personal (artículo 3 de la LORTAD). Además están contenidos en ficheros automatizados, con independencia de que el tratamiento ulterior que reciban sea o no automatizado (artículo 2.1 LORTAD) y, por último, dichos ficheros automatizados son de titularidad pública, por lo que les son aplicables las disposiciones sectoriales de los artículos 18 a 22 de la LORTAD.

La información que incluyen los ficheros creados por las Administraciones

muestra sus dudas sobre si el artículo 18.1 CE donde se recogen el derecho a la intimidad, personal y familiar, y los derechos al honor y a la propia imagen, significa que se trata de tres derechos ontológicamente distintos, o se trata de diversas manifestaciones de un genérico derecho a la vida privada.

■41 Así se expresa ROMEO CASABONA, C.M. en "Infracciones administrativas y penales en relación con la protección de datos" en "Informática y Derecho 6-7" UNED. Mérida, 1994.

■42 Como los relativos a la ideología, religión, creencias, origen racial, a la salud, vida sexual o infracciones penales o administrativas, que reciben un protección reforzada, aunque con diferentes intensidades, según su índole.

Tributarias carece de otras características que justifiquen, por sí mismas, la existencia de un régimen jurídico, como el establecido en la LGT, específico y diferente del régimen jurídico general que ya se brinda [43] en materia de protección de datos a dicha información, como se desprende de los artículos 1, 2.1, 2.2, y 2.3 y la Disposición Adicional 1ª de la Ley Orgánica 5/1992. Tampoco figuran incluidas las informaciones tributarias entre aquellas materias que hayan de regirse por sus disposiciones específicas y a las que se remite el artículo 2.3 de la LORTAD [44].

Por todo lo dicho, hay que concluir que la LORTAD es de perfecta aplicación a los datos de carácter personal incluidos en los ficheros fiscales, que ya contenía previsiones específicas en materia de cesiones de datos en los artículos 6, 11 y 19.

B) LA TECNICA DEL SECRETO.

La protección de la intimidad de los datos personales se sustenta en una técnica de uso frecuente, de la que el secreto y la reserva son dos rangos o categorías que suponen dos niveles diferentes de intensidad o grados de protección. [45]

Dicha técnica básicamente consiste en sustraer del conocimiento de personas ajenas o no autorizadas determinadas informaciones, que de no mantenerse circunscritas a determinado ámbito de confidencialidad, sea personal,

■ [43] Según asegura LUCAS MURILLO DE LA CUEVA, Pablo, en " Informática y protección de datos personales. Estudio sobre la LORTAD." Cuadernos y Debates. Centro de Estudios Constitucionales. Madrid,1993.

■ [44] Así lo entiende también el ejecutivo, a tenor de lo dispuesto en la Disposición Adicional 3ª del Real Decreto 1332/1994, de 20 de junio, por el que se desarrollan determinados aspectos de la LORTAD, cuando establece que: "Los ficheros creados por las Administraciones Tributarias para la gestión de los tributos que se les encomienden, se regirán por las disposiciones del presente Real Decreto y por las demás disposiciones reglamentarias que, en desarrollo y con sujeción a lo dispuesto en la Ley Orgánica 5/1992, específicamente se aprueben para los mismos."

■ [45] En la legislación sobre Secretos Oficiales, por ejemplo, el secreto y la reserva son dos categorías, de una misma técnica, la técnica de calificación de materias clasificadas (artículo 3 LSO), si bien el bien jurídico protegido es diferente al del caso que nos ocupa.

o compartida [46], se pondría en riesgo la integridad de determinados bienes sensibles (en nuestro caso, la intimidad, el honor o la imagen) y que se apoya para su efectividad en el correlativo deber de secreto de aquellas personas, funcionarios o autoridades que por razón de su profesión, cargo u oficio han tenido conocimiento de las mismas.

El reformado artículo 113 en su apartado 1 establece el *carácter reservado* de toda la información relativa a los contribuyentes obtenida por la Administración Tributaria en el desempeño de sus funciones, tal declaración sirve como un instrumento de garantía de la otra cara del derecho, el derecho al silencio del afectado respecto de aquellos datos que conciernen a su propia persona, frente a los potenciales riesgos que pueden derivarse del conocimiento de los mismos por personas ajenas, o no aut rizadas. o

Los efectos que esta declaración conlleva, como ya hemos señalado, son su *utilización exclusiva* dentro del ámbito de confidencialidad que comparte la persona concernida con la Administración Tributaria que los custodia, y para la específica finalidad que autorizó su lícita obtención, es decir, la efectiva aplicación de los tributos y de los recursos cuya gestión le encomienda el ordenamiento jurídico y la *prohibición de su cesión o comunicación a terceros*, salvo lo atinente a la represión de los delitos públicos y a los deberes de colaboración entre Administraciones Públicas.

Efectivamente, el órgano jurisdiccional que pretenda conocer dichos datos personales es un tercero [47] y su toma de conocimiento tiene una finalidad distinta de aquella que justificó la recogida de los datos económicos de carácter personal con trascendencia tributaria, por lo que constituye una injerencia en un ámbito

■[46] En este sentido, ROMEO CASABONA, C.M., en " Infracciones administrativas y penales en relación con la protección de datos" en Informática y Derecho 6-7, UNED. Mérida, 1994., quien entiende confidencialidad compartida, como aquel ámbito que comprende aquellos aspectos de la intimidad que por prescripción de la Ley o por la propia naturaleza de las relaciones interindividuales o sociales, facultan el acceso a terceros, pero que por su deber de secreto profesional están obligados a mantener su confidencialidad.

■[47] El artículo 2, f) de la Directiva 95/46/CE define "tercero" como persona distinta del interesado, del responsable del tratamiento y de las personas autorizadas para tratar los datos bajo la autoridad directa del responsable del tratamiento o del encargado del tratamiento.

que el ordenamiento quiere mantener reservado de la persona concernida para así garantizar su derecho a la autodeterminación informática.

Sin embargo, no se debe olvidar que es un tercero, muy singular, es un tercero imparcial, con un desinterés objetivo y que actúa para tutelar otros derechos o intereses también legítimos, y si accede a una pretensión que implique aquella injerencia, para que ésta no sea ilegítima deberá fundarse en una justa causa, pues como exige el artículo 11.2 de la LOPJ, los Juzgados y Tribunales (de oficio) rechazarán fundadamente (previa ponderación y juicio de proporcionalidad entre los valores en conflicto) las peticiones, incidentes y excepciones que se formulen con manifiesto abuso de derecho o entrañen fraude de ley o procesal (en el ámbito procesal civil, art. 497 II de la LEC).

Los eventuales riesgos que puedan menoscabar la privacidad del afectado, realmente, no se teme que procedan del propio órgano jurisdiccional, ni siquiera de su entorno inmediato, esto es, del personal a su servicio y colaboradores, a los que debe alcanzar el desinterés objetivo de aquél y, en todo caso, sujetos por la obligación de guardar sigilo de todo aquello que conozcan en el desempeño de sus cargos o funciones, como todos los profesionales que intervienen en el proceso. Obligación cuya vulneración puede conllevar responsabilidades civiles, penales y disciplinarias graves o muy graves para el culpable.

Los citados peligros proceden, más bien, de las otras personas implicadas en el mismo proceso, normalmente con intereses subjetivos contrapuestos a los del afectado y que por su condición de interesados y titulares de un interés legítimo y directo, bien directamente o bien a través de los profesionales que les asisten, tienen acceso, en virtud del principio de publicidad de las actuaciones y de defensa, a informaciones ajenas.

Una vez conocidas éstas, el afectado se vuelve más vulnerable y el adversario refuerza su posición, pues apenas hay posibilidad de impedir que tales datos una vez conocidos sean aprovechados y utilizados, en el mejor de los casos, de modo contrario o perjucial para los intereses del afectado.

C) LA INTIMIDAD DE LAS PERSONAS COMO LÍMITE AL DERECHO DE ACCESO A LOS DOCUMENTOS Y ARCHIVOS ADMINISTRATIVOS.

Los límites del acceso por parte de los ciudadanos a los registros y a los documentos que, formando parte de un expediente, obren en los archivos administrativos suelen estar en la intimidad del afectado. Los ficheros automatizados creados por la Administración Tributaria son archivos administrativos, al igual que, salvando las distancias, las actuaciones judiciales, pues también participan de tal carácter, aunque sin perder su naturaleza jurisdiccional.

Así, en el orden administrativo, dicha limitación viene establecida en el artículo 105 b) de la CE y en el artículo 37.2 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común (LRJPAC).

Pese a ello, en el artículo 37.3 de la LRJPAC cabe apreciar un interesante matiz referido al alcance del acceso a los documentos de carácter *nominativo* [48] que, sin incluir otros datos pertinentes a la intimidad de las personas figuren en los procedimiento de aplicación del derecho (*sic*), salvo los de carácter sancionador o disciplinario, y que en atención a su contenido puedan (legítimamente) hacerse valer para el ejercicio de los derechos de los ciudadanos, podrá ser ejercido, además de por sus titulares - lo que es obvio-[49] , por terceros

■[48] Esta expresión es utilizada en el sentido de personal por la Ley francesa 78-17, del 16 de enero de 1978, de informática, ficheros y libertades, cuyo artículo 4 establece: "se entienden como nominativas, en el sentido de la presente ley, las informaciones que permitan bajo cualquier forma, directa o indirectamente, la identificación de personas físicas." con el mismo significado que se utiliza en el artículo 3.a) de nuestra LORTAD, que en realidad traspone el artículo 2.a) del Convenio 108 del Consejo de Europa, la expresión datos DE CARACTER PERSONAL, puesto que con ella se define cualquier información concerniente a personas físicas identificadas o identificables.

■[49] No lo entendió así la STSJ, Sala C-A de Madrid, de 13 de noviembre de 1991, de cuya argumentación discrepa certeramente ALVAREZ CIENFUEGOS, José María, en "La confidencialidad de los datos tributarios y el derecho de acceso de los contribuyentes", en Actualidad Jurídica Aranzadi. nº 226 Diciembre de 1995, pues según el Tribunal no puede confundirse el derecho de acceso con el derecho del artículo 18.4 CE, negando así relevancia

que acrediten un interés legítimo y directo.

El ejercicio de los derechos de acceso referidos en los tres primeros apartados del artículo 37 de la LRJPAC, según el apartado 4 del mismo precepto, pueden ser denegados cuando prevalezcan razones de interés público, por intereses de terceros más dignos de protección o cuando así lo disponga una Ley, debiendo en estos casos, el órgano competente dictar resolución motivada. Entre esta dispo ición y las contenidas en slos artículos 21 y 22 de la LORTAD, promulgada apenas un mes antes que la Ley 30/1992, respecto de las excepciones a los derechos del afectado, existe cierta similitud de espíritu.

Merece ser subrayado el medio específico de reacción otorgado al afectado, por el apartado 3 del artículo 21 LORTAD, ante la Agencia de Protección de Datos o el Organismo competente de cada Comunidad Autónoma, en el caso de los ficheros automatizados mantenidos por las Administraciones Tributarias Autonómicas, quien deberá asegurarse de la procedencia o improcedencia de la denegación.

Por su parte, en el orden procesal, el artículo 232.1 de la LOPJ, en relación con el Artículo 120 de la CE, atribuye al Juez o Tribunal la facultad de limitar el ámbito de la publicidad y acordar, mediante resolución motivada, el secreto (incluso para las propias partes) de todas o parte de las actuaciones, y entonces sólo podrán los interesados obtener las informaciones no declaradas secretas (arts. 234 y 235 LOPJ).

III. LA OBLIGACION DE COLABORACION CON LA JUSTICIA.

A) EL CONTENIDO DE LA OBLIGACION. EXCEPCIONES.

Entre las obligaciones derivadas de la obligación constitucional de organización del poder y de defensa de las libertades, que afectan tanto a los poderes públicos como a los ciudadanos, se sitúa la obligación constitucional de cooperación. [50]

constitucional al primero de ellos.

■[50] A nivel legal y, dentro del ámbito de aplicación (art. 2) de la Ley 30/1992, de 26 de noviembre,

De la obligación jurídica superior de solidaridad [51] surge la obligación de colaboración entre las Administraciones Públicas, que se desenvuelve a través de tres mecanismos: a) Auxilio u obligación de colaborar en sentido estricto. b) Coordinación y c) Cooperación.

El primero de estos mecanismos se concreta en la obligación de comunicación entre las diversas instancias, con diverso alcance, puede ser: una obligación recíproca de intercambio de información, en la cual los efectos son bilaterales o multilaterales, de simple traslado de información, cuando sólo produce efectos unilaterales y una mera comunicación registral.[52]

El Poder Judicial, para la perfecta realización de esta obligación, va a necesitar, en ocasiones, de la ayuda o colaboración en sentido amplio, no sólo de otras instancias públicas, sino también de los particulares. En este sentido, el artículo 118 de la Constitución establece: "*Es obligado cumplir las sentencias y demás resoluciones firmes de los Jueces y Tribunales, así como prestar la colaboración requerida por éstos* en el curso del proceso y en la ejecución de lo resuelto."

Este precepto plantea la existencia de obligaciones susceptibles de ser contempladas separadamente. [53] Por un lado, la *obligación de cumplir las sentencias y demás resoluciones judiciales*, que se sitúa dentro del significado mismo de la función judicial, subrayando la necesidad de eficacia y seguridad y el valor de la división de poderes, y como una manifestación clara de la obligación constitucional de obediencia de todos, justiciables y poderes públicos. Y por otro, *la obligación de*

de Régimen Jurídico de las Administración Públicas y del Procedimiento Administrativo Común (LRJPAC), donde no se incluye, por cierto, a la Administración de Justicia, se recepciona este principio general por el que se rigen sus relaciones (art. 3 y todo el Título I - arts. 4 a 10-).

■[51] La solidaridad, primero de los valores tratados por VILLAPALOS, Gustavo y LOPEZ QUINTAS, Alfonso, en su obra "El libro de los valores", Planeta, 1997 (3ª edición), implica un espíritu de cooperación y participación, compromete más que la mera ayuda, tiene carácter creativo.

■[52] Vid. DE ASIS ROIG, Rafael, en "Deberes y obligaciones en la Constitución". Centro de Estudios Constitucionales. Madrid, 1991.

■[53] Apunta DE ASIS ROIG, Rafael, Op. Cit. p. 439.

prestar la colaboración requerida por Jueces y Tribunales, de carácter instrumental y para posibilitar la eficacia del Derecho judicial.

Ambas obligaciones han sido recalcadas en numerosas [54] Sentencias del Tribunal Constitucional. Destacamos aquí, -in extenso- por su interés, una cita de la STC 67/1984, en cuyo FJ 2º se declara que:

"la ejecución de las Sentencias ... es una cuestión de capital importancia para la efectividad del Estado social y democrático de Derecho que proclama la Constitución ..., que se refleja ... en la sujeción de los ciudadanos y los poderes públicos a la Constitución y al resto del Ordenamiento jurídico, cuya efectividad ... se produce normalmente por medio de la actuación del Poder Judicial ... que finaliza con la ejecución de sus sentencias y resoluciones firmes. Por ello, difícilmente puede hablarse de la existencia de un Estado de Derecho cuando no se cumplen las Sentencias y resoluciones firmes. .. "

Y además, cuando los obligados son personas públicas, precisa al respecto que:

"Cuando este deber de cumplimiento y colaboración ... se incumple por los poderes públicos, ello constituye un grave atentado al Estado de Derecho ..."

Puntualizando, más adelante, cuál ha de ser la actitud del órgano judicial a fin de obtener el cumplimiento efectivo de sus propias resoluciones:

" ... la ejecución de las Sentencias y resoluciones firmes corresponde a los titulares de la potestad jurisdiccional ..., lo que les impone el deber de adoptar las medidas oportunas para llevar a cabo esa ejecución ... Cuando para ejecutar lo juzgado el órgano judicial adopta una resolución que ha de ser cumplida por un ente público, ésta ha de llevarla a cabo con la necesaria diligencia, sin obstaculizar el cumplimiento de lo acordado, por imponerlo así el artículo 118 de la Constitución; y cuando tal obstaculización se produzca, el Juez ha de adoptar las medidas necesarias para la ejecución, de acuerdo con las Leyes ... Si tales medidas no se adoptan con la intensidad necesaria -y legalmente posible- para remover la obstaculización producida, el órgano judicial vulnera el derecho fundamental a la

■[54] Vid. SSTC 54/1983, 62/1984, 15/1986, 4/1988, 149/1989 y 298/1994.

ejecución de las Sentencias "como parte integrante del derecho a la tutela judicial efectiva (art. 24.1 CE), que le impone el deber de adoptar las medidas oportunas para llevarlas a cabo..."

En orden a *las excepciones*, el propio texto constitucional establece algunas excepciones a la colaboración, como las contenidas en el artículo 24.2 (por razón de parentesco o de secreto profesional), aunque puede entenderse que dichas excepciones sólo se refieren al proceso penal, opinión que no es pacífica, y que la propia Constitución remite a la regulación legal de los casos en que pueden oponerse.

Es a nivel legal (art. 17.1 de la LOPJ), donde la obligación constitucional de colaborar con la Justicia se configura y modula, por un lado, el aspecto modal de la prestación, que se acomodará a "la forma que la ley establezca" y por otro, "con las excepciones que establezcan la Constitución y las leyes", no pudiendo ser obstáculo el que su cumplimiento conlleve determinados trastornos o molestias, pues el mismo artículo 17.1 de la LOPJ, establece que se prestará la colaboración "sin perjuicio del resarcimiento de los gastos y del abono de las remuneraciones debidas que procedan conforme a la ley."

Respecto de la obligación de cumplir las resoluciones judiciales, el artículo 18.1 de la LOPJ establece que sólo podrán dejarse sin efecto en virtud de los recursos previstos en las leyes, de donde puede inferirse que para los terceros son siempre obligatorias, pues carecen de legitimación para impugnarlas, siendo obligatorio su cumplimiento para las partes cuando las consientan o sean desestimados los recursos que, con efecto suspensivo, se interpongan contra ellas.

Por su parte, el artículo 17.2 LOPJ establece la obligación de todos de respetar y cumplir las resoluciones judiciales que hayan ganado firmeza o sean ejecutables de acuerdo con las leyes.

B) EL AMBITO SUBJETIVO DE LA OBLIGACION.

El ámbito subjetivo de la obligación del artículo 118 CE se establece utilizando La expresión *-es obligado-* logrando así incluir, como sujetos pasivos de esta obligación, a toda clase de personas, privadas o públicas, estén o no investidas de autoridad, que vendrán obligados a prestarla cuando sean requeridos para ello en virtud de disposiciones que establezcan deberes u obligaciones

concretas.

Sin perjuicio de la genérica referencia contenida en el artículo 118 por la que se designa a quienes incumbe la obligación de *colaborar*, la Constitución, dentro del propio Título VI, Del poder judicial, designa en distintos preceptos los sujetos concretamente obligados a *cooperar* y *auxiliar* a la Administración de Justicia, como el Ministerio Fiscal en el artículo 124, la policía judicial en el 126, y el personal al servicio de la Administración de Justicia en el 122.1.

No obstante, todas estas previsiones constitucionales aparecen moduladas a nivel legal, principalmente, en el marco de la Ley Orgánica 1/1985 del Poder Judicial.

Pese a ser perfectamente aplicable a la Administración Tributaria la regulación legal de la obligación genérica de colaboración contenida en Título Preliminar de la LOPJ, esencialmente, en los artículos 17 y 18, los servicios jurídicos de la Agencia Tributaria consideran que la excepción a aquel deber que el artículo 113.1 de la LGT implica, no es más que una posibilidad expresamente contemplada y admitida por el propio artículo 17.1 de la LOPJ. [55]

Sin embargo, el artículo 469.1 resulta de directa aplicación [56] a la Administración Tributaria, ya que dicho precepto dispone:

"Sin perjuicio de lo demás dispuesto en el presente Título, los Jueces y Tribunales podrá recabar el auxilio, colaboración o asesoramiento de *cualesquiera funcionarios u órganos técnicos de la Administración Pública*, que vendrán *obligados* a prestárselos."

A diferencia de lo establecido en el artículo 17.1 de la misma LOPJ, el artículo 469.1 no contempla ningún supuesto de excepción. La expresión de su

■[55] En este sentido se pronuncia el Informe del Servicio Jurídico de la Agencia Tributaria de 15 de diciembre de 1995.

■[56] A pesar de no ser, en general, aplicables a la Administración Pública, las normas contenidas en el primero de los Títulos del Libro VI (arts. 454 a 508) dedicado a regular el estatuto jurídico del personal auxiliar y colaborador, denominado personal al servicio de la Administración de Justicia, este precepto se refiere expresamente a ella.

inciso final "*que vendrán obligados a prestárselos.*" es categórica. Por ello, resulta sorprendente que dicho precepto no ha sido invocado ni en el citado informe de 15 de diciembre de 1995, ni tampoco en la Sentencia del Tribunal de Conflictos de Jurisdicción de 25 de junio de 1996. [57]

En dicho conflicto se cuestionaba si la Administración estaba o no obligada a expedir y remitir al Juzgado copia certificada de las declaraciones del IRPF presentadas en varios ejercicios por una de las partes, requeridas en virtud de oficio, acordado librar en un proceso civil de menor cuantía, para la práctica de una prueba documental pública previamente propuesta por una de las partes litigantes y admitida por el órgano judicial, por tratarse de datos declarados reservados por el artículo 113.1 de la LGT.

Lo dispuesto por el artículo 113.1 de la LGT, en la redacción dada al mismo por la Ley 25/1995, colisiona, a juicio del Tribunal de Conflictos Jurisdiccionales, con lo dispuesto en el artículo 17.1 LOPJ.

Si bien este último precepto no encuentra excepción a nivel legal hasta la promulgación de la citada Ley 25/1995. Unicamente, a nivel reglamentario, la Orden Ministerial de 30 de julio de 1982, sobre limitación de acceso a la información contenida en las bases de datos fiscales,[58] podía ser invocada caso de estimarse no atendible un requerimiento judicial que, en el ejercicio de sus funciones, pretendiera acceder o tener conocimiento de dichos datos.

Pero esta eventual justificación carecería de virtualidad suficiente porque,

■[57] Dictada en el Conflicto 5/96-T, planteado -a juicio del Tribunal, sólo formalmente, motivo por el cual fue declarado como conflicto improcedente- entre el Juzgado de Primera Instancia número 15 de los de Madrid y la Delegación Especial de la Agencia Estatal de la Administración Tributaria de Madrid, ejemplo de paradigmático de la polémica producida, a raíz de la promulgación de la Ley 25/1995, entre la Administración Tributaria y la Jurisdicción, por la negativa a ceder datos tributarios para un fin no exceptuado de la reserva.

■[58] Esta orden ya disponía el uso de la información contenida en la bases de datos fiscales exclusivamente reservado al cumplimiento de los fines que el ordenamiento jurídico encomienda al Ministerio de Hacienda, considerando como violación del secreto profesional, y en consecuencia, como falta disciplinaria muy grave, todo acceso no autorizado a los mismos, o su utilización o difusión fuera del estricto ámbito exigido por la función y puesto de trabajo desempeñado por el funcionario.

por un lado, los titulares de la potestad jurisdiccional, sometidos únicamente al imperio de la Ley, se hallan facultados para inaplicar los reglamentos o cualquier otra disposición (que estimen) contraria a la Constitución, a la ley o al principio de jerarquía normativa (arts. 117.1 CE y 6 de la LOPJ) y, por otro, porque expresamente la propia LOPJ (art. 17.1) prevé para las excepciones al comentado deber de auxilio judicial un rango normativo de ley, según se desprende de la dicción: "las excepciones que establezcan la Constitución y las leyes" .

IV. EL DILEMA DEL RESPONSABLE DEL FICHERO ANTE LAS PETICIONES DE CESIÓN DE DATOS RESERVADOS.

Las autoridades y funcionarios de la Administración Tributaria, depositaria y responsable [59] de la custodia de los datos obtenidos para la consecución de fines concretos y específicos, ante el carácter taxativo de las indicadas excepciones al principio de reserva, precisamente reconocidas en favor de los órganos jurisdiccionales y del Ministerio Público, cada vez que reciben de éstos una solicitud de cesión de datos afectados por la reserva, se encuentran ante el dilema de acceder o no a dichas peticiones.

Por un lado, atender la petición supone violar el deber de sigilo respecto de dichos datos, cuya infracción será, con independencia de las responsabilidades penales o civiles que pudieran corresponder, considerada siempre falta disciplinaria muy grave, es decir, de las castigadas hasta con separación del servicio (artículo 113.2 LGT). Y por otro, si no atienden dicha petición se enfrentan a la eventual exigencia de responsabilidad penal por delito de desobediencia y denegación de auxilio a la autoridad judicial.

A) LA ECLECTICA POSTURA DE LA ADMINISTRACIÓN.

En esta difícil tesitura la Administración Tributaria adoptó una postura

■[59] Este deber de sigilo para los guardianes de la información, es el derecho al silencio (fácilmente comprendible en expedientes sancionadores, por ejemplo) de la persona concernida, observa OROZCO PARDO, Guillermo, en "Los derechos de las personas en la LORTAD" en Informática y Derecho 6-7, UNED Mérida,1994.

ecléctica, pues adecuó su conducta a la recomendación del informe que su servicio jurídico emitió el 15 de diciembre de 1995 con el objeto de determinar qué peticiones de cesión de información han de ser atendidas y cuáles no, y así establecer criterios uniformes de actuación por todos los órganos de la Agencia Tributaria frente a las numerosísimas peticiones procedentes de los órganos jurisdiccionales que solicitan información obtenida por la Administración Tributaria en el ejercicio de sus funciones.

El citado informe, reconoce (apartado VII) que es indudable que la Agencia Estatal de Administración Tributaria (AEAT) no puede convertirse [60], en un órgano de control de las resoluciones dictadas por los órganos jurisdiccionales, pues es el Poder Judicial al que corresponde el control de la actuación administrativa (artículo 106.1 CE) y no al contrario.

También reconoce que el hecho de que la cesión de información tributaria en los casos no autorizados pueda afectar al honor y a la intimidad de las personas afectadas no desvirtúa la anterior afirmación, pues son en principio (sic) los Tribunales de Justicia los garantes de los derechos fundamentales de las personas y no la Administración Pública.

Termina el dictamen por considerar que la única forma práctica de actuar, ante tales peticiones de información, consiste en que la AEAT ponga de manifiesto (al requeriente) las limitaciones que el artículo 113.1 de la LGT impone al uso de los datos de que dispone, pero "dejando en mano de los jueces, tribunales y fiscales la decisión última sobre si dicha información ha de ser cedida o no y, en caso de conclusión afirmativa, trasladar a éstos la responsabilidad por el eventual uso indebido de la información cedida".[61]

En realidad, con esta hábil modalidad "práctica" de actuación, la Administración logra estratégicamente su confesado objetivo, poner a salvo su responsabilidad, exigible por dos frentes, dependiendo de la decisión que adopte

■[60] So pena, a nuestro entender, de incurrir en el tipo criminal de usurpación de atribuciones previsto y penado en los artículos 506 a 509 del Código Penal aprobado por la Ley Orgánica 10/1995, de 23 de noviembre.

■[61] Consideración innecesaria, a nuestro juicio, pues este traslado de responsabilidad ya está previsto en la LORTAD respecto de las cesiones de datos (art. 11.5).

de atender o no la petición de cesión de datos.

B) CONSECUENCIAS DE LA NO CESIÓN.

En primer lugar, supongamos que la Administración Tributaria decide incumplir la orden de ceder los datos reservados, por estimar que el mandato no es de obligado cumplimiento.

Cabe considerar, por una parte, que si las resoluciones judiciales, según el artículo 18.1 de la LOPJ sólo pueden dejarse sin efecto en virtud de los recursos previstos en las leyes, y que como tercero que es, la Administración carece de legitimación procesal para recurrir, no le queda otra alternativa al cumplimiento del mandato que la desobediencia al mismo.

Por otra parte, ha de tenerse presente que, la obediencia debida ha sido suprimida del catálogo de las causas de justificación en el nuevo Código Penal, por entenderse que su presencia tan sólo pretendía reforzar extremadamente el deber de obediencia en determinados ámbitos (militar, funcionarial), aun a costa de resignarse a que sea jurídicamente obligatorio el cumplimiento de órdenes ilegales.[62]

Además, y en último lugar, el vigente Código Penal hace perdurar la figura de los mandatos antijurídicos obligatorios, como se desprende del artículo 410, correlato del artículo 367 del CP/73, pues delimita un ámbito de órdenes que, por no infringir, clara, terminante y manifiestamente la ley, deben ser cumplidas siempre que revistan las formalidades prescritas.[63]

Sin embargo, la actuación administrativa no es una negativa abierta a dar el debido cumplimiento a una resolución judicial, no es la conducta que tipifica el

■[62] Existe un riesgo en el caso de diligencias probatorias, que puede ser fuente de problemas, pues la parte perjudicada por la información así obtenida puede invocar su nulidad, pues en puridad dicha prueba es ilícita, ya que aquellas pruebas obtenidas, directa o indirectamente, violentando los derechos o libertades fundamentales lo son (artículo 11. 1 de la LOPJ).

■[63] En este sentido OBREGON GARCIA, Antonio, en "Las Causas de exclusión de la responsabilidad criminal en el Código Penal de 1995" Boletín de Información del Ministerio de Justicia nº 176-87, pp. 5 y ss.

artículo 410.1 del CP/1995, sino una suspensión de la ejecución de una orden, que tras recibir la desaprobación será efectivamente ejecutada.

No obstante, si fuera una negativa abierta, según el art. 410.2 del texto punitivo, podría estar exenta de responsabilidad, si se estima que el mandamiento constituye una infracción manifiesta, clara y terminante del artículo 113.1 de la LGT.

También cabe, por otra parte, la posibilidad de que la negativa a ceder los datos reservados fuera calificada jurídicamente como una conducta delictiva de denegación de auxilio a la Administración de Justicia, previsto y penado en el artículo 412.1 y 2 del CP/1995, y en este caso no cabe suspender la obligación de prestar la colaboración requerida.

C) CONSECUENCIAS DE LA CESION.

Por el contrario, y en segundo lugar, puede que la Administración decida cumplir la orden de ceder datos, bien desde el primer momento en que la reciba, bien en un momento posterior, tras la desaprobación por el Juez de la suspensión o inejecución de su orden de ceder los datos, para no incurrir en ninguno de los tipos penales comentados ni en el de usurpación de funciones del artículo 508.1 CP/1995, aún le quedaría como recurso, para tratar de salvar su posible responsabilidad penal por un presunto delito de violación de secretos previstos y penados en los arts. 415 y 417 del CP/1995, la alegación de las eximentes de estado de necesidad (art. 20.5) y/o de obrar en cumplimiento de un deber (art. 20.7).

En cuanto a responsabilidad disciplinaria en materia de protección de datos personales, la vulneración del deber de guardar secreto puede constituir una infracción grave o muy grave. Constituye infracción grave, cuando no se refiera a datos especialmente sensibles, en que sería muy grave (art. 43. 3. g LORTAD). La cesión o comunicación de los datos de carácter personal, fuera de los casos en que estén permitidas, es una infracción muy grave (art. 43. 4. b LORTAD).

No obstante, según el art. 45.2 LORTAD, en el caso de ficheros de titularidad pública, podrán iniciarse actuaciones disciplinarias a propuesta del Director de la Agencia, pero el procedimiento y sanciones a aplicar serán las establecidas en la legislación sobre régimen disciplinario de las Administraciones Públicas.

Por lo que se refiere a las eventuales responsabilidades civiles, dimanantes de un presunto uso indebido de los datos objeto de cesión no permitida, habrán de canalizarse por los trámites de la Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen, cuyo artículo 9.1 establece como cauces para la tutela judicial frente a las intromisiones ilegítimas en los derechos a que dicha ley se refiere los ofrecidos por las vías procesales ordinarias, Ley 62/1978, de protección jurisdiccional de los derechos fundamentales, o por procedimiento jurisdiccional ordinario de amparo previsto en el art. 53.2 CE (aún sin desarrollar) o, cuando proceda, por el recurso de amparo ante el TC (arts. 41 y siguientes de la LOTC).

CONCLUSIÓN

Las interferencias derivadas de la común proyección de las respectivas esferas de actuación de las dos instancias públicas implicadas, la tributaria y la judicial, sobre un mismo campo de operaciones: la información económica personal de los ciudadanos, se han saldado, en ocasiones, con situaciones de tensión y cierto enfrentamiento, entre ambas instituciones, evidenciando una notable confusión jurídica surgida a raíz de la diversidad en la inteligencia y aplicación práctica del artículo 113 de la LGT.

El núcleo de la cuestión se centra en si cabe oponer a la petición de cesión de información procedente de un Juzgado o Tribunal (o del Ministerio Fiscal) el carácter reservado de la misma declarado por el artículo 113.1 de la Ley General Tributaria, siempre que dicha cesión esté directamente relacionada con la funciones legítimamente atribuidas y ejercidas. La respuesta, a nuestro entender, en justicia, ha de ser negativa.

El citado debate evidencia la dificultad del legislador para determinar a través de disposiciones generales [64], de una parte, el alcance de los derechos fundamentales como límites a la actuación del poder público y, de otra, la de articular las relaciones entre las diversas instancias del Estado, por ser cuestiones que se sitúan en dos planos diferentes, el de la legalidad y el de constitucionalidad, pero que pueden afectar a particulares.

■[64] PRIETO SANCHIS, Luis, en "El sistema de protección de los derechos fundamentales: el artículo 53 de la C.E.". Anuario de Derechos Humanos nº 2. Madrid, 1983.

La solución al conflicto de las cesiones de datos personales a requerimiento judicial, creemos que puede ser contemplado como un problema de eficacia de los derechos fundamentales frente a terceros, que se reduce a un problema de coexistencia de derechos e incluso de valores constitucionales, que no puede resolverse en abstracto y de una vez para siempre.

La medida práctica que procede adoptar es de carácter normativo, consistente en establecer una cláusula de excepción a la reserva que, junto a los restantes supuestos de excepción b) a e) del artículo 113 de la LGT, sustituya a los actuales apartados a) y f) por una previsión genérica que diga: "salvo resolución judicial motivada", -al estilo de los supuestos previstos en los apartados 2 y 3 del artículo 18 de la Constitución, y art. 232.2 de la LOPJ- para que sea entonces el Juez quien determine caso por caso la prevalencia entre los intereses en conflicto, pero, desde luego, sin excluir a priori la eficacia de las libertades en las relaciones entre particulares.

Dicha resolución judicial debe revestir la forma de auto, en cuyo seno se pondere y realice un previo juicio de proporcionalidad de los valores en juego. Así, la injerencia autorizada judicialmente, rodeada de las necesarias garantías y circunscrita al ámbito de lo que resulte indispensable para defender o salvaguardar otros derechos e intereses dignos de protección, no se consideraría productora de un menoscabo ilícito del derecho a la intimidad del afectado, alcanzándose un equilibrio con el derecho de otras personas a la tutela judicial efectiva sin indefensión.[65]

El efecto práctico de la medida normativa propuesta, sin perjuicio de los cauces ordinarios previstos en la Constitución (art. 87 CE) para la iniciativa legislativa, puede alcanzarse de la mano de los jueces con ocasión de la aplicación del principio de interpretación y aplicación de las normas conforme a la Constitución (artículo 5.1 de la LOPJ) que han de buscar el acomodo de la norma

■[65] Las resoluciones de los tribunales, según QUADRA SALCEDO, Tomás de la, en "El recurso de amparo y los derechos fundamentales en las relaciones entre particulares" Cívitas. Madrid, 1981, si se entiende que no protegen adecuadamente y correctamente los derechos y libertades, pueden ser recurridas ante el Tribunal Constitucional por la vía de amparo, puesto que aquí tenemos un acto del poder público que ha desconocido un derecho fundamental.

aplicable -en el presente caso el artículo 113, 1 de la LGT- al ordenamiento constitucional, y si esta es de rango legal y de su validez depende el fallo de algún proceso, cuando dicho acomodo no sea posible, plantearán la cuestión de inconstitucionalidad ante el Tribunal Constitucional, pues lo que en ningún caso cabe es una actuación contraria a los derechos fundamentales, a cuya protección están llamados (artículo 7 de la LOPJ) y a garantizar su integridad bajo su tutela judicial efectiva, sin indefensión.

Confiemos pues en que, a través de la cuestión de inconstitucionalidad prevista en el artículo 163 de la Constitución, pueda dilucidarse, cuanto antes, si el responsable de los ficheros fiscales en los casos de cesión legalmente no permitida, se encuentra en un auténtico estado de necesidad -pues para evitar un mal propio (la responsabilidad criminal, exigible por incumplir una orden judicial o denegar un auxilio judicial, o usurpar funciones impidiendo la ejecución de aquella) o ajeno (menoscabar el derecho a la tutela judicial de quien precisa la información para defender sus legítimos derechos e intereses) lesiona un bien jurídico de otra persona (la intimidad del afectado) o infringe un deber (de secreto profesional)-. Así como aclarar si es obligatorio cumplir un mandato que, se reputa antijurídico en términos de legalidad, pero, en cambio, puede mostrarse lleno de justicia en parámetros constitucionales.

Como se puede deducir de la situación descrita, el Derecho, en general, se adapta mal a los desafíos a que conduce el irreversible fenómeno de la informática, se hace patente que las nuevas tecnologías de la información constituyen un auténtico factor de subversión del Derecho común,[66] y queda evidenciado, al mismo tiempo, la incidencia de la informática en el proceso, y por tanto la necesidad de armonizar ambas legislaciones, buscando la unidad, plenitud y coherencia que deben presidir el ordenamiento jurídico.

Superar con éxito el reto que supone pacificar la cuestión del acceso judicial a los datos tributarios reservados exige diseñar con especial mesura una nueva regulación de las c siones de datos personales contenidos en los ficheros tributarios que, a la luz de los principios del ordenamiento, faros guía que iluminan la labor de los juristas, logre conciliar los diferentes intereses en juego,

■[66] CARRASCOSA LOPEZ, Valentín y otros, en "El derecho de la prueba y la informática" en Informática y Derecho 2-UNED. Mérida, 1991.

pero esto, como ya hemos apuntado, resulta difícil de realizar en términos abstractos y de una vez por todas, por lo que proponemos confiar la resolución de estos conflictos a quienes el ordenamiento jurídico designa como garantes prioritarios de los derechos y libertades de los ciudadanos, esto es, a los Jueces y Tribunales.

BIBLIOGRAFIA

ALVAREZ CIENFUEGOS, José María : "Sistemas informáticos para la Administración de Justicia, en el ámbito de las Comunidades Autónomas. Planes Territoriales de Formación" C.G.P.J. 1993.

ALVAREZ CIENFUEGOS, José María: "La confidencialidad de los datos tributarios y el derecho de acceso de los contribuyentes", en Actualidad Jurídica Aranzadi. (Núm.226) Diciembre/1995.

ALVAREZ CIENFUEGOS, José María: "Función de los Jueces en la creación del Derecho", Ciclo de Conferencias LA UNIVERSIDAD Y LAS PROFESIONES JURÍDICAS: Deontología, función social y responsabilidad". Organizado por el Consejo Social de la Universidad Complutense de Madrid. Enero, 1997.

ASIS ROIG, Rafael De: "Deberes y obligaciones en la Constitución" Centro de Estudios Constitucionales. Madrid, 1991.

CABAÑAS GARCIA, Juan Carlos: "La valoración de las pruebas y su control en el proceso civil. Estudio dogmático y jurisprudencial". Ed. Trivium. Madrid, 1992.

CALVO ORTEGA, Rafael: "El fraude fiscal como factor de desigualdad" en Jornadas sobre El principio de Igualdad (conferencia 7 marzo 1996) Universidad de Alcalá de Henares.

CARRASCOSA LOPEZ, Valentín y OTROS: "El derecho de la prueba y la informática", en Informática y Derecho Núm 2, UNED-Mérida, 1992.

CARRASCOSA LOPEZ, Valentín: "La LORTAD: una necesidad en el panorama legislativo español", En Informática y Derecho Núm. 6-7, UNED-Mérida, 1994.

CHECA GONZALEZ, Clemente: " La interpretación de las normas tributarias en la Ley de modificación parcial de la LGT", en Actualidad Jurídica Aranzadi (Núm. 216) Octubre / 1995.

CORTES DOMINUGEZ, Valentín: Prólogo a la primera edición de la Ley de Enjuiciamiento Civil, Ed. Tecnos, 1985.

DAVARA RODRIGUEZ, Miguel Angel: "Derecho informático", Ed. Aranzadi, 1993.

DAVARA RODRIGUEZ, Miguel Angel: " La Ley Orgánica de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal", en Encuentro sobre Informática y Derecho 1992/1993, Ed. Aranzadi.

ESTADELLA YUSTE, Olga: "La protección de la intimidad frente a la transmisión internacional de datos personales". De. Tecnos. Madrid. 1995.

GESTO ALONSO, Blanca: " La pertinencia y utilidad de las pruebas" Servicio de Publicaciones de la Universidad de Navarra. Pamplona, 1991.

GIMENO SENDRA,Vicente: "Constitución y proceso" Ed. Tecnos. Madrid, 1988.

HEREDERO HIGUERAS, Miguel: "La Ley Orgánica 5/1992, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal. Comentarios y Textos." Ed. Tecnos. Madrid, 1996.

LUCAS MURILLO DE LA CUEVA, Pablo: "Informática y protección de datos personales. (Estudio sobre la LORTAD), en Cuadernos y Debates. Centro de Estudios Constitucionales. Madrid. 1993.

MARZAL HERCE, Gloria: "Bases de datos personales: requisitos para su uso. Comentarios a la LORTAD y normativa complementaria", Ediciones Deusto. Bilbao. 1996.

MUÑOZ SABATÉ, Luis: "Técnica probatoria. Estudios sobre las dificultades de la prueba en el proceso." Ed. Praxis. Barcelona, 3ª ed. 1993.

OBREGON GARCIA, Antonio: "Las causas de exclusión de la responsabilidad

criminal en el Código Penal de 1995" Boletín de Información del Ministerio de Justicia, núms. 1786-87.

OROZCO PARDO, Guillermo: en "Informática y Derecho 6-7" UNED-Mérida, 1994.

ORTIZ NAVACERRADA, Santiago: "La prueba de documentos privados en el proceso civil", en Cuadernos de Derecho Judicial XXXIV. C.G.P.J.-1993

PEREZ LUÑO, Antonio Enrique: "Entre las luces y las sombras", en Informática y Derecho 6-7, UNED-Mérida.1994

POMED SANCHEZ, Luis Alberto: "El derecho de acceso de los ciudadanos a los archivos y registros administrativos". Instituto Nacional de Administración Pública. Madrid, 1989.

PRIETO SANCHÍS, Luis: "El sistema de protección de los derechos fundamentales: el artículo 53 de la C.E." Anuario de Derechos Humanos nº 2. Madrid, 1983.

QUADRA SALCEDO, Tomás de la: " El recurso de amparo y los derechos fundamentales en las relaciones entre particulares" Cívitas. Madrid, 1981.

ROMEO CASABONA, C. M.: "Infracciones administrativas y penales en relación con la protección de datos", en Informática y Derecho 6-7, UNED-Mérida.1994.

SAINZ MORENO, Fernando: en "Principios éticos y responsabilidad en el ejercicio de la función pública" Ciclo de conferencias sobre La Universidad y las profesiones jurídicas: Deontología, función social y responsabilidad. Organizado por el Consejo Social de la Universidad Complutense de Madrid. Enero, 1997.

TIJERAS COZAR, Ramón: "Abogados de oro. El negocio de los bufetes". Ediciones Temas de hoy. Madrid, 1997.

VILLAPALOS, Gustavo y LOPEZ QUINTAS, Alfonso: "El libro de los valores", Planeta, 1997 (3ª edición).

WESTIN, Alan F.: "Privacy and Freedom" Atheneum. Nueva York, 1970 (6ªreimpresión de la edición de 1967).

Los programas de ordenador: Análisis de su imposición directa

MARÍA JESÚS GARCÍA-TORRES FERNÁNDEZ

Doctora en Derecho. Profesor Asociado de Derecho Financiero Universidad de Granada

1. INTRODUCCION

En nuestro panorama diario se encuentra presente, y para muchos de una manera imprescindible, el ordenador. Pero, al margen del aspecto tangible de esta máquina, se encuentran el conjunto de ordenes intelectuales internas destinadas a regir su funcionamiento, el programa de ordenador o software, sin en cual el hardware o maquinaria resulta inservible.

Dentro del concepto de software, se pueden distinguir dos tipos de programas principales: el unido al material, es decir, a la máquina e imprescindibles para que esta dé algún resultado, y los programas de aplicación del usuario [67].

Los programas de aplicación del usuario son consecuencia de una relación mercantil larga que va desde la creación del programa por el autor y su comercialización hasta llegar al consumidor final, el usuario, lo que hace que el

■[67] El Consejo de Cooperación Aduanera de Bruselas, en el Estudio III sobre "Valor en Aduana de los ordenadores y soportes de programas", recogido en el Anexo 4 de la circular 824 de la DG de Aduanas e Impuestos Especiales, define como programa "las instrucciones que mandan el funcionamiento del ordenador", distinguiendo dos tipos de programas principales: a) El (...) unido al material, y b) los programas de aplicación del usuario.

tratamiento de los sistemas y programas de ordenador en nuestro sistema tributario es complejo en cuanto que en un mismo objeto, el programa, están implicados distintos sujetos pasivos con distintos derechos sobre él, cada uno sujetos a su modalidad tributaria. La existencia de distintos sujetos pasivos tiene su origen en la compleja relación mercantil que genera este tipo de elementos.

Por ello, es necesario determinar en un primer lugar su calificación según el ordenamiento jurídico civil, para después situarlo en el plano tributario y contable.

2. CLASIFICACION DESDE EL PUNTO DE VISTA CIVIL

Al analizar la clasificación jurídica de los programas de ordenador nos encontramos en un primer momento con la duda de si se tratan de elementos de la propiedad intelectual o de la propiedad industrial, ya que el soporte lógico es mas un producto de empresa, producto industrial, que una creación que pone en juego la persona del autor [68]. No obstante, esta polémica ya ha sido resuelta y los programas de ordenador no se consideran como propiedad industrial porque no constituyen una solución que consiga un determinado resultado por el empleo de las fuerzas naturales, sino que poseen un contenido esencialmente intelectual, es una obra de una concepción humana[69]. El reconocer la probabilidad de que si otros realizan los esfuerzos adecuados pueden llegar a crear un soporte sustancialmente idéntico no les excluye la protección a la que tienen derecho, que viene dada por el reconocimiento de su primacía.

El objeto de la propiedad intelectual son las creaciones originales literarias, artísticas o científicas expresadas en cualquier medio o soporte, tangible o intangible, actualmente conocido o que se invente en el futuro.

■[68] ALBALADEJO, MANUEL Y OTROS "Comentarios la Código Civil y Compilaciones forales". Editorial Edersa. Página 731.

■[69] BAYLOS CORROZA; Hermenegildo: Derecho de Tratado Industrial. Editorial Civitas.1993. Página 630.

Los artículos 428 y 429 del Código Civil regulan la propiedad intelectual mediante una remisión directa a la normativa específica sobre la materia [70].

Los programas de ordenador se definen en el artículo 96-1 del Real Decreto Legislativo 1/1993 del Texto Refundido de la Propiedad Intelectual,[71] como" *(...)toda secuencia de instrucciones o indicaciones destinadas a ser utilizadas, directa o indirectamente, en un sistema informático para realizar una función o una tarea o para obtener un resultado determinado, cualquiera que sea su forma de expresión y fijación*". Con relación a la documentación técnica y a los manuales de uso del programa, el artículo 96-2 los asimila al propio programa en la medida que les otorga la misma protección.

Los programas de ordenador se califican por la legislación sobre propiedad intelectual como derechos de autor [72] , que posee una doble vertiente: Derecho moral y derecho de explotación. La propiedad intelectual, o también denominada derechos de autor, es el derecho absoluto de señorío que tiene el autor sobre su obra intelectual, ya sea literaria, artística o científica. Junto con el derecho moral, el derecho de explotación constituye un derecho de contenido económico, temporalmente limitado e incluido dentro del inmovilizado inmaterial.

■[70] Artículo 429 del Código Civil: "La ley sobre propiedad intelectual determina las personas a quienes pertenece ese derecho, la forma de su ejercicio y el tiempo de su duración. En los casos no previstos ni resueltos por dicha Ley se aplicarán las reglas generales establecidas en este Código sobre la propiedad.".

■[71] El Real Decreto Legislativo 1/1996, de 12 de abril se aprueba el Texto Refundido de la Ley de Propiedad Intelectual, regularizando, aclarando y armonizando las disposiciones vigentes sobre la materia. Esta norma viene a sustituir un gran cantidad de disposiciones que se habían ido dictando tras la Ley 22/1987, de 11 de noviembre, de Propiedad Intelectual. En materia de propiedad intelectual referida a las aplicaciones informáticas, deroga la Ley 16/1993, de 23 de diciembre sobre la Protección Jurídica de Programas de Ordenador, que se dictó en adaptación a la Directiva del Consejo de 14 de mayo de 1991 relativa a la Protección Jurídica de los Programas de Ordenador (DOCE, núm. L.122/42, 17 mayo de 91), y en otras Propuestas de directiva relacionadas con la Propiedad Intelectual

■[72] Artículo 95, RDL 1/1996: "El derecho de autor de los programas de ordenador se regirá por los preceptos del presente Título y, en los que no esté específicamente previsto en el mismo, por las disposiciones que resulten aplicables de la presente Ley."

Desde el punto de vista jurídico, los sistemas y programas informáticos son considerados como propiedad intelectual del creador y están protegidos por el Real Decreto Legislativo 1/1996 del Texto Refundido de la Propiedad Intelectual. Y como consecuencia de su clasificación jurídica de propiedad intelectual, por regla general, cuando son adquiridos por terceras personas no se adquiere la propiedad de los mismos sino su licencia de uso, es decir, un derecho, ya que la creación es la única manera de adquisición originaria del derecho de autor [73].

De la calificación de los sistemas y programas de ordenador como propiedad intelectual se extraen dos características importantes:

1º) Es un derecho limitado. En principio, la propiedad intelectual no está sometida a plazo alguno por lo que se refiere a su vertiente "moral o personal mínima". Unicamente estará sometida a plazo la protección de su vertiente patrimonial o de explotación [74], que en el caso de los programas de ordenador dependerá si se trata de persona física o jurídica.

En el supuesto de que el autor sea una persona física, la protección del derecho de explotación será toda la vida del autor y los sesenta años siguientes [75].

■73 Para conocer la clasificación de los sistemas informáticos como propiedad intelectual: OROZCO PARDO, GUILLERMO: "Informática y propiedad intelectual". Actualidad Informática Aranzadi nº 19. Abril 1996. Página 1. ALBALADEJO, MANUEL Y OTROS "Comentarios la Código Civil y Compilaciones forales". Editorial Edersa. Página 747. BONDIA ROMAN, FERNANDO: "Los programas de ordenador en la Ley de Propiedad Intelectual y en la Directiva CEE de 14 de mayo de 1991". Revista Derecho de los Negocios. Año 3. Nº 27.

■74 Artículo 17 del RDL 1/1996: "Derecho exclusivo de explotación y sus modalidades." Corresponde al autor el ejercicio exclusivo de los derechos de explotación de su obra en cualquier forma y, en especial, los derechos de reproducción, distribución, comunicación pública y transformación, que no podrán ser realizadas sin su autorización, salvo en los casos previstos en la presente Ley".

■75 El artículo 98, párrafo 1 del RD 1/1996 nos remite al Capítulo I del Título III para determinar la protección del derecho de explotación de las personas físicas. En el artículo 26 se regula este supuesto en los siguientes términos. Artículo 26. Duración y cómputo." Los derechos de explotación de la obra durarán toda la vida del autor y setenta años después de su muerte o declaración de fallecimiento".

En el caso de que el autor sea una persona jurídica durará 60 años contados desde el día uno de enero del año siguiente al de la divulgación lícita del programa o al de su creación si no se hubiera divulgado [76].

Los plazos de protección establecidos en esta Ley se computarán desde el día 1 de enero del año siguiente al de la muerte o declaración de fallecimiento del autor o al de la divulgación lícita d la obra, segúnproceda.

Así, tras la extinción de los derechos de explotación se determinará su paso al dominio público, de forma que podrán ser utilizadas por cualquiera tanto la explotación como actuar sobre la propia obra, quien podrá introducir en ella variaciones esenciales. La falta de protección de la obra por el derecho interno no impide que pueda quedar protegida la obra española en otros países en virtud de sus leyes territoriales o de los convenios internacionales suscritos por España [77].

2º) Es un derecho transmisible. El autor o sus causabientes pueden disponer de ella a su voluntad en lo que se refiere a los derechos de explotación. En consecuencia, pueden transmitir el derecho por un período de tiempo definido o indefinido. En este último caso, sabemos que se extingue el derecho de la exclusividad en el plazo señalado anteriormente.

3. INTRODUCCION AL ESTUDIO TRIBUTARIO DE LOS PROGRAMAS INFORMATICOS.

El reconocimiento de los programas de ordenador como parte del inmovilizado inmaterial y de la Propiedad Industrial se realiza también por el Ministerio Economía y Hacienda en contestación a consultas planteadas por el contribuyente:

■[76] Artículo 98, párrafo 2, del RD 1/1996.

■[77] ALBALADEJO, MANUEL Y OTROS "Comentarios al Código Civil y Compilaciones forales". Editorial Edersa. Página 788.

" No forma parte del equipo informático (inmovilizado material), el programa necesario para su utilización. Los programas de ordenador están regulados expresamente en el título VII de la Ley 22/87 de la Propiedad intelectual como uno de los derechos de autor" [78].

La dificultad entraña en el estudio tributario de las aplicaciones informáticas parte de las distintas personas, físicas o jurídicas, que pueden estar ligadas a un mismo producto, sobre el que disfrutan de distintos derechos. Así, una misma aplicación de software implica para el usuario, el autor y el titular de los derechos de explotación, como consecuencia de ejercer los derechos que cada uno de ellos ostentan, circunstancias que generan hechos imponibles distintos y simultáneos [79] .

El objeto de este trabajo se centra en determinar la naturaleza de cada hecho imponible que se da alrededor de una aplicación informática, desde su creación hasta su comercialización, su calificación tributaria y las especialidades que reúne frente a hechos imponibles de naturaleza similar, sin entrar a analizar aquellas características comunes con carácter general a todos ellos. Para hacer frente a este estudio vamos a analizar cada uno de los sujetos implicados y los hechos imponibles que se derivan como consecuencia de su relación con la aplicación informática.

3.1. EL AUTOR.

El autor es la persona física que ha desarrollado el programa de ordenador [80]. El derecho de autor comprende dos derechos protegidos como propiedad intelectual:

■[78] Resolución de la Dirección General de Tributos de 9 de marzo de 1990.

■[79] La importancia de determinar el hecho imponible está recogida en el artículo 25 de la LGT: "1°. El impuesto se exigirá con arreglo a la verdadera naturaleza jurídica o económica del hecho imponible; 2°.- Cuando el hecho imponible consista en un acto o negocio jurídico se calificará conforme a su verdadera naturaleza jurídica, cualquiera que sea la forma elegida o la denominación utilizada por los interesados, prescindiendo de los defectos intrínsecos o de forma que pudieran afectar su validez; 3°.- Cuando el hecho imponible se delimite atendiendo a conceptos económicos, el criterio para calificarlos tendrá en cuenta las situaciones y relaciones económicas que, efectivamente, existan o se establezcan por los interesados, con independencia de las formas jurídicas que se utilicen".

■[80] Artículo 97,1 RDL 1/1996: "Será considerado autor del programa de ordenador la persona o grupo de personas naturales que lo hayan creado, o la persona jurídica que sea contemplada como titular de los derechos de autor en los casos expresamente previstos por esta Ley."

- Derecho moral del autor: es un derecho irrenunciable e intransferible, y al mismo tiempo no es susceptible de valoración económica, luego carece de relevancia tributaria.

- Derechos de explotación: Es la venta o comercialización de la aplicación informática y, por tanto, lo que reporta beneficios económicos al autor. Es el derecho que tiene relevancia económica, y será el objeto de la imposición tributaria.

No puede confundirse la cesión de los derechos de propiedad intelectual sobre un programa de ordenador con la venta de los productos derivados de la explotación de los derechos cedidos; tales productos se conocen con la denominación de software standard, que puede ser adquirido en propiedad por cualquier persona que lo necesite, es decir, el usuario, cuyas consecuencias tributarias vamos a estudiar mas adelante.

El derecho de explotación es transferible, total o parcialmente, y abre la posibilidad de que una persona distinta del autor lo gestione, de lo que resultan dos situaciones:

-El autor ejerce directamente el derecho de explotación.
- El autor cede los derechos de explotación, tanto por transmisión onerosa o lucrativa.

Junto con el autor persona física, una persona jurídica podría ser el autor de un programa de ordenador, pero en última instancia éste sería desarrollado por personas físicas, sus autores materiales, que habrían renunciado a sus derechos de explotación como consecuencia de su relación laboral con la empresa para la que trabajan [81]. No es este lugar de entrar a discutir en que queda derecho moral del autor que trabaja como asalariado para una persona jurídica, sobre todo porque carece de relevancia tributaria, pero sí tener presente la posibilidad de la persona jurídica que genera en su actividad empresarial un programa de ordenador para utilizarlo como mercadería.

[81] El artículo 97, párrafo cuatro del RD 1/1996 establece: "Cuando un trabajador asalariado cree un programa de ordenador, en el ejercicio de las funciones que le han sido confiadas o siguiendo las instrucciones del empresario, la titularidad de los derechos de explotación correspondientes al programa de ordenador así creado, tanto el programa fuente como el programa objeto, corresponderán, exclusivamente, al empresario, salvo pacto en contrario".

Tras esta introducción a la persona del autor nos interesa analizar sus consecuencias desde el punto de vista tributario. En cuanto que el ejercicio del derecho moral de autor no tiene incidencia en nuestro derecho tributario, nos debemos centrar en cómo repercute el derecho de explotación en la figura del autor. El derecho de explotación encierra la única forma de remuneración del trabajo del autor en el desarrollo del programa de ordenador y esta remuneración la podrá obtener bien cediendo este derecho de explotación o bien ejerciéndolo directamente. No vamos a centrar en la repercusión tributaria en la persona del autor de la cesión del derecho de explotación a terceras personas, ya que su ejercicio directo tiene carácter de actividad empresarial y lo analizaremos mas adelante [82].

3.1.1. EL IMPUESTO SOBRE LA RENTA DE LAS PERSONAS FISICAS:

En última instancia el autor es una persona física, por lo que los rendimientos que obtenga en el desarrollo de la actividad de explotación de los derechos de ordenador están sometidos al IRPF, si bien se encuadrarán en rendimientos de distinta naturaleza dependiendo de la relación mercantil que exista entre el autor y su obra.

3.1.1.1. RENDIMIENTOS DE ACTIVIDADES PROFESIONALES:

Cuando el autor renuncia el ejercer directamente el derecho de explotación del programa de ordenador, en este caso, se ha debido transmitir el derecho de explotación a una persona física o jurídica, y los rendimientos que por ello le satisfagan tendrán la consideración de rendimientos de actividades profesionales.

■[82] La naturaleza de la cesión del derecho de autor no está definida en el Impuesto sobre la Renta de las Personas Físicas. Sin embargo, en el Impuesto sobre el Valor Añadido se define como prestación de servicios la remuneración que se recibe a cambio por parte del autor. El artículo 11 en su párrafo 2, 4° de la Ley del IVA, Ley 37/1992, de 28 de diciembre establece: Se considerarán prestaciones de servicios las cesiones y concesiones de derechos de autor,..., y demás derechos de la propiedad intelectual.

■Esta definición es importante porque de considerarse entrega de bienes podría haber planteado problemas de considerar la cesión de explotación de la aplicación informática, como elemento del inmovilizado inmaterial que es, incremento o disminución de patrimonio afecto a la actividad empresarial. En cambio, al tener la consideración de prestación de servicios encaja con la naturaleza de rendimientos de actividades profesionales como vamos a estudiar a continuación.

El modo en el que se ha realizado el traspaso de la titularidad del derecho de explotación desde el autor a la empresa tendrá importantes repercusiones:

a) Si se ha abonado un canon periódico, no se produce cesión de la titularidad por parte del autor, sino una cesión temporal del derecho de explotación. En este caso, el ingreso del titular será importe total del canon recibido cada período impositivo. El canon tiene el mismo tratamiento tributario del alquiler y tiene en todo caso la consideración de renta regular del ejercicio.

b) Si se ha abonando una remuneración a tanto alzado por la cesión del programa, se ha de analizar si se podrá clasificar como renta regular o irregular, circunstancia que tendrá importantes repercusiones tributarias en el sujeto pasivo.

En el Impuesto sobre la Renta de las Personas Físicas [83] la duración del período impositivo se establece, con carácter general, en el artículo 93 de la Ley del Impuesto identificándolo con el año natural. Esta concordancia entre período impositivo y año natural ocasiona que en aquellos supuestos en que la generación de una determinada renta supere dicho período de tiempo, ésta reciba un tratamiento especial: el de renta irregular [84].

■[83] La normativa reguladora del Impuesto sobre la Renta de las Personas Físicas (IRPF) es la Ley 18/1991, de 6 de junio por la que se aprueba la Ley reguladora del impuesto, y el Real Decreto 1841/1991, de 30 de diciembre, por el que se aprueba su Reglamento.

■[84] Artículo 57 de la Ley 18/1991 del IRPF establece: "A los efectos de esta Ley la renta de cada sujeto pasivo se dividirá, en su caso, en dos partes:

a) Renta regular
b) Renta irregular"

El tratamiento en el IRPF de cada una de las masas de renta será distinto: La renta regular se compensará e integrará conforme a las normas del Capítulo IV del Título V del texto legal y, en particular, se integrará y compensará exclusivamente con los restantes incrementos y disminuciones regulares del período impositivo, de acuerdo con lo dispuesto por el apartado uno del artículo 62 de la citada Ley de IRPF.

Los rendimientos irregulares del trabajo personal o del capital así como los rendimientos irregulares positivos de actividades empresariales o profesionales, se dividirán por el número de años comprendidos en el período en que se hayan generado, contados de fecha a fecha. En el caso de que no pueda determinarse dicho período se tomará el de cinco años.

El artículo 59 de la Ley del IRPF considera irregulares *"los rendimientos que se obtengan por el sujeto pasivo de forma notoriamente irregular en el tiempo o que, siendo regular, su ciclo de producción sea superior a un año"*. Conforme con lo aquí expuesto, el requisito básico que tiene que concurrir para calificar como irregulares unos rendimientos es que su período de producción exceda del año. Esto supone una correlación absoluta entre rendimientos y período de generación, es decir, que el acto productor de los ingresos se desarrolle a lo largo de un período temporal superior al año.

El caso de nuestro estudio es aquel por el que se realiza una remuneración única que engloba el total de tiempo trabajado: De acuerdo con lo establecido en el artículo 59, Uno.b) de la Ley del IRPF, si la prestación representa el pago único por todos los años trabajados del consultante, dicha cantidad tendrá, a la vista del citado artículo, el carácter de renta irregular a efectos de la liquidación anual por el IRPF. El desarrollo de un programa de ordenador por parte de su autor puede exceder con creces de un año natural. Existen clasificaciones de renta irregular para aquellas producciones que necesitan mas de un año para producir rendimientos y cuya constatación con la realidad es fácil, como es el caso de las producciones madereras. Sin embargo, cuando entramos a valorar el trabajo profesional, en cuanto que son temas subjetivos difícilmente cuantificables, no existe una solución única.

Uno de los requisitos, junto con el temporal, que se exigen para que tenga la consideración de renta irregular es que no se trate de actuaciones aisladas [85] que aunque puedan producirse en distintos años, no suponen una dedicación superior al año. Lo que excluiría aquellas cantidades recibidas en concepto de mantenimiento de actualización del programa informático, y siempre tendría la consideración de renta regular.

Pero para continuar en este tema de la renta irregular no hay que analizar únicamente los ingresos, sino también hay que tener en cuenta los gastos necesarios

El cociente así hallado se integrará con los rendimientos regulares del sujeto pasivo para determinar su renta irregular.

■[85] Consultas no vinculante de la Dirección General de Tributos sobre rentas irregulares: 6 de marzo de 1996 ; 7 de febrero de 1996.

para obtenerlos [86]. Este dato es importante en el caso de las obras en curso, que es el caso que estamos analizando. Si trasladamos nuestro análisis al sector inmobiliario, los promotores inmobiliarios no pueden deducir los intereses de los capitales ajenos utilizados para financiar obra en curso -que se debe contabilizar como existencia- ni los gastos que a dichas obras se refieran, hasta que se computen los correspondientes ingresos. El devengo, conforme al Plan de Contabilidad Sectorial de empresas inmobiliarias no se produce hasta el momento de la entrega efectiva de los inmuebles [87]. La conclusión que obtenemos de este pronunciamiento de la Dirección General de Tributos es que si se imputan los gastos antes de que se produzca el devengo de la renta irregular, se estaría negando implícitamente el carácter de irregular de este rendimiento. Por tanto, es importante determinar el momento del devengo de la obligación tributaria.

En la determinación en estimación directa del rendimiento neto de las actividades empresariales y profesionales de personas físicas serán de aplicación, sin perjuicio de lo previsto para la estimación objetiva, las normas del Impuesto sobre Sociedades. El artículo 42 de la Ley del IRPF remite a las normas del Impuesto sobre Sociedades [88], con carácter general. El Impuesto sobre Sociedades recoge, junto con el principio del devengo, el principio de correlación de ingresos y gastos, por el que el resultado de un ejercicio está constituido por los ingresos del período menos los gastos del mismo para la obtención de aquellos. Esta remisión a la normativa del IS es importante puesto que el IRPF adopta el concepto de exigibilidad como criterio de imputación de ingresos y gastos [89]: Los gastos, desde que su importe sea exigible por

■86 Para la determinación del rendimiento neto de una actividad empresarial se deducirán de los ingresos los gastos necesarios para su obtención, y por lo que respecta de a la modalidad de coeficientes, exclusivamente los gastos enumerados en las letras a) a f) y el porcentaje que corresponda. Dirección General de Tributos Contestación de 23 de marzo de 1994.

■87 Dirección General de Tributos, Resoluciones de 23 de enero de 1989 y de 14 de febrero de 1989.

■88 La normativa fundamental reguladora del Impuesto sobre Sociedades (IS) está formada por la Ley 43/1995, de 27 de diciembre , Ley del Impuesto, y el Real Decreto 537/1997, de 14 de abril, por el que se aprueba el Reglamento del Impuesto.

■89 El artículo 14.1 del Reglamento del IRPF establece como regla general para la imputación temporal de ingresos y gastos: Se imputarán al período en que se hubiesen devengado los unos y producido los otros, con independencia del momento en que se realicen los correspondientes

quien haya de percibirlos; los ingresos, desde el momento en que sean exigibles por el acreedor. En el IS, por un criterio económico influenciado por la contabilidad, se imputan los ingresos y gastos generados en el ejercicio, aunque se haya producido su exigibilidad con anterioridad.

Esta divergencia entre el IRPF y el Impuesto sobre Sociedades referida a las personas físicas se salva en el Reglamento del Impuesto sobre Sociedades, Real Decreto 537/1997, en cuya Disposición Adicional 1° recoge la posibilidad de imputar temporalmente los ingresos y los gastos conforme al criterio de cobros y pagos mediante una simple manifestación en tal sentido, en la declaración del IRPF, entre otros, los profesionales en estimación directa. La consecuencia que se extrae es importante en relación a la calificación de renta irregular, ya que el haber deducido los gastos antes de imputarse los ingresos no conllevará una renuncia al tratamiento de renta irregular porque no se ha incumplido el principio del devengo tributario, sino que se ha utilizado un sistema alternativo autorizado por la norma fiscal, resolviendo así la problemática que se había planteado antes de esta disposición.

En conclusión, no se puede determinar a priori y como regla general la naturaleza de renta irregular de los rendimientos profesionales del autor de un programa de ordenador, sino únicamente plantear esta posibilidad y estudiar cada caso concreto, teniendo siempre presente que lo importante es que la carga de la prueba recae sobre el sujeto pasivo y será el autor el que deberá probar que el trabajo se ha realizado en más de un ejercicio fiscal.

Un tema distinto a la consideración de renta irregular de la remuneración a tanto alzado por el derecho de explotación, es el caso de que el canon periódico satisfecho al autor se pague de una sola vez. En este caso nos encontramos con una renta del ejercicio pero se pueden plantear dos casos:

1. Que el período de devengo de dicho canon sea de un ciclo superior al año, por lo que la exigibilidad del primer ciclo de alquiler se produce a final del mismo, y la imputación del importe del alquiler se producirá en dicho año, y tendrá el tratamiento de renta irregular a efectos del IRPF. [90]

cobros y pagos.

■[90] Dirección General de Tributos, consulta de 3 de marzo de 1994 referida al arrendamiento de finca rústica en el que el alquiler se paga al final de los cinco años: Tendrá la consideración de renta

2. Que se satisfagan los cánones devengados mediante un pago único: El pago único es imputable, en la parte en que le corresponda, a los distintos años trabajados. Según lo dispuesto en el número seis del artículo 14 del Reglamento del IRPF, cuando se produzcan las situaciones reguladas en el mismo, deberán practicarse las liquidaciones complementarias correspondientes a los ejercicios en que, de acuerdo con las estipulaciones contractuales o disposiciones aplicables, fueran exigibles las contraprestaciones objeto de estudio ajustándose a la normativa entonces vigente, liquidaciones que no conllevan intereses de demora ni recargos y cuya presentación podrá efectuarse hasta el último día de plazo reglamentario de presentación de la declaración propia del año en que se perciben los atrasos.

Lo expuesto anteriormente son consideraciones generales sobre los rendimientos de actividades profesionales sometidos al IRPF. Sin embargo, para el cálculo de estos rendimientos la regulación del IRPF establece dos sistemas voluntarios: la estimación directa y la estimación objetiva.

A. ESTIMACION DIRECTA.

El cálculo de rendimientos de actividades profesionales sometidos al régimen de estimación directa se hará mediante la aplicación de la normativa del Impuesto sobre Sociedades, por lo que nos remitimos a la parte de este trabajo en la que se analiza la tributación de los rendimientos del derecho de explotación.

B. ESTIMACION OBJETIVA.

El régimen de estimación objetiva es un régimen voluntario de estimación de rendimientos de pequeños empresarios y profesionales que se articula en dos modalidades: estimación objetiva por signos, índices o módulos y estimación objetiva por coeficientes.

La estimación objetiva por signos, índices o módulos no es aplicable a actividades profesionales y únicamente a determinadas actividades empresariales que tienen asignadas los parámetros de cálculo en la Orden Ministerial que se aprueba cada año, siendo la última la Orden Ministerial de 27 de noviembre de 1997.

irregular.

La aplicación de esta modalidad en la persona del autor del programa informático está excluida por los propios requisitos que se exigen, y respecto del autor como empresario está excluido al carecer de referencia expresa en la Orden Ministerial citada. Contemplar la posibilidad de que se incluya en ediciones sucesivas es difícil dada la naturaleza y variedad del trabajo, tanto de programación como de distribución de las aplicaciones informáticas que son difíciles de reducir a parámetros generales para todo tipo de actividad.

La modalidad de estimación objetiva por coeficientes es aplicable a actividades empresariales que no les sea aplicable el sistema de signos, índices o módulos, por lo que será de aplicación en todo caso para los que desarrollan el derecho de explotación de los programas informáticos, siempre que el personal asalariado no exceda de 12 trabajadores y el volumen general de ventas no supere los 5.000.000 ptas. En el caso de los profesionales se exige que no superen los ingresos los 5.000.000 ptas. y no tengan personal asalariado.

El rendimiento neto en el sistema de estimación objetiva por coeficientes se calcula minorando el volumen de ingresos o ventas con determinados gastos establecidos por la ley, y además, el resultado se minora por un porcentaje sobre el volumen de ingresos, porcentaje cifrado en el 10% en el caso de profesionales y el 15% en el de empresarios. La aplicación de este porcentaje estimativo hace interesante este sistema para aquellos programadores que trabajan de forma independiente y tienen pocos gastos.

3.1.1.2. RENDIMIENTOS DE TRABAJO PERSONAL:

Cuando el autor material del programa ha trabajado para una persona jurídica, esta es la que en última instancia se reserva el derecho de autor en su vertiente de explotación. En este supuesto, el autor recibirá una remuneración a cambio de su trabajo y a efectos del IRPF tendrá la consideración de rendimientos de trabajo personal [91].

■[91] Artículo 24 de la Ley del IRPF establece: Se considerarán rendimientos íntegros del trabajo todas las contraprestaciones o utilidades, cualquiera que sea su denominación o naturaleza, que deriven directa o indirectamente, del trabajo del sujeto pasivo y no tengan el carácter de rendimientos empresariales o profesionales.

Los gastos deducibles aplicables a este tipo de rendimientos serán los previstos en el impuesto para este tipo de rentas, sin que se establezca ninguna excepción específica para la propiedad intelectual de las aplicaciones informáticas.

3.1.1.3. RENDIMIENTO DE CAPITAL MOBILIARIO:

Hemos visto que siempre se transmite por el autor el derecho de explotación, nunca el derecho de autor que es intransmisible, y esta transmisión puede hacerse a título lucrativo o a título oneroso. A su vez, la persona física que recibe este derecho de explotación puede ejercerlo de forma directa o indirecta, asignándose en consecuencia a distintas masas patrimoniales:

- Rendimientos de capital mobiliario, si cede su ejercicio a otra empresa a cambio de un canon, y siempre que quien realiza la cesión no sea su autor, puesto que en ese caso tendría la consideración de actividad empresarial.

-Rendimientos de actividades empresariales, si ejercita directamente el derecho de explotación del programa de ordenador.

Son rendimientos íntegros de capital la totalidad de las utilidades o contraprestaciones que provengan de elementos patrimoniales mobiliarios de los que es titular el sujeto pasivo y que no estén afectos a actividades empresariales o profesionales. Tradicionalmente se engloban dentro del los rendimientos del capital mobiliario todos aquellos rendimientos que proceden de la cesión de uso por parte del titular de determinados bienes muebles, en este caso el derecho de explotación.

El artículo 37.3.a de la Ley del IRPF establece:
" 3. Otros rendimientos de capital mobiliario. Quedan incluidos en este epígrafe, entre otros:
a) Los procedentes de la propiedad intelectual cuando el sujeto pasivo no sea el autor"

Por tanto, se somete a gravamen la cuantía íntegra devengada de la cesión de los derechos de explotación, lo que nos plantea dos cuestiones que debemos resolver:

a) Gastos deducibles: En los rendimientos de capital mobiliario los gastos aplicables a este tipo de ingresos están limitados. En concreto, en el caso de la propiedad intelectual no es posible deducir gasto alguno, salvo en los casos de prestaciones de asistencia técnica .

La expresión asistencia técnica no tiene un contenido netamente definido en nuestro sistema tributario. El Código de liberación de operaciones invisibles y corrientes de la OCDE (Anexo A, Apartado A.3) concibe la asistencia técnica como una actividad relacionada *"con la producción y distribución de bienes y servicios en todos sus grados, suministrada por un período de tiempo fijado en función del objeto particular de esta asistencia y en la que se incluyen, por ejemplo, consultas y visitas de expertos, preparación de planos y diseños, supervisión de fabricación, estudio de mercado y formación profesional"*, definición que se acepta como aplicable en nuestro sistema tributario [92]. Por tanto, únicamente tendrán la consideración de gasto deducible del capital mobiliario los gastos derivados de asistencia técnica al sujeto pasivo no autor que posee el derecho de explotación de la aplicación informática.

b) Retenciones aplicables: Como regla general los rendimientos de capital mobiliario procedentes de la propiedad intelectual están sujetos a retención, y a la hora del cálculo de la renta debemos partir de los ingresos íntegros. Sin embargo, estos rendimientos se exceptúan cuando constituyen ingresos de la actividad habitual. Por consiguiente, la cesión de derechos de autor realizada por una editorial a otra está sujeta a retención si cedente y cesionaria realizan la misma actividad, y el propósito de la cesión no es sino una actividad distinta, cercana a la comisión mercantil. Al contrario, si la cesión de derechos persigue una subcontratación o utilización de maquinaria ajena para llegar al tráfico regular de edición de libros, debe entenderse que los ingresos así obtenidos son ingreso de la actividad empresarial no susceptibles de retención [93].

3.1.1.4. RENDIMIENTOS DE ACTIVIDAD EMPRESARIAL.

El autor podrá ejercer directamente el derecho de explotación de su obra, si bien tendrá los rendimientos obtenidos tendrán la consideración de actividad empresarial desde el punto de vista tributario. Cuando la actividad empresarial de la

■[92] Resolución del TEAC de 22 de octubre de 1991.

■[93] Artículo 43 del Reglamento del IRPF e Informe de la Dirección General de Tributos de 16 de marzo de 1988.

A efectos del Impuesto sobre Sociedades cuando un mismo contrato realice una prestación de servicios y una cesión de derechos procedente de la propiedad intelectual cuando el sujeto pasivo no sea su autor, será obligatorio practicar la retención sobre el importe total de la contraprestación establecida en el contrato. (artículo 56.2 RIS).

persona física está sometida al régimen de estimación directa, su regulación se remite a lo dispuesto en el Impuesto sobre Sociedades que vamos a estudiar a continuación en el caso de la persona jurídica.

En el caso de estimación objetiva por coeficientes o estimación objetiva por signos, índices o módulos me remito a lo expuesto para los rendimientos de actividad profesional.

3.1.2. IMPUESTO SOBRE EL PATRIMONIO.

A efectos del Impuesto sobre el Patrimonio están exentos los derechos derivados de la propiedad intelectual del autor, mientras permanezcan en su patrimonio y no se utilicen para el comercio. Por tanto, es aplicable la exención del art. 4.3 de la Ley del Impuesto sobre el Patrimonio a la obra propia de los artistas mientras permanezca en el patrimonio de autor, lo que equivale a otorgar a la obra propia del artista el carácter económico financiero de existencias.

Sí se gravarán los derechos derivados de la Propiedad Intelectual cuando pertenezcan a los herederos del autor o a un tercero. En el caso de adquisición onerosa, el artículo 22 de la Ley del Impuesto sobre el Patrimonio establece con carácter general que los derechos adquiridos a terceros deben incluirse por su valor de adquisición.

A efectos del Impuesto sobre el Patrimonio, si el propio autor decide explotar la propiedad intelectual en un contexto empresarial, le serán de aplicación las normas y criterios de valoración de esta categoría de actividad. El artículo 4 de la Ley del Impuesto sobre el Patrimonio establece que los bienes y derechos de las personas físicas necesarios para el desarrollo de su actividad empresarial estarán exentos, siempre que la actividad se ejerza de forma habitual, personal y directa por el sujeto pasivo y que la actividad constituya su principal fuente de renta.

El valor de tales bienes y derechos se determinará conforme a lo establecido en el artículo 11 de la Ley del Impuesto.

3.2. EL DERECHO DE EXPLOTACION:

3.2.1. CONSIDERACIONES GENERALES

La cesión del derecho de uso un programa de ordenador está contemplada en el Texto Refundido del la Ley de Propiedad Intelectual [94] .

Los derechos de explotación los puede ejercitar una persona física o una persona jurídica, pero no se puede confundir la cesión de los derechos de propiedad intelectual sobre un programa de ordenador con la venta de los "productos " derivados de la explotación de los derechos cedidos tales productos se conocen con la denominación de software standard y que puede ser adquirido en propiedad por cualquier persona que lo necesite, y que vamos a estudiar sus consecuencias fiscales en el apartado destinado al usuario.

■[94] Artículo 99 del RDL 1/1996. Contenido de los derechos de explotación."Sin perjuicio de lo dispuesto en el artículo 100 de esta Ley los derechos exclusivos de la explotación de un programa de ordenador por parte de quien sea su titular con arreglo al artículo 97, incluirán el derecho de realizar o de autorizar:

La reproducción total o parcial, incluso para uso personal, de un programa de ordenador, por cualquier medio y bajo cualquier forma, ya fuere permanente o transitoria. Cuando la carga, presentación, ejecución, transmisión o almacenamiento de un programa necesiten tal reproducción deberá disponerse de autorización para ello, que otorgará el titular del derecho.

La traducción, adaptación, arreglo o cualquier otra transformación de un programa de ordenador y la reproducción de los resultados de tales actos, sin perjuicio de los derechos de la persona que transforme el programa de ordenador.

Cualquier forma de distribución pública incluido el alquiler del programa de ordenador original o de sus copias.

A tales efectos, cuando se produzca cesión del derecho de uso de un programa de ordenador, se entenderá, salvo prueba en contrario, que dicha cesión tiene carácter no exclusivo e intransferible, presumiéndose, asimismo, que lo es para satisfacer únicamente las necesidades del usuario. La primera venta en la Unión Europea de una copia de un programa por el titular de los derechos o con su consentimiento, agotará el derecho de distribución de dicha copia, salvo el derecho de controlar el subsiguiente alquiler del programa o de una copia del mismo".

Nos vamos a centrar en el estudio de la persona jurídica en el ejercicio del derecho de explotación, ya que las conclusiones que se extraen son extrapolables a la persona física es estimación directa que ejerce estos mismos derechos.

La persona jurídica puede poseer el derecho de explotación sobre un programa de ordenador tanto si ha desarrollado el programa en el seno de la propia empresa con la intención de enajenarlo, como si lo ha adquirido de forma onerosa a su autor.

Tanto si ejerce el derecho de explotación directamente o cede su explotación a terceros, los rendimientos obtenidos estarán sujetos al Impuesto sobre Sociedades.

En el ámbito del Derecho Fiscal no se contempla aisladamente la transmisión de programas de ordenador, sino que siempre se hace referencia al concepto genérico de transferencia de tecnología, y la contraprestación tiene, en principio la consideración de rendimiento de capital mobiliario en el caso de que el autor sea persona jurídica [95]. El Impuesto sobre Sociedades actualmente vigente y regulado por la Ley 43/95, de 27 de diciembre establece un concepto sintético de renta, con independencia de la fuente, de ahí que en este caso no exista tratamiento diferenciado como rendimiento de capital mobiliario o de la explotación económica como ocurre en el caso de las personas físicas. No obstante, cualquiera otras operaciones que impliquen la transmisión de la propiedad y no la mera cesión de uso, la contraprestación no podrá ser considerada como rendimiento de capital mobiliario.

Los derechos de explotación de una aplicación informática pueden provenir de:

■[95] Artículo 256,1 de derogado Reglamento del Impuesto sobre Sociedades, Real Decreto 2631/1982, de 15 de octubre disponía que tendrá la consideración de rendimientos de capital mobiliario "f) .. Los procedentes del arrendamiento de bienes muebles, de derechos, negocios, minas, películas cinematográficas, de la cesión de la propiedad industrial o intelectual y de las prestaciones de asistencia técnica." Este reglamento fue derogado por la Ley 43/1995, de 27 de diciembre, del nuevo Impuesto sobre Sociedades, si bien es importante tenerlo en cuenta en relación con las resoluciones del TEAC sobre la materia que remiten a esta norma.

1. Generación del programa por la propia empresa [96].

Desde el punto de vista contable, a la empresa que ha desarrollado la aplicación informática se plantea el problema de activar como inmovilizado inmaterial el programa de ordenador o no [97]. En el caso de que se contabilizase como inmovilizado inmaterial, se podrá amortizar con efectos en el Impuesto sobre Sociedades siempre que se demuestre por el sujeto pasivo que la pérdida de valor responde a una depreciación irreversible y continuada [98].

Una de las cuestiones importantes a determinar es si la creación de programas de ordenador por parte de su autor podría tener la consideración de gastos de investigación y desarrollo (I+D). En la resolución del ICAC de 21 de enero de 1992 [99], sobre contabilización del inmovilizado inmaterial se definen lo que son actividades de investigación y desarrollo como la indagación original y planificada que persigue descubrir nuevos conocimientos y superior comprensión en los terrenos científico o técnico, en el caso de la primera, y la aplicación concreta de los logros obtenidos en la investigación hasta que se inicia la producción comercial, en el caso de la actividad de desarrollo.

De tener la consideración de gastos I+D serían importantes las consecuencias, tanto en amortizaciones como en deducciones del Impuesto sobre Sociedades, puesto que existe un tratamiento fiscal favorable a este tipo de resultados. Sin embargo, si aplicamos estas definiciones de I+D a la creación de programas de ordenador, obtenemos dos conclusiones:

1. El desarrollo de un software específico puede conformar una actividad I+D, además de cumplir los requisitos que se exigen para ello, en dos supuestos:

■[96] Lo contenido en este apartado también es aplicable al autor persona física.

■[97] La empresa que genere una aplicación informática podrá activar el nuevo producto mediante la cuenta 73 de trabajos realizados por la empresa para su inmovilizado, mediante la activación de los gastos de personal y demás gastos necesarios invertidos en este trabajo.

■[98] Artículo 11, 5 in fine de la Ley 43/1995, de 27 de diciembre, del Impuesto sobre Sociedades.

■[99] Nos remitimos al comentario sobre esta resolución del ICAC realizada al comienzo del trabajo.

a) La creación de un lenguaje informático nuevo, que resulte como instrumento para desarrollar otros programas informáticos.

b) La generación de un software específico inseparablemente unido a una maquinaria o instalación industrial o científica, es decir, conformar la parte de un todo.

2. La creación de programas informáticos en general, no tiene por qué constituir actividad de investigación y desarrollo.

En conclusión, la clasificación del software como I+D en la mayoría de las veces obedece a razones de índole fiscal y no contable, lo que obligará al sujeto pasivo a probar esta naturaleza en el caso de que sea requerido por la Administración Tributaria para justificar el disfrute de los beneficios fiscales que tienen este tipo de elementos. En cuanto que consideramos que la mayoría de las aplicaciones informáticas no tienen la naturaleza de gastos I+D vamos a seguir nuestro estudio dentro de esta perspectiva, sin perjuicio de aquellas que sí lo sean.

2. Derecho de explotación por adquisición onerosa:

En este caso que nos ocupa, la persona jurídica debe adquirir el derecho de explotación de su autor a título oneroso, si bien la contraprestación se puede hacer efectiva de dos formas:

a) Abonando una remuneración a tanto alzado.

b) Abonando al autor una participación proporcional en los ingresos de su explotación o canon periódico [100]. Esta participación se irá abonando conforme se vaya desarrollando la actividad empresarial.

■ [100] El artículo 112 del Reglamento del Impuesto sobre Sociedades de 1982 define canon como "las cantidades de cualquier clase pagadas por el uso o la concesión del uso de un derecho de autor sobre una obra literaria, artística, informativa o científica, incluidas las películas cinematográficas, de un modelo, plano, fórmula o procedimiento secreto; y por las informaciones relativas a experiencias industriales, comerciales o científicas".

En cualquiera de los dos casos, se adquieren los derechos de explotación sobre dicho programa. El problema que se plantea es que la forma de contraprestación de la transacción determina el traspaso de la titularidad del derecho de explotación desde el autor a la empresa o no:

a) Si se ha abonado una remuneración a tanto alzado la empresa adquiere en este caso un derecho patrimonial que puede reflejar en el activo del balance por su precio o valor de adquisición y amortizarlo contablemente de acuerdo con los principios contables.

b) Si se ha abonado un canon, no se produce cesión de la titularidad por parte del autor, sino una cesión del derecho de explotación. En este caso, hay una correlación entre el gasto de la empresa y el ingreso del titular del derecho de explotación del programa, que conserva la titularidad del mismo. Desde el punto de vista contable y fiscal será gasto en cada ejercicio la retribución devengada en el mismo.

En resumen, la adquisición del derecho de explotación del programa de ordenador implica un régimen fiscal que depende del contrato celebrado. Por tanto, desde el punto de vista del Impuesto sobre Sociedades, se debe distinguir si se cede la titularidad del derecho de explotación y por tanto formará parte del activo empresarial y será amortizable, o bien se transmite a través de un canon, siendo un elemento de la actividad empresarial pero no formará parte de su activo.

3.2.2. ADQUISICION DE LA TITULARIDAD DEL DERECHO DE EXPLOTACION: IMPUESTO SOBRE SOCIEDADES.

3.2.2.1. AMORTIZACION.

Los derechos de explotación de los programas de ordenador tienen un tratamiento especial en la propia Ley de Propiedad Intelectual [101] en relación con la duración de su protección [102]. El artículo 98, párrafo 1 del RD 1/1996 nos remite al

■[101] Artículo 97 de la Ley 22/1987, de 11 de noviembre, de Propiedad Intelectual.

■[102] En el supuesto de que el autor sea una persona física, la protección del derecho de explotación será toda la vida del autor y los sesenta años siguientes:

Capítulo I del Título III para determinar la protección del derecho de explotación de las personas físicas. En el artículo pues se regula en este supuesto en los siguientes términos:

Artículo 26. Duración y cómputo.
Los derechos de explotación de la obra durarán toda la vida del autor y setenta años después de su muerte o declaración de fallecimiento[103].

Artículo 98, párrafo 2, RD 1/1996[104] , por tanto nos encontramos con un elemento del inmovilizado inmaterial limitado en el tiempo, tanto si el contrato de cesión del derecho de explotación es limitado expresamente como si no, puesto que transcurrido ese plazo pasará a formar parte del dominio público.

El inmovilizado inmaterial es el gran favorecido por la reforma del Impuesto sobre Sociedades en materia de amortizaciones ya que se han relajado los requisitos para la deducción de su depreciación, reforma en la que se manifiesta una clara influencia contable. Las consecuencias que se derivan son:

- Se facilita la amortización de los elementos del inmovilizado inmaterial, que como inversión económica de la empresa se encontraba discriminada respecto el inmovilizado material.

- Se igualan, de una forma definitiva, al fondo de comercio, las marcas y derechos de traspaso el resto de los bienes, incluida la propiedad intelectual.

Tradicionalmente [105], se establecían unos requisitos estrictos para admitir la amortización de los elementos del inmovilizado inmaterial:

En el caso de que el autor sea una persona jurídica durará 60 años contados desde el día uno de enero del año siguiente al de la divulgación lícita del programa o al de su creación si no se hubiera divulgado

a) 60 años desde la divulgación de la obra, efectuada dentro de los 60 años siguientes a la muerte del autor.

b) Las obras anónimas o seudónimas tendrán una duración de 60 años desde la divulgación.

■[105] Los apartados 1 y 3 del artículo 65 del RIS de 1982 establecían estos requisitos estrictos para admitir la amortización del los elementos del inmovilizado inmaterial

a) Ser susceptibles de valoración económica.
b) Estar registrados contablemente.
c) Ser adquiridos mediante contraprestación onerosa.
d) Que se deprecien con el paso del tiempo o tengan una duración determinada.

Estos requisitos han sufrido alguna transformación con la nueva norma tributaria:

Los dos primeros desaparecen absorbidos por el artículo 10,3 de la LIS: Se remite directamente a las normas contables de aplicación directa en la determinación de la base imponible del Impuesto sobre Sociedades. En nuestro tema de estudio, la adquisición de la titularidad de los derechos de explotación, están totalmente cubiertos, ya que es requisito su activación como inmovilizado inmaterial.

El requisito de onerosidad está recogido expresamente en el artículo 11, 4 a) y 11, 4. b) de la LIS: Se pondrán de manifiesto en virtud de una adquisición a título oneroso. A este requisito hay que añadir la exigencia de que la entidad adquirente y la transmitente no se encuentren en situaciones de vinculación previstas en el artículo 42 del Código de Comercio. Para poder ser amortizado necesita que medie contraprestación, es decir, que sea objeto de adquisición onerosa. Así, el propio autor del elemento de propiedad intelectual no podrá amortizarlo, salvo que demuestre su depreciación permanente, pero sí si ha sido cedido tal derecho mediante transmisión onerosa a una empresa que se dedique a la distribución y explotación del mismo, en cuanto que tal empresa tiene limitada su exclusividad en la utilización de la obra al tiempo que marca el acuerdo o en su defecto, el límite que marca la ley.

Por último, hemos estado resaltando la necesidad de una adquisición onerosa, pero debemos hacer hincapié en que no toda transmisión onerosa es admitida sino que es necesaria el establecimiento de un tanto alzado, de forma que cualquier otra forma de cesión o alquiler no tendrá la consideración de amortizable [106]. El último requisito también se cumple en nuestro objeto de estudio, ya que el ejercicio exclusivo del derecho de explotación será como máximo de 60 años. Este requisito pretende dar cumplimiento a la causa de depreciación por paso del tiempo. Sin embargo, pueden concurrir otras razones, principalmente la obsolescencia, que dan lugar a depreciación irreversible y anticipada.

■ [106] Dirección General de Tributos. Resolución de 9 de marzo de 1993.

Hay que insistir que aquí no se está amortizando la aplicación informática propiamente dicha, sino su derecho de explotación comercial, un derecho de Propiedad Intelectual.

En el caso del inmovilizado inmaterial Propiedad Intelectual, en cuanto que no son susceptibles de aplicación de los métodos de amortización fiscales al carecer de CMA y PMA establecido en las tablas [107], la vida útil será *"el período durante el cual se espera que, razonadamente, produzca ingresos"*. Este período de vida útil tiene un límite mínimo de diez años que viene dado por la propia norma de amortización con carácter imperativo y no establece un límite máximo que podrá ser determinado libremente por el sujeto pasivo. En el caso que nos ocupa, los derechos de explotación, sí que existe un límite máximo, los 60 años que marca la ley de propiedad intelectual.

En conclusión, el derecho de explotación es un derecho derivado de la propiedad intelectual de las aplicaciones informáticas, y como tal es amortizable conforme el sistema propio de los elementos del inmovilizado inmaterial, si bien es un elemento distinto, y no le son aplicables los coeficientes previstos para ellos, de los sistemas y programas informáticos recogidos en las tablas de amortización cuya naturaleza vamos a definir a continuación.

3.2.2.2. PROVISION POR DEPRECIACION DE EXISTENCIAS.

Una de las novedades de la Ley del Impuesto sobre Sociedades de 1995 es la provisión por depreciación de existencias de fondos editoriales, fonográficos, audiovisuales y similares. Se trata de una especialidad dentro de la depreciación de existencias y son exclusivamente las empresas productoras, no las empresas distribuidoras, las que tienen derecho a aplicar este gasto fiscalmente deducible.

Respecto a la aplicación de esta provisión hay que hacer dos consideraciones:

1. Aunque no se incluyen expresamente a los fondos informáticos, dado su carácter análogo con los fondos editoriales se pueden incluir en esta modalidad de provisión.

■ [107] Ver mas adelante el comentario sobre las nuevas tablas de amortización.

2. Esta provisión se refiere a los fondos de la emp
soportes del producto, no al derecho de explotación del mismo, que forma parte de su inmovilizado.

Esta provisión consiste en una presunción legal de depreciación transcurridos dos años desde la puesta en el mercado de las producciones o antes si se prueba la depreciación por parte del sujeto pasivo.

3.3. EL USUARIO

El usuario es el destinatario de los programas de ordenador, el consumidor final, y a quién va dirigida toda la actividad comercial de las aplicaciones informáticas, desde la producción a la comercialización, y para él no tiene repercusión quién ejerce el derecho de explotación del programa, sino de qué modalidad de programa informático se trata. Aquí el objeto de cambio es el programa en sí, no su derecho de explotación como hemos analizado en el apartado anterior, aunque como veremos se da una licencia de uso de este programa.

Desde el punto de vista mercantil, el software tiene la consideración de un producto que se vende de forma standard incorporado a un soporte físico; concretamente la CEE lo califica, cuando se adquiere y se introduce en otro país, como una incorporación de mercancías, en cuyo caso el precio que se pague no tendrá la consideración de canon o royalty. El software standard se puede definir como la adquisición del derecho de uso de los programas de ordenador para su utilización por una generalidad de usuarios que pretenden resolver programas comunes que satisfacen una cantidad única y por una sola vez, pero que el cesionario se reserva todos sus derechos dominicales. Se da al adquirente del programa de ordenador el uso no exclusivo del mismo, sino una licencia de uso.

En nuestro sistema tributario, la distribución de productos informáticos está definida en el IVA. El artículo 8 en su párrafo 2, 7° de la Ley del IVA, Ley 37/1992, establece que se considerarán productos informáticos normalizados los que de esta naturaleza se hayan producido en serie, de forma que puedan ser utilizados indistintamente por cualquier consumidor final. Se considerarán entrega de bienes, el suministro de productos informáticos normalizados, comprensivos del soporte u los programas o informaciones incorporados al mismo.

Las entregas de bienes se definen como la transmisión del poder de disposición sobre bienes corporales, pero también se consideran entregas de bienes

otras operaciones en las que no se produce la transmisión del poder de disposición, pero que tienen efectos económicos equiparables, entre otras el suministro de productos informáticos normalizados.

Junto con los programas standard, existen programas concretos realizados especialmente para un determinado usuario, supuesto que se suele articular, la mayoría de las veces, mediante una cesión de uso, y consiguientemente, los pagos que se efectúen tendrán la consideración de cánones.

El artículo 11 en su párrafo 2, 16° de la Ley del IVA establece: Se considerarán prestaciones de servicios el suministro de programas informáticos específicos, considerándose accesoria a la prestación del servicio la entrega del correspondiente soporte. Se considerarán productos informáticos específicos los de esta naturaleza que hayan sido producidos previo encargo del cliente.

Se considera accesoria a la prestación del servicio la entrega del correspondiente soporte.

En conclusión, la licencia de uso de un programa forma parte del inmovilizado inmaterial de la empresa cuando es un gasto plurianual, aunque puede ocurrir que su utilización no supere un año puesto que están preparados para realizar una labor que prescribe, piense en los programas para el cálculo del IRPF, en cuyo caso tendrán la consideración de gasto del ejercicio. Otra posibilidad es disfrutar del uso del programa a través del pago de un canon periódico. En este caso, en cuanto que se trata de un alquiler o prestación de servicios, tendrá la consideración de gastos.

El tratamiento de los derechos de uso de los programas de ordenador está claramente explicado por el Ministerio de Economía y Hacienda en contestación a consultas planteadas por el contribuyente:

" Cuando los adquirientes de los derechos de uso de los programas abonan una remuneración a tanto alzado al autor, adquieren un elemento patrimonial intangible (inmovilizado inmaterial), que pueden reflejar en el activo de su balance por su precio o valor de adquisición y amortizarlo cuando sufra una depreciación continuada o se adquiera por un tiempo limitado, sin posibilidad de prórrogas sucesivas, siempre que se produzca una depreciación efectiva y se halle contabilizada." [108]

■[108] Normativa: Artículo 65 Reglamento del Impuesto sobre Sociedades y Resolución de 9 de marzo de 1990 de la Dirección General de Tributos.

Por una parte, se refiere a la distinta forma de adquisición según tanto alzado o por canon de la que ya hemos tratado.

En segundo lugar, hace referencia directa a su amortización en el supuesto de que se haya activado como inmovilizado inmaterial en el balance de la empresa. Este último aspecto, la amortización, ha sido objeto de importantes novedades en 1997.

El RD 537/97, de 14 de abril en el que se aprueba el Reglamento del Impuesto sobre Sociedades, recoge a su vez unas nuevas tablas de amortización. Uno se los aspectos mas destacados de esta reforma de las tablas de amortización es el nuevo elemento introducido, los sistemas y programas informáticos. Este elemento se ha situado dentro de los Elementos Comunes, el apartado 7 y se le ha dotado de un CMA de 33% y un PMA de 6 años.

La importancia de esta novedad se extrae de las siguientes conclusiones:

1. Se recogen por primera vez en las Tablas de amortización un elemento del inmovilizado inmaterial. Los elementos allí contemplados no son propiedad intelectual de la empresa, son una herramienta de trabajo, como una mesa o una máquina de escribir, pero pertenecen al inmovilizado inmaterial, consecuencia de su carácter intangible.

2. Se exceptúan estos elementos, como consecuencia de punto anterior, de su aplicación del sistema especial destinado para los elementos del inmovilizado inmaterial (artículos 11, 4 y 5 LIS).

3. Le será de aplicación cualquiera de los sistemas de amortización, con excepción del sistema de bienes usados, que exigen expresamente que se trate de elementos del inmovilizado material.

En conclusión, la inclusión de los sistemas y programas informáticos en las tablas del RD 537/97, establece una tratamiento distinto a estos elementos respecto de los demás que conforman el inmovilizado inmaterial, del que podemos establecer dos situaciones diferenciadas:

- Si se cede el derecho de uso de programa, adquiriéndolo mediante contraprestación por tiempo limitado e inferior al período mínimo establecido en las tablas de amortización, es decir, mas de uno u menos de tres años, podrá amortizarlo

fiscalmente en ese plazo, si bien la carga de la prueba recaerá en el sujeto pasivo, pero en este caso será fácil de probar.

- Si el derecho de uso es por tiempo ilimitado, se aplicarán los coeficientes recogidos en tablas de amortización de acuerdo con el sistema de amortización elegido.

Para finalizar, unas notas sobre la prestación de asistencia técnica al usuario. La adquisición por parte del usuario de programas de ordenador puede hacerse tanto a empresas residentes en territorio español como a empresas no residentes. En el supuesto de empresas residentes no se plantea ningún problema, tanto en el caso de adquisición del programa como de la asistencia técnica que se deriva de él. Sin embargo, en el mundo de la informática es frecuente la transferencia de tecnología y por tanto las transmisiones entre países distintos. La naturaleza de la entrega del bien como importación, en cuanto que procede de una empresa no residente no presenta la menor duda. Sin embargo, la adquisición de estos programas puede llevar aparejado un derecho de asistencia técnica de ayuda al programador y al usuario que plantea, respecto de la empresa que presta el servicio, la duda de si son rendimientos obtenidos en territorio español o no. La Dirección General de Tributos resuelve este problema en la consulta vinculante de 22 de mayo de 1984 en la que se pronuncia en los siguientes términos: *"La importación del (...) conteniendo los lenguajes de programación, los sistemas operativos y las utilidades de ayuda al programador supone la realización de una operación de importación que incorpora en razón de su propio contenido un aspecto importante de asistencia técnica, cuya retribución debe ser considerada como un rendimiento obtenido en España y, como tal, sujeto al IS, siendo sujeto pasivo del mismo la entidad vendedora no residente* [109]*"*.

4. CONCLUSIONES

Bajo la denominación de sistemas y aplicaciones informáticas o programa de ordenador se reúnen distintos sujetos pasivos cuya imposición directa es distinta dependiendo de su relación con el producto, de forma que debemos distinguir entre el autor, el derecho de explotación y el usuario del programa de ordenador.

■[109] Sobre este aspecto y en los mismos términos se pronuncian las Resoluciones del TEAC de 25 de septiembre de 1991 y de 22 de octubre de 1991.

El autor y el derecho de explotación, como derechos derivados de la Ley de Propiedad Intelectual están bajo la protección de ésta, y tienen la consideración de elementos del inmovilizado inmaterial, cuyas consecuencias tributarias se derivan de esta consideración pero con las particularidades que encierran las aplicaciones informáticas.

El caso del usuario es distinto ya que la aplicación informática se sustantiviza, y aunque continúa bajo la protección de la Propiedad Intelectual, a efectos tributarios tiene un tratamiento distinto.

Una vez que se define la naturaleza tributaria de cada uno de los rendimientos que genera la aplicación informática, tanto para el autor, el derecho de explotación y el usuario, su imposición dependerá de la forma en que se obtengan los rendimientos, ya sea a través de un canon o de una retribución a tanto alzado.

En conclusión, la dificultad que encierra el tema de los programa de ordenador comienza en su clasificación como rendimiento, y una vez determinado este aspecto, en aplicar las obligaciones contables, de amortización, provisión y demás gastos deducibles especificados para este tipo de bienes.

ADENDA

La imposición sobre la renta procedente de actividades empresariales y profesionales de las personas físicas ha sufrido una importante modificación para este año 1998. Aunque las novedades introducidas no afectan directamente a las consideraciones y conclusiones presentadas en este trabajo sobre la imposición directa de los programas de ordenador, considero necesario hacer una referencia escueta a la nueva situación tributaria de los sujetos pasivos personas físicas empresarios y profesionales.

Como hemos expuesto en este trabajo, la imposición de actividades empresariales y profesionales personas físicas hasta el 31 de diciembre de 1997 se concretaba en los siguientes sistemas de determinación de la Base Imponible: Estimación directa y Estimación Objetiva, esta última con dos modalidades:

Estimación objetiva por coeficientes y estimación objetiva por índices, signos o módulos.

Por tanto, para los ejercicios comenzados a partir del 1 de enero de 1998 desaparece la estimación objetiva por coeficientes.

La estimación objetiva por índices, signos o módulos se mantiene con idéntica configuración y aunque está prevista legalmente su aplicación a los rendimientos de profesionales, no aparece en los nuevos módulos aprobados por la OM de 13 de febrero de 1998 ninguno que se refiera a la materia que nos ocupa.

Respecto de la estimación directa, la modalidad normal coincide con la conceptuación de la regulación anterior, y su remisión a las normas del Impuesto sobre Sociedades.

La mayor novedad de esta nueva regulación se centra en la estimación directa simplificada. Su cálculo se realiza aplicando los artículos 41 y 42 de la Ley 18/1991, de 6 de junio, es decir, ingresos menos gastos necesarios para el desarrollo de la actividad. El conjunto de provisiones deducibles y los gastos de difícil cuantificación se calcularán aplicando el 5% sobre el rendimiento neto. Las modificaciones sobre amortizaciones no afectan al inmovilizado inmaterial.

Con estas notas presento el nuevo esquema de cálculo de los rendimientos empresariales y profesionales y mantengo las consideraciones presentadas en este trabajo.

Notas acerca del Régimen Jurídico de los Ficheros de Datos Personales de Titularidad Universitaria

GUILLERMO OROZCO PARDO

Profesor Titular del Departamento de Derecho Civil. Universidad de Granada

I.- PLANTEAMIENTO DEL TEMA.

I.1- Introducción y antecedentes:

Estas breves líneas pretenden iniciar al lector en el conocimiento de una temática nueva que ya está generando problemas en la gestión de los diversos órganos universitarios y que, en tiempos venideros, puede generar una diversidad de cuestiones de mayor enjundia. En efecto, el volumen de información que hoy se genera y procesa en los diversos ámbitos del quehacer universitario ha tenido como primera consecuencia la necesidad de aplicar los medios informáticos a la recogida, almacenamiento, proceso y transmisión de información y, dentro de esta, la más importante está referida a los datos personales de diverso orden que las universidades poseen relativos a sus trabajadores, alumnos y terceros que con ellas entran en relación.

Esta dinámica ha ido generando la aparición de ficheros automatizados que sirven para el tratamiento de esos datos personales y que han de estar necesariamente sometidos al régimen jurídico general establecido por el Ordenamiento jurídico para regular tales cuestiones. Dichas normas pretenden, como objetivo básico, asegurar que estos tratamientos y cesiones no vulneren en ningún caso los derechos y libertades de las personas concernidas. Los ficheros universitarios están encuadrados dentro de lo que las leyes denominan "ficheros de titularidad pública" merced a la naturaleza jurídica de sus titulares y los fines a que están afectos.

En consecuencia, como antes dijimos, estos ficheros se encuentran sometidos a un régimen jurídico que, "prima facie", puede parecer dispar pero

que, una vez aclarado, conforma un panorama nítido en su composición, aunque cambiante en un futuro próximo merced a la adaptación de una Directiva comunitaria y a una "previsible" sentencia de nuestro Tribunal Constitucional. Nuestra intención no es "agotar" el tema sino llamar la atención sobre esta temática y tratar de aventurar posibles soluciones a cuestiones ya suscitadas y promover posturas coordinadas en las distintas universidades españolas a la hora de abordar la problemática que, a buen seguro, se nos va a plantear.

I.2- Derecho e Informática:

El tema que abordamos se inserta en un contexto más amplio integrado por la multitud de consecuencias socio-jurídicas que las nuevas tecnologías están planteando al Derecho. La aplicación de los medios automatizados de recogida, tratamiento y transmisión de la información referida a las personas ha supuesto un "salto cualitativo" más importante que los que puedan suponer la imprenta o la televisión. La informática es la técnica de tratamiento y transmisión automatizada de información y supone la base de la llamada "sociedad de la información", y sus implicaciones socioeconómicas son de muy diverso orden: banca, gestión de empresa, correo, policía, seguridad, bolsa, son algunos de los sectores en los que este avance tecnológico se ha vuelto imprescindible. Incluso estamos ya ante la llamada "informática decisional" que muchas veces prepara, condiciona o adopta decisiones que afectan al ciudadano de forma relevante; además la informática sirve para obtener una información nueva, y más sensible, sobre la base de datos precedentes merced a su capacidad de relacionarlos entre sí, tal y como reconoce nuestro Legislador al afirmar que hoy las fronteras del tiempo y el espacio han "caído" por obra de la transmisión automatizada, y casi instantánea, de la información dentro de la "aldea global". A causa de lo anterior la informática permite acceder al conocimiento de una persona, de datos o perfiles concretos, en unos parámetros que ni él mismo puede sospechar, llegándose a un precipitado que podríamos denominar "personalidad informática".

Lógicamente, los medios informáticos se han vuelto hoy unos decisivos instrumentos de poder a los que el Derecho debe imponer unas normas de ética jurídica para impedir abusos: Es por ello que nuestra Constitución de 1978 habla en su artículo 18.4 de que la Ley "... limitará el uso de la informática..." en defensa de los derechos y libertades de los ciudadanos. Con ello pretende evitar que un avance decisivo y positivo pueda convertirse, por mor de un mal uso, en un instrumento de dominación al servicio de intereses antisociales.

I.3- La necesidad de una Ley general a desarrollar:

De todo lo anterior se deduce paladinamente que nuestro Legislador constituyente consideró necesario encauzar la aplicación de esta tecnología a través de unos parámetros de ética jurídica acorde con los principios y valores de un Estado democrático y social de Derecho. Como quiera que el artículo 18.4 CE se encuadra dentro del Capítulo 2º del Título I, relativo a los derechos fundamentales, no cabe la menor duda de la importancia que este precepto, y sus normas derivadas, posee dentro del contexto de nuestro Ordenamiento jurídico. Principios como la seguridad jurídica, la igualdad, el respeto a los derechos y libertades fundamentales, la responsabilidad o la interdicción de la arbitrariedad están consagrados en el artículo 9.3 CE y obligan de manera directa e inmediata a los ciudadanos y a los poderes públicos, dentro de los cuales se integran las Universidades. Todo ello se ha de proyectar en una Universidad que se integra en un marco del Estado, entendido como una "organización democrática de servicios", para proveer uno de los más esenciales: la enseñanza superior.

Por tanto, y como luego veremos, el precepto constitucional que sirve para dotar de una sólida base a todo el conjunto normativo aplicable a la materia es el 18.4 CE, que nos sirve además de criterio interpretativo y de instrumento integrador de las lagunas u obscuridades que pudieran surgir, tal y como ha afirmado nuestro Tribunal Constitucional. Con ello queremos desechar de salida visiones más o menos "administrativizadas" desde la perspectiva del artículo 105-b CE relativo al acceso a los archivos y registros administrativos, pues no hay una "vía paralela" sino que este mismo precepto ya se somete "per se" a los dictados antes citados cuando limita ese acceso mediante garantías en favor de la seguridad, la defensa, la averiguación de los delitos y "... la intimidad de las personas ...".

Por tanto, al margen de textos como el Convenio 108 de Consejo de Europa, el Acuerdo de Schenguen o la Directiva 95/46 cuya transposición obligará modificar la legislación española, podemos afirmar que en esta materia debemos partir de los dictados del artículo 18.4 CE y normas desarrolladoras.

I.4- Cuadro normativo:

Inicialmente, al aprobarse la Constitución de 1978, nuestro país no contaba con una norma legal "ad hoc" que regulara esta materia. Tan solo podíamos partir de los preceptos antes citados:

18.4 CE: "La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos ".

105 CE: " La ley regulará:

b) El acceso de los ciudadanos a los archivos y registros administrativos, salvo en lo que afecte a la seguridad y defensa del Estado, la averiguación de los delitos y la intimidad de las personas".

El problema básico que es que no existía una norma de rango adecuado que desarrollara el artículo 18.4, verdadera piedra angular del sistema. No obstante, la Ley Orgánica 1/82 de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen, establecía en su Disposición Transitoria 1ª que, en tanto no se promulgara la normativa prevista en el artículo 18.4 CE, las intromisiones contra tales derechos, provenientes de la utilización de la informática, se regularía por lo previsto en ella.

Pero esta norma era a todas luces insuficiente para resolver la variada problemática que este tema estaba ya suscitando y ello no escapa a la percepción del legislador. Prueba de ello son las diversas iniciativas parlamentarias que se siguieron desde 1979 hasta 1992, año en que se aprobó una ley específica desarrolladora del precepto constitucional de referencia. Esta laguna de nuestro Ordenamiento fue parcialmente paliada, parece que como imposición para aplicar el Tratado de Schenguen, mediante la firma por España del Convenio 108 del Consejo de Europa, Convenio de Estrasburgo para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, cuyo instrumento de ratificación es de 27 de enero de 1984. (BOE 15/11/85) La aplicación directa, o siquiera como norma interpretativa, suscitó una interesante problemática resuelta por el Tribunal Constitucional en la sentencia del llamado "caso Olaverri" (STC 254/1993) que puso de manifiesto la insuficiencia de los instrumentos legales que había a la sazón en nuestro país para afrontar el problema, si bien sirvió para que nuestro Alto Tribunal sentara doctrina sobre otras cuestiones interesantes a efectos prácticos y científicos.

Partiendo de la base de que para desarrollar un precepto constitucional relativo a derechos fundamentales debe optarse por la vía de la ley Orgánica y que tal norma ha de colocarse en lugar preferente dentro de ese "edifico normativo",

podemos citar como normas específicas para la regulación de la materia, en lo que a nuestro propósito interesa:

- El Convenio 108 del Consejo de Europa, de 28 de enero de 1981.

- La Directiva 95/46 del Parlamento Europeo, de 24 de octubre de 1995, cuyo plazo para ser adaptada termina en 1998.

- El artículo 18.4 CE.

- La Ley Orgánica 5/92 de 29 de octubre de Regulación del Tratamiento Automatizado de los Datos de carácter personal.(v. gr. LORTAD)

- R.D. 1332/1994 de 20 de Junio, que desarrolla determinados preceptos de la anterior.

- L.O. 10/1995, de 23 de noviembre, del Código Penal.

- En desarrollo del artículo 105.b CE cabe destacar la Ley 30/92 de 26 de noviembre de Régimen Jurídico de las Administraciones Públicas y Procedimiento Administrativo Común.

Obviamente existen otras normas complementarias pero a los efectos del presente estudio no poseen relevancia como para integrarlas en este cuadro.

Al margen de otras consideraciones relativas a las norma procedentes de Organismos supranacionales, debemos tener muy presente que las leyes se relacionan entre sí por los principios de jerarquía normativa y especialidad de materia. Es por ello que no cabe la menor duda de que la LORTAD se convierte en la pieza clave de este sistema y es a partir de ella como debemos aplicar el resto de los preceptos citados.

II.- CUESTIONES GENERALES.

II.1- Conceptos previos:

Vamos a recoger aquí aquellas definiciones legales referidas a los conceptos más esenciales que se manejan en esta temática, utilizando preferentemente los recogidos en el artículo 3 de la LORTAD y normas de desarrollo:

- Fichero automatizado: todo conjunto organizado de datos de carácter personal que sean objeto de un tratamiento, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización o acceso.

- Tratamiento de datos: operaciones y procedimientos técnicos, de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias.

- Cesión de datos: toda obtención de datos resultante de la consulta de un fichero, la publicación de los datos contenidos en el fichero, su interconexión con otros ficheros y la comunicación de datos realizada por una persona distinta de la afectada.

- Procedimiento de disociación: todo tratamiento de datos personales de modo que la información que se obtenga no pueda asociarse a persona determinada o determinable.

- Transferencia de datos: el transporte de datos entre sistemas informáticos por cualquier medio de transmisión, así como el transporte de soportes de datos por correo o por cualquier otro medio convencional.

- Bloqueo de datos: la identificación y reserva de datos con el fin de impedir su tratamiento.

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

- Encargado del tratamiento: introducido por la Directiva es la 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.

Como puede observarse, la Ley no incluye entre sus definiciones al "Titular del fichero", y ello porque opta por hacer hincapié en la responsabilidad por la gestión del mismo, antes que por la relación de pertenencia o titularidad. Ello ha provocado cierta polémica doctrinal en cuanto vincula directamente al titular/responsable del fichero con las consecuencias que de un incumplimiento de las normas se pudieran deducir.[110] Para resolver la cuestión la Directiva incorpora al "Encargado de tratamiento" como figura intermedia e instrumental que realiza el tratamiento, por cuenta del anterior, y de cuya actuación responde el titular del fichero, según las normas comunes de responsabilidad civil.

II.2- Especial referencia a los datos personales:

Digamos de salida que la Ley no ampara a las personas jurídicas, aunque al Proyecto si se les aplicaban los beneficios de la misma, pues se circunscribe a las personas físicas. En consecuencia, todas la definiciones que se refieren a la persona concernida titular de los datos objeto de tratamiento se refieren a ámbitos de la vida de tales sujetos.

- Afectado: persona física titular de los datos que sean objeto del tratamiento.

- Consentimiento del interesado: toda manifestación de voluntad libre, específica e informada, mediante la que el interesado consienta el tratamiento de datos que le conciernen.

- Identificación del afectado: cualquier elemento que permita determinar directa o indirectamente la identidad física, fisiológica, psíquica, económica, cultural o social de la persona física afectada.

- Datos de carácter personal: cualquier información concerniente a personas físicas identificadas o identificables.

■ 110 No obstante la propia Ley habla de ficheros de titularidad pública o privada, con lo cual da a entender que acepta la distinción entre la persona, organismo o autoridad pública a cuyo nombre ha de figurar el fichero en el Registro y el responsable.

Esta información puede estar referida a las más diversas esferas de la vida de las personas físicas, razón por la cual la propia Ley considera que el concepto de intimidad no es suficiente para dotar de contenido a tan amplia definición, razón por la cual opta por más amplio de privacidad. Tal y como lo recoge el RD 1332/94 puede ser toda información "numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo, susceptible de recogida, registro, tratamiento o transmisión concerniente a una persona física identificada o identificable".

La Directiva alude al interesado como titular de esos datos personales que permiten su identificación: números de identificación o uno o varios elementos específicos, característicos de su identidad física, fisiológica, psíquica, económica, cultural o social".

Por tanto, los más diversos ámbitos de la vida de las personas pueden ser objeto de protección de esta Ley en la medida en que no se circunscribe a ese "núcleo central" de su actividad personal que él mismo trata de preservar del conocimiento de los demás ("intimidad"), sino que se construye sobre el concepto de privacidad a la que la propia LORTAD entiende como "... un conjunto más amplio, más global, de facetas de su personalidad que, aisladamente consideradas, pueden carecer de significación intrínseca pero que, coherentemente enlazadas entre sí, arrojan como precipitado un retrato de la personalidad del individuo que éste tiene derecho a mantener reservado".

Cobra especial relevancia el hecho de que los datos puedan servir para identificar cualquiera de las facetas de personalidad del afectado, por lo que aquellos datos disociados que no pueden ponerse en conexión con los sujetos quedan fuera del ámbito de la Ley: por ejemplo datos estadísticos o de investigación. Ahora bien, tales elementos característicos de la personalidad del sujeto pueden ser más o menos "sensibles" según la esfera o faceta a que estén referidos. Es por lo que se establece un régimen legal más o menos estricto a la hora de autorizar el tratamiento de los datos según su naturaleza. Existen unos "datos especialmente protegidos" o "datos sensibles" sobre los que pesa una prohibición de tratamiento, salvo autorización legal o consentimiento del afectado: datos relativos a ideología, religión o creencias, vida sexual, origen racial o salud.

El régimen jurídico de tales datos especialmente protegidos se establece en el artículo 7 de la Ley a cuyo tenor podemos distinguir:

A - Datos sobre ideología, religión o creencias. Están tutelados por el artículo 16 CE y no se puede obligar a declarar sobre ello a ninguna persona y, por lo tanto, no cabe almacenarlos salvo que el afectado consienta expresamente por escrito, siendo revocable este consentimiento.

B - Datos sobre origen racial, salud o vida sexual. Sólo pueden recogerse cuando así lo dispone una ley, por razones de interés general, o lo consienta el afectado expresamente por escrito u otra forma susceptible de prueba.

Sólo se admiten la excepciones al consentimiento previstas para las Fuerzas de Seguridad. No se admiten ficheros cuya única finalidad sea almacenar datos especialmente protegidos.

Incluso se habla de datos "supersensibles" que son aquellos obtenidos de un tratamiento sobre datos previos de los que puede ser ignorante el propio afectado: resultado de un test, etc... No obstante, no debemos "obsesionarnos" con la sensibilidad del dato pues, como dice la teoría del "mosaico", un dato aparentemente irrelevante "ab initio" puede volverse enormemente significativo y revelador una vez puesto en relación con su contexto, al igual que la tesela que completa el mosaico o la pieza que completa u orienta al autor de un "puzzle".

De otro lado, existen otros datos que por su propia naturaleza o por la actuación del sujeto afectado, están a disposición del conocimiento de los demás son los llamados Datos accesibles al público definidos como "los que se encuentran a disposición del público en general, no impedida por cualquier norma imitativa, y están recogidos en medios tales como censos, anuarios, bases de datos públicas, repertorios de jurisprudencia, archivos de prensa, repertorios telefónicos o 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 su pertenencia al grupo" (Cfr. RD 1332/94 art. 1.3) Por tanto, son datos de esta naturaleza los repertorios telefónicos o las relaciones de cargos y unidades que las universidades publican; no lo son, sin embargo, las listas de calificaciones académicas del alumnado, toda vez que su publicación sustituye a la "papeleta" o carta de calificación de la nota, pero no es un instrumento de publicidad para terceros que les permita recoger y tratar esas calificaciones, que son datos personales protegidos por la Ley.

Teniendo presente el amplio y global concepto que la Ley contiene de lo que es un "dato personal" es ya indudable que nuestros ficheros universitarios están plagados de ellos y que estos afectan incluso a terceros como padres, cónyuges, hijos y demás personas relacionadas con los trabajadores, el alumnado y los servicios prestados por o a la Universidad.

III.- ANALISIS DE LA LORTAD.

III. 1- El régimen establecido por la LORTAD:

La LORTAD contiene unas disposiciones generales que se aplican a todo tipo de ficheros y luego unos preceptos específicos para los ficheros públicos y los privados. La estructura podría sintetizarse de la siguiente manera:

- Título 1º: Disposiciones generales, arts. 1 a 3.

- Título 2º: Principios de protección de datos, arts. 4 a 11

- Título 3º: Derechos de las personas, arts. 12 a 17.

- Título 4º: Disposiciones sectoriales, este título recoge preceptos específicos para los ficheros de titularidad pública o privada, si bien la Directiva parece imponer la necesidad de regularlos de forma unitaria. Se subdivide en:

- Capítulo 1º: Ficheros de titularidad pública, arts 18 a 22, donde se contienen una serie de excepciones a los principios y derechos de la parte general que han sido muy criticadas e incluso fueron objeto de recurso de inconstitucionalidad.

- Capítulo 2º: Ficheros de titularidad privada, arts 23 a 31, que regulan materias específicas de ficheros de personas, empresas o entidades privadas, pero que no se benefician de las excepciones antes comentadas.

Lógicamente, los ficheros de los que son titulares las Universidades están regulados en el capítulo primero ántes comentado, aunque las excepciones más polémicas no se les aplican en ningún caso.

- Título 5º: Movimiento internacional de datos, arts. 32 y 33.

- Título 6º: Agencia de Protección de Datos: arts 34 a 41, donde se regula la estructura esencial de la llamada "Autoridad de control", y otras cuestiones como la competencia de las Comunidades Autónomas en esta materia. El Estatuto de la Agencia de Protección de Datos fue desarrollado por el RD 428/93 de 26 de Marzo. Este es el órgano que vela por el cumplimiento de la Ley, emite las autorizaciones precisas, dicta las instrucciones adecuadas, atiende las peticiones y reclamaciones, proporciona información sobre la materia, ordena el cese de los tratamientos y ejerce la potestad sancionadora prevista en la Ley.

- Título 7º: Infracciones y sanciones, arts 42 a 48, en ellos la Ley establece un catálogo de infracciones leves, graves o muy graves y las sanciones correspondientes. Este título debe se puesto en conexión con otros textos legales como el Código Penal y las normas que regulan el régimen disciplinario de las Administraciones Públicas y su responsabilidad.

En definitiva, la LORTAD se presenta como la "piedra angular" del sistema merced a su carácter de norma especial sobre la materia y su jerarquía orgánica, si bien debe ser puesta en conexión con otras normas del Ordenamiento que regulan cuestiones conectadas con sus preceptos. Así mismo, la Ley no entra a regular materias que son objeto de otras leyes especiales: régimen electoral, materias clasificadas, Registro civil, Registro de penados y rebeldes, personal militar o función estadística pública.

III.2- Excepciones a la aplicación de la LORTAD:

Esta norma pretende regular sólo aquellos ficheros que no están recogidos en otras leyes especiales en razón de su materia o dependencia orgánica. Se excluyen de la misma:

- Ficheros públicos cuyo objeto establecido por ley es almacenar datos para publicidad con carácter general: Registro Civil, Mercantil o de la Propiedad.

- Ficheros cuyo titular es persona física y tienen una finalidad exclusivamente personal.

- Ficheros de información técnica o comercial que reproducen datos accesibles al público aparecidos en boletines, repertorios, etc...

- Ficheros integrados por bases de datos de resoluciones jurídicas de carácter legal o jurisprudencial.

- Ficheros de datos de miembros, ex miembros de partidos, sindicatos, confesiones, iglesias, etc... No obstante, en estos ficheros se exige el consentimiento del afectado para la cesión de datos y se aplica la Ley a los datos especialmente protegidos.

III.3- Principios/deberes relativos a los datos:

Están referidos a los datos y los tratamientos de los que pueden ser objeto, funcionan como "condiciones para la licitud del tratamiento" al decir de la Directiva. Como tales principios constituyen mandatos que imponen deberes de conducta para los titulares y responsables de los ficheros y el tratamiento, quienes tienen que garantizar el cumplimiento de los mismos por todo el personal.

Podríamos sintetizarlos de la siguiente manera:

1- Se prohibe su recogida por medios fraudulentos, desleales o ilícitos. Por tanto, se han de recoger con fines determinados, explícitos y legítimos por lo que no se les puede tratar después de manera incompatible con aquellos fines, salvo que sean razones históricas, estadísticas o científicas.

2- Deben ser exactos y actualizados, de lo contrario han de cancelarse o rectificarse de oficio o a petición del interesado.

3- No pueden usarse para finalidades distintas a aquellas para las que se recogieron, con las precisiones antes comentadas.

4- Serán cancelados cuando dejen de ser necesarios, por lo que no deben ser conservados una vez que han dejado de ser útiles para la función prevista. De ello se exceptúa su mantenimiento por razones históricas, estadísticas o científicas o cuando existen normas legales que prevean otra cosa: fiscales, seguros, etc... En estos casos deben someterse al proceso de disociación cuando ello sea oportuno.

5- Se han de almacenar de forma que permitan el ejercicio del derecho de acceso a los afectados.

6- Han de ser adecuados, pertinentes y no excesivos en relación con los fines para los que se han recabado.

Otros deberes que han de observar los responsables de los ficheros son:

1- Inscribir debidamente los ficheros en el Registro a través de la Resolución correspondiente.

2- Adoptar las medidas necesarias para garantizar la seguridad de los datos evitando su alteración, pérdida o el acceso no autorizado. A tal efecto, el Mº de Justicia debe elaborar un reglamento que establezca las condiciones técnicas de seguridad en relación con los centros de tratamiento, locales, equipos, sistemas y programas. No obstante, la ausencia de esta norma no empece que los responsables de los ficheros adopten las medidas necesarias para asegurar el cumplimiento de estos deberes, pues esta laguna legal no les exime de responsabilidad. A título indicativo el artículo 9 de la LORTAD le impone el deber de adoptar las medidas técnicas y organizativas necesarias que garanticen la seguridad de los datos y eviten los perjuicios antes previstos, para lo cual han de tenerse en cuenta el estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural.

3- El deber de secreto que afecta a todas las personas relacionadas con el tratamiento y los ficheros, incluso con posterioridad a que concluya su relación con el titular o responsable del fichero.

Queda patente el elevado nivel de responsabilidad que se impone a los titulares y responsables de los ficheros que, en muchas ocasiones, no se corresponde con los medios técnicos de control de los que disponen para verificar el cumplimiento de lo establecido en la Ley. Es por ello muy necesario que las Secretarías Generales, que suelen figurar como responsables en la resoluciones del Rector, establezcan con toda claridad un esquema de competencias y responsabilidades que "impliquen" a los distintos sujetos que se encargan de los tratamientos y al personal que dirige los servicios a los que está adscrito el fichero en cuestión. Así mismo, es importante promover una Comisión técnica que se encargue de establecer esas medidas de seguridad que garantizan el cumplimiento de los deberes arriba reseñados.

III.4- <u>El consentimiento del afectado</u>:

Es el eje sobre el que gira todo el sistema, dado que esta materia parte de un nuevo derecho fundamental consagrado en el artículo 18.4 CE y reconocido por nuestro Tribunal Constitucional: el derecho a la llamada "autodeterminación informativa" frente a la informática o "libertad informática", que asegura a la persona un poder de decisión y control sobre el tratamiento de datos personales que le afectan.

Como principio general hemos de decir que todo tratamiento (que incluye la recogida de datos y su cesión) requiere el consentimiento del afectado. Dicho consentimiento ha de ser libre, informado y se puede prestar por cualquiera de las formas establecidas en Derecho, sea expreso, tácito o presunto, según proceda (debemos recordar los datos especialmente protegidos). Se exceptúan los casos en que una Ley permite un tratamiento sin consentimiento del afectado. Este consentimiento es revocable por causa justificada, pero sin que se le atribuyan efectos retroactivos.

A la hora de la recogida de los datos, el afectado debe ser informado de los siguientes extremos:

1- La existencia del fichero, de la identidad y dirección del responsable del fichero, su finalidad y los destinatarios de la información.

2- El carácter obligatorio o facultativo de las respuestas.

3- De las consecuencias de la obtención de los datos y de la negativa a suministrarlos.

4- De la posibilidad de ejercitar sus derechos legales: acceso, rectificación, cancelación, oposición y bloqueo.

Todos estos extremos deben figurar en los cuestionarios y demás documentos que se utilizan para la recogida de los datos: v.gr. impresos de matricula.

En cuanto a la cesión exige un consentimiento previo sobre la base de un cesionario determinado o determinable y que conste la finalidad de la cesión, pues de lo contrario el consentimiento es nulo. Ello implica que no se admiten previsiones de futuras cesiones al libre arbitrio del cedente de suerte que el

afectado no pueda determinar quienes serán esos futuros cesionarios: bastaría con prever, por ejemplo, otras universidades u organismos públicos dedicados a la educación superior.

No obstante, se establecen unas excepciones al consentimiento, algunas muy criticadas, de las que a nosotros interesan:

A-Que una "ley" disponga otra cosa.

- Que se recojan para el ejercicio de las funciones propias de las Administraciones Públicas.

B- Que se refieran a personas vinculadas por una relación negocial, laboral, administrativa o un contrato y sean necesarias para el mantenimiento de las relaciones o el cumplimiento del contrato.

C- Que la cesión que deba efectuarse tenga por destinatario el Defensor del Pueblo, el Ministerio Fiscal o los Jueces y Tribunales, en el ejercicio de sus funciones.

D- Los casos previstos en el artículo 19 de la LORTAD:

1º- Los datos recogidos o elaborados por las Administraciones Públicas para el desempeño de sus atribuciones sólo se pueden ceder a otras Administraciones Públicas para el ejercicio de competencias diferentes o competencias que versen sobre materias distintas, cuando la cesión hubiera sido prevista en las disposiciones de creación del fichero o por disposición posterior de igual o superior rango que regule su uso.

2º- Pueden cederse en todo caso los datos que una Administración Pública elabore para otra.

Veda también la Ley la cesión de los datos de los ficheros públicos a ficheros privados (academias, etc...) salvo cuando sean datos recogidos de fuentes accesibles al público y lo consienta el interesado o una ley prevea otra cosa.[111]

E- Cuando sean datos relativos a la salud y la cesión sea precisa para solucionar una urgencia o para realizar los estudios epidemiológicos.(Cfr. art.8 de la Ley 14/1988 General de Sanidad)

Por supuesto, el cesionario se obliga igualmente a cumplir todas las disposiciones legales. Igualmente se puede proceder a la cesión cuando los datos han sido sometidos a un proceso de disociación.

IV- LOS DERECHOS DE LAS PERSONAS.

IV.1- Un nuevo derecho fundamental:

Ya hemos puesto de relieve anteriormente la dimensión constitucional de esta materia y la sede en que nuestra Carta Magna consagra las garantías que pretende instituir en favor de los ciudadanos: Título I, Capítulo 2º: de los derechos y libertades fundamentales. Ello ha llevado al Legislador, así como a la Doctrina más autorizada y a nuestro Tribunal Constitucional, a afirmar con rotundidad que el artículo 18.4 CE no sólo pretende promover una acción legislativa y funcional de los poderes públicos para limitar el uso de la informática (aspecto pasivo) sino que quiere garantizar al ciudadano una esfera de poder autónomo que le permita decidir acerca del tratamiento automatizado de los datos que le conciernen, no solo del nivel de conocimiento de su vida privada, sino el control de la información que le concierne y los usos que de ella se puedan realizar.

Como afirma el Ministerio Fiscal en el caso "Olaverri" la ya citada STC de 20 de julio de 1993) el Constitución consagra "una libertad positiva para ejercer un derecho de control sobre los datos referidos a la propia persona, que han salido ya de la esfera de la intimidad, para convertirse en elementos de un

■[111] Recordemos aquí que las calificaciones académicas no son datos accesibles al público, y las direcciones, cargos y demás datos de guías, agendas y repertorios sí lo son, pero están sometidos a las excepciones que la LORTAD establece.

archivo electrónico". No se trata por tanto de un derecho "semi-gaseoso", sino de un pleno derecho fundamental a una libertad positiva de control democrático que garantiza al ciudadano el libre ejercicio de sus derechos y libertades fundamentales y un digno desarrollo de su personalidad frente a los posibles abusos del uso de la información personal tratada en los ficheros públicos y privados.

Este derecho tiene sus propios instrumentos de tutela y puesta en práctica: el llamado "hábeas data" y los derechos instrumentales o garantías jurídicas subjetivas. Todo ello lo pone de manifiesto el Legislador en la Exposición de Motivos de la LORTAD y lo ha consagrado el Tribunal Constitucional.

En definitiva, se trata de un derecho implícitamente formulado en la Constitución que otorga el poder de conocer y decidir qué datos son recogidos y para qué finalidad. Parafraseando al Tribunal Constitucional podemos definirlo como "el derecho fundamental de la persona al libre control de las informaciones referidas a su privacidad, frente a las posibles agresiones a su dignidad y libertad producidas por un uso ilegítimo del tratamiento automatizado por medios informáticos de datos personales que le conciernen".

Este es un derecho que corresponde a toda persona física, con independencia de su estado civil o nacionalidad, que sea titular de los datos objeto del tratamiento y se puede ejercitar frente a todos aquellos que realicen tratamientos automatizados que le afecten: titulares, responsables de ficheros, encargados del tratamiento y personas vinculadas a ellos.[112]

Este derecho tiene un contenido positivo integrado por la facultad de control sobre los datos, básicamente el consentimiento, y los derechos instrumentales o garantías jurídicas subjetivas. De otro lado, tiene un contenido negativo integrado por los deberes que se imponen a los terceros: respeto a los principios de calidad de los datos, etc... Conlleva también unas cargas que obligan

■ [112] Menores, incapacitados y personas fallecidas están tuteladas por la Ley, si bien los mecanismos para ejercer este derecho son los establecidos para el caso: representes legales y legitimados "mortis causa".

al titular del derecho: facilitar los datos en ciertos casos, aceptar las excepciones legalmente previstas, aportar datos veraces, etc..

IV.2- LOS DERECHOS INSTRUMENTALES:

Son los "elementos nutrientes" del derecho fundamental antes citado, responden a las diversas facetas de su contenido positivo y sirven para su puesta en práctica y refuerzan su aplicación, razón por la cual se les denomina "garantías jurídicas subjetivas". Así mismo, son derechos personalísimos por lo que la Ley exige que sean ejercitados por el propio titular o su representante legal.

1°- Derecho de Impugnación:

Este derecho permite oponerse a los llamados "juicios informáticos" es decir, con su ejercicio el afectado impugna los actos administrativos o decisiones privadas que impliquen una valoración de su comportamiento cuyo único fundamento sea un tratamiento automatizado de datos de carácter personal que ofrezca una definición de sus características o personalidad. A tal efecto, se elevó una consulta a la A.P.D. acerca de la validez de las pruebas o exámenes realizados por computadora, y la Agencia se pronunció en favor de su validez, toda vez que no suponen una decisión basada en datos personales.(art. 12 LORTAD).

2°- Derecho de Información:

Este derecho implica que al momento de la recogida de datos debe ponerse en conocimiento del sujeto los siguientes extremos:

- De la existencia del fichero automatizado.

- De su finalidad.

- De los destinatarios de la información.

- Del carácter obligatorio o voluntario de la respuesta a las cuestiones planteadas.

- De las consecuencias de la obtención de los datos y de la negativa a suministrarlos.

- De la posibilidad de ejercitar los derechos de acceso, rectificación y cancelación.

- De la identidad y dirección del responsable del fichero.

Esta información no es necesaria si su contenido se deduce claramente de la naturaleza de los datos personales que se solicitan o de las circunstancias en que se recaban.

Todo ello se debe reflejar en los cuestionarios de recogida de datos, así mismo se refleja en la Resolución que se publica en el B.O.E. y consta en el Registro General de Protección de Datos en la A.P.D., en el que se han de inscribir los ficheros, y que es de consulta pública y gratuita. De ello se deduce la importancia de cumplir con el deber de dictar la Resolución donde se recogen los ficheros y su estructura, así como cualquier modificación, supresión o creación de un nuevo fichero. (arts 5 y 13 LORTAD)

3°- El derecho de Acceso:

En virtud del mismo el afectado puede acceder al fichero para recabar información acerca de sus datos personales que son objeto de tratamiento en un fichero automatizado. Sus condiciones de ejercicio, criticables en algunos aspectos, están recogidas en la Ley y en el RD 1332/94 ya citado. Debe ejercitarse en intervalos no inferiores a 12 meses, salvo que se acredite un interés legítimo.

El afectado debe plantear su solicitud ante el responsable del fichero formulada por cualquier medio que garantice la identificación del afectado y en la que conste el fichero(s) a consultar. Para la consulta, el solicitante puede optar por uno o varios de los distintos sistemas que la Ley establece, siempre que la configuración e implantación del fichero:

- Visualización en pantalla.

- Escrito, copia o fotocopia remitida por correo.

- Telecopia.

- Cualquier otro procedimiento que sea adecuado a la configuración e implantación material del fichero, ofrecido por el responsable del mismo.

Es importante adoptar un modelo de solicitud que se ponga a disposición de los afectados en el que consten todos los extremos exigidos por la Ley. Así mismo, cabe plantearse el sistema de consulta que se está poniendo a disposición de muchos alumnos para acceder a su expediente académico, mediante claves de seguridad e identificación y "tarjetas inteligentes", que no permiten modificarlos pero sí que facilitan el acceso. Hemos de recordar asimismo, que son derechos personalísimos que sólo puede ejercitar el afectado o su representante legal.

Sea cual sea el soporte elegido, la información ha de facilitarse en forma legible e inteligible y comprenderá los datos de base del interesado y los resultantes de cualquier elaboración o proceso informático, así como el origen de los datos, los cesionarios de los mismos y la especificación de los concretos usos y finalidades para los que se almacenaron los datos.

El responsable del fichero debe resolver la petición en el plazo máximo de 1 mes a contar desde la recepción de la solicitud. Si no se contesta en este período, se entiende denegada. La negativa al acceso, en el caso de los ficheros que nos ocupan, sólo puede basarse en las siguientes circunstancias:

- Razones de interés general.

- Intereses de terceros más dignos de protección.[113]

En tales casos, dado lo ambiguo de la causa, deberá necesariamente dictarse resolución motivada por parte del responsable del fichero. Ante esta decisión, el afectado puede acudir al Director de la Agencia de Protección de Datos, quien dará traslado de la reclamación al responsable del fichero para que formule las alegaciones pertinentes en el plazo de 15 días. Pasado este plazo, la Agencia, previos los informes, pruebas y otros actos de instrucción pertinentes, incluida la audiencia al afectado y al responsable del fichero, resolverá sobre la reclamación, dando traslado a los interesados. Contra esta resolución cabe interponer recurso contencioso-administrativo, aspecto este criticado por cuanto "desvía" a esa "vía lenta" una cuestión relativa a derechos fundamentales.

■[113] Obviamos aquí la cuestión de los ficheros de los Cuerpos Seguridad y Hacienda, que se "benefician" de unas excepciones criticables en algunos casos.

Es en este punto donde debemos hacer de nuevo referencia a la vía abierta por el artículo 105.b CE sobre el acceso a los archivos de las Administraciones Públicas. Como puede deducirse paladinamente, este es un supuesto que por la ubicación de dicha norma en la Carta Magna no debe interpretarse en ningún caso como de aplicación preferente, siquiera paralela, con lo establecido en el 18.4 CE referido a derechos fundamentales, pues esta es la norma a partir de la cual debe interpretarse lo dispuesto en dicho artículo 105.b CE, tal y como expresamente establece el artículo 35.h) de la Ley 30/92 de Régimen Jurídico y Procedimiento Administrativo Común, que reconoce el derecho de los ciudadanos "al acceso a los registros y archivos de las Administraciones Públicas en los términos previstos en la Constitución y en esta u otras Leyes ".

Así lo ha entendido el propio Legislador al desarrollarla en el Título IV, Capítulo primero de la citada Ley 30/92, pues consagra en su artículo 35 los "derechos de los ciudadanos" y regula en el artículo 37 el derecho de acceso a los Archivos y Registros. A tenor del párrafo 1° mismo 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.

Esta norma general viene limitada por los párrafos 2° y 3° que salvaguardan la protección de los datos personales de terceras personas incluidas en tales documentos:

2."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 figuran incompletos o inexactos, podrán exigir que sean rectificados o completados, salvo que figuren en expedientes caducados por el transcurso del tiempo, conforme a los plazos máximos que determinen los diferentes procedimientos, de los que no pueda derivarse efecto sustantivo alguno".

Como puede apreciarse esta norma veda el acceso de terceros a los datos personales de otros sujetos, a tal efecto el concepto de intimidad debe interpretarse como referido a la privacidad, en el sentido establecido por la Exposición de Motivos de la LORTAD que hace referencia al mismo en los siguientes términos:

"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. Nótese que se habla de la privacidad y no de la intimidad: Aquella es más amplia que ésta, pues en tanto la intimidad protege la esfera en que se desarrollan las facetas más singularmente reservadas de la vida de la persona -el domicilio donde realiza su vida cotidiana, las comunicaciones en las que expresa sus sentimientos, por ejemplo- la privacidad constituye un conjunto más amplio, más global de facetas de su personalidad que, aisladamente consideradas, pueden carecer de significación intrínseca pero que, coherentemente enlazadas entre sí, arrojan como precipitado un retrato de la personalidad del individuo que éste tiene derecho a mantener reservado. Y si la intimidad, en sentido estricto, está suficientemente protegida por las previsiones de los tres primeros párrafos del artículo 18 de la Constitución y por las leyes que lo desarrollan, la privacidad puede resultar menoscabada por la utilización de las tecnologías informáticas de tan reciente desarrollo".

Por tanto, la legislación especial aquí aplicable está integrada, básicamente, por la LORTAD como norma específica para ficheros automatizados y, por extensión, a los mecanizados.

El artículo 37.3 L.P.A. permite el acceso de los terceros que acredite un interés legítimo y directo, pero sólo en determinadas circunstancias:

"El acceso a los documentos de carácter nominativo que sin incluir otros datos pertenecientes a la intimidad de las personas, figuren en los procedimientos de aplicación del derecho, salvo los de carácter sancionador o disciplinario, y que, en consideración a su contenido, puedan hacerse valer para el ejercicio de los derechos de los ciudadanos, podrá ser ejercido, además de por sus titulares, por terceros que acrediten un interés legítimo y directo".

Por tanto, el margen de actuación del tercero en el acceso a los datos personales ajenos es muy estrecho y, en todo caso debemos tener muy presente lo establecido en el artículo 11 del RD 1332/94 que desarrolla una materia relativa a garantías subjetivas integradas en un derecho fundamental, tal y como hemos afirmado. A su tenor:

"Los derechos de acceso a los ficheros automatizados, así como los de rectificación y cancelación de datos son personalísimos y serán ejercidos por el

afectado frente al responsable del fichero, sin otras limitaciones que las que prevén la Ley Orgánica 5/1992 y el presente Real Decreto.

Podrá, no obstante, actuar el representante legal del afectado cuando éste se encuentre en situación de incapacidad o minoría de edad que le imposibilite el ejercicio personal de los mismos". A tal efecto, en los ficheros de titularidad privada, la única razón para denegar el acceso es que la solicitud sea formulada por persona distinta del afectado, según el artículo 14.2 del Real Decreto citado.[114]

Por tanto, el acceso a los datos de los trabajadores y del alumnado de la Universidad obrantes en sus ficheros sólo se puede permitir al propio afectado o a su representante legal. No obstante, pueden ser objeto de cesión siempre que se cumpla el principio general del artículo 11 de la LORTAD, o se acojan a una de las excepciones legalmente previstas. Como norma general, los datos sólo pueden ser cedidos para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario con el previo consentimiento del afectado.

No obstante, caben algunas excepciones al consentimiento, entre las cuales destacamos:

A)- Cuando una Ley prevea otra cosa.

Esta excepción ha sido muy criticada porque no concreta cuál ha de ser el rango de esa "Ley" por lo que puede permitir que un Reglamento o Resolución limite un derecho fundamental.

B)- Cuando se trate de datos recogidos de fuentes accesibles al público. En este punto conviene recordar que el artículo 19.3 no permite ceder datos de esta

■[114] El artículo 32 L.P.A. regula la representación de los interesados admitiendo éste cuando ambos, representante y representado, posean plena capacidad de obrar y siempre que se haga constar de forma fidedigna por un medio válido en Derecho, salvo para los actos "de mero trámite" en los que se presume la representación. No obstante, tan "generoso" criterio no puede aplicarse al ejercicio de estos derechos, pues el RD 1332/94 lo veda expresamente al circunscribirse a la representación legal de menores e incapacitados.

naturaleza recogidos en ficheros de titularidad pública a los ficheros privados, sino con el consentimiento del afectado o cuando una Ley prevea otra cosa.

C)- Cuando el establecimiento del fichero automatizado responda a la libre y legítima aceptación de una relación jurídica cuyo desarrollo, cumplimiento y control implique necesariamente la conexión de dicho fichero con ficheros de terceros. En este caso la cesión sólo será legítima en cuanto se limite a la finalidad que la justifique.

Esta es una de las excepciones que más juego pueden dar en los ficheros universitarios toda vez que la actividad de las universidades cada vez provoca una mayor necesidad de interconexión.

D)- Cuando la cesión es a órganos tales como el Defensor del Pueblo, Ministerio Fiscal, Jueces y Tribunales en el ejercicio de sus funciones.

E)- Cuando se produzca entre Administraciones Públicas en los supuestos del artículo 19 LORTAD, ya comentado.

Debemos recordar en este punto las cautelas antes reseñadas al hablar del consentimiento del afectado en la cesión de datos y la conveniencia de preverlo en los formularios de recogida de datos.[115]

4°- <u>Los derechos de Rectificación y Cancelación</u>:

Son consecuencia del anterior y permiten al afectado instar al responsable del fichero para que, en cumplimiento de sus deberes deducidos de los principios

■[115] Reiteramos la necesidad de que el cesionario sea determinado o determinable y que el consentimiento es revocable. Es por ello importante que las Universidades prevean un sistema coordinado de cesiones entre ellas bajo el amparo de las excepciones previstas en la Ley y, cuando sea preciso, un consentimiento previo recabado al afectado. Así mismo, la acción social desempeñada por muchas Universidades les ha llevado a tratar datos "sensibles" que afectan al sujeto que facilita el dato y a terceros, cónyuge, hijos, padres, convivientes, etc... que pueden ser relativos a la salud, rendimientos económicos, sanciones y demás cuyo tratamiento está muy restringido por el artículo 7 y 8, por lo que no deben ser objeto de cesión y en esos ficheros deben extremarse las medidas de seguridad previstas en el artículo 9 y 10, cuya supervisión corresponde, en última instancia, al responsable del fichero.

de calidad y licitud de los tratamientos, mantenga la exactitud, veracidad y oportunidad de los datos obrantes en el fichero rectificando o cancelando los datos incompletos, inexactos, inadecuados, excesivos o no pertinentes. No obstante, los datos que reflejan hechos constados en un procedimiento administrativo se considerarán exactos si coinciden unos y otros.

La solicitud debe dirigirse al responsable del fichero, con las precisiones de identidad antes enunciadas, y haciendo constar los datos que se han de rectificar o cancelar y el fichero(s) en que se encuentran.

El responsable del fichero debe hacer efectiva la rectificación o cancelación procedente en el plazo de 5 días siguientes a la recepción de la solicitud. Si los datos rectificados o cancelados hubiesen sido cedidos previamente, el responsable del fichero debe comunicarlo al cesionario dentro del mismo plazo.

La petición puede ser desestimada de dos maneras:

A - Por transcurso del plazo de 5 días sin contestación expresa.

B - Por resolución motivada en la que se comunica la decisión de acceder a la solicitud. Las razones en que ello puede fundarse son:

- Que la legislación aplicable al caso imponga un plazo determinado de conservación de los datos en cuestión.

- Cuando su cancelación pueda causar un perjuicio al propio afectado o a un tercero.

- Cuando concurran razones de interés general.

- Cuando concurran intereses de terceros más dignos de protección.

Ante la denegación el afectado puede iniciar el procedimiento de tutela de sus derechos ante la Agencia de Protección de Datos, descrito anteriormente y que se regula en los artículos 17.1 LORTAD y 17 del RD 1332/94

5°- Otros derechos instrumentales:

Nos referimos en concreto a dos facultades que se encuentran implícitas en el contenido del derecho a libre autodeterminación informativa. El primero de ellos el derecho de bloqueo, recogido en el artículo 16 del RD 1332/94 y que permite exigir que, cuando sea procedente la cancelación de datos personales y no sea posible su extinción física, tanto por razones técnicas, como por causa del procedimiento o soporte utilizado, el responsable del fichero proceda al bloqueo de los datos con la finalidad de impedir su ulterior proceso o utilización. Tal extremo habrá de ser comunicado igualmente a los posibles cesionarios de los datos objeto de bloqueo.

No obstante, cuando tales datos han sido recogidos o registrados por medios fraudulentos, desleales o ilícitos y ello se demuestre, la cancelación de los mismos comporta siempre la destrucción del soporte en que figuren.

Como quiera que el bloqueo supone una decisión del responsable que podemos considerar subsidiaria de la cancelación, el afectado puede recurrirla ante la Agencia de Protección de Datos.

El llamado derecho de Oposición esta formulado en el artículo 14 de la Directiva 95/46 y está conectado con las excepciones al consentimiento en la recogida y tratamiento de datos. Como se ha dicho, el tratamiento o cesión de datos personales en los ficheros de titularidad pública puede llevarse a cabo sin consentimiento del afectado cuando sea necesario para el cumplimiento de una misión de interés público o inherente al ejercicio del poder público conferido al responsable del tratamiento o al cesionario. Igualmente, se admite esta excepción cuando sea necesario para la satisfacción de un interés legítimo perseguido por el responsable del tratamiento o por el cesionario, siempre que frente a ello no deban prevalecer el interés o los derechos y libertades fundamentales del interesado que deban ser protegidos.

En tales casos, el afectado puede oponerse, en cualquier momento y por razones legítimas propias de su situación particular, a que los datos sean objeto de tratamiento, salvo que la legislación nacional disponga otra cosa. En caso de oposición justificada, el tratamiento que efectúe el responsable no podrá referirse a esos datos.

Este derecho es también ejercitable, previa petición y sin gastos, al tratamiento de los datos personales respecto de los cuales el responsable prevea un tratamiento destinado a la prospección. Debe ser informado previamente en caso de cesión para el mismo destino, a la cual podrá oponerse, sin que ello le ocasione gasto alguno.

V.- TUTELA DE LOS DERECHOS

Los mecanismos de tutela de estos derechos poseen varias vías de aplicación. Además de la autotutela del interesado que diligentemente debe ejercitar sus derechos en tiempo y forma, podemos citar tres posibles actuaciones.

V.1- La reclamación administrativa:

Los actos que supongan infracción de los deberes establecidos en la Ley o la lesión de un derecho del afectado pueden ser objeto de reclamación ante la Agencia de Protección de Datos. Para ello se arbitran dos procedimientos:

A)- Reclamación ante la Agencia de Protección de Datos:

Los artículos 17 de la LORTAD y del RD 1332/94 establecen y regulan un procedimiento que se aplica frente a la negativa por parte del responsable del fichero al ejercicio de los derechos de acceso, rectificación y cancelación. Para ello el afectado debe comunicar a la Agencia los hechos alegados y los preceptos legales que se entienden infringidos. De la reclamación se da traslado al responsable del fichero para que, en el plazo de 15 días, formule las alegaciones oportunas. Transcurrido este plazo, la Agencia resolverá la cuestión planteada, previos los informes, pruebas y otros actos que considere oportunas, incluida la audiencia a las partes. Debemos entender que este mismo procedimiento debe aplicarse en el caso de que el responsable opte por el bloqueo de los datos.

B)- Recurso ante los Tribunales:

Contra esta decisión de la Agencia cabe plantear recurso contencioso administrativo, cuestión que como se ha dicho ha sido criticada por un sector doctrinal, que hubiera preferido un procedimiento judicial más rápido y menos costoso.

C)- El procedimiento sancionador:

Viene recogido en el artículo 47 de la LORTAD y se regula en los artículos 18 y 19 del RD 1332/94. A tal efecto la Ley hace una precisión muy importante en su artículo 42: los responsables de los ficheros están sujetos al régimen sancionador establecido en la misma. Incluso el artículo 45.2 establece para los ficheros de las Administraciones Públicas la posibilidad de que el Director de la Agencia de Protección de Datos proponga la iniciación de actuaciones disciplinarias por la vía establecida en la legislación sobre régimen disciplinario de las Administraciones Públicas.[116]

A tal efecto, la LORTAD establece en su artículo 43 un catálogo de infracciones leves, graves y muy graves, que se completa con los tipos recogidos en el Código Penal. De entre todas ellas podemos citar las siguientes:

A) Leves:

- No proceder a la rectificación o cancelación de errores, lagunas o inexactitudes de carácter formal de los ficheros, bien sea de oficio o a petición de persona o institución capacitada para ello.

- No cumplir las instrucciones del Director de la Agencia, o no suministrar la información requerida.

- No conservar los datos actualizados en los ficheros.

- Cualquier otra que afecte a cuestiones formales o documentales y que no constituya una infracción más grave.

B) Graves:

- Proceder a la creación de ficheros de titularidad pública o iniciar la recogida de datos para los mismos sin cumplir las formalidades legales previstas.

■ 116 Cfr. arts 127 y siguientes de la Ley 39/92 de Procedimiento Administrativo y RD 1398/93 de 4 de agosto por el que se aprueba el Reglamento para el ejercicio de la potestad sancionadora.

- Recoger datos sin el consentimiento preceptivo o sin dar la información legalmente requerida.

- Realizar el tratamiento sin cumplir los principios de calidad y licitud o infringiendo los deberes establecidos en la Ley y demás disposiciones.

- Impedir u obstaculizar el ejercicio del derecho de acceso o negar la información solicitada.

- Mantener los datos inexactos o no proceder a rectificarlos o cancelarlos cuando ello proceda y resulten afectados los derechos de las personas.

- La vulneración del deber de secreto, cuando no sea infracción grave.

- No observar las medidas de seguridad técnicas y organizativas que reglamentariamente se determinen en los locales, programas y equipos.

- No remitir a la Agencia las notificaciones previstas en la Ley o en sus disposiciones de desarrollo o no proporcionarle cuantos documentos e informaciones deba recibir.

- Obstruir el ejercicio de la labor inspectora.

C) Muy Graves:

- La recogida de datos en forma engañosa o fraudulenta.

- Comunicar o ceder datos fuera de los casos permitidos.

- Recabar y tratar datos sensibles del artículo 7.2 sin consentimiento del afectado o los del artículo 7.3 sin consentimiento o cuando no lo permita una Ley.

- Crear ficheros cuya única finalidad sea tratar datos relativos a ideología, creencias, religión, origen racial o vida sexual.

- No cesar en el uso ilícito de los tratamientos cuando sea requerido por la Agencia.

- Transferir datos personales a países que no proporcionen un nivel adecuado de protección.[117]

- Realizar un tratamiento de los datos personales de forma ilegítima o con menosprecio de los principios y garantías que les sean de aplicación, si con ello se impide o atenta contra el ejercicio de los derechos fundamentales.

- La vulneración del deber de secreto con respecto a los datos especialmente protegidos.

La iniciación del procedimiento sancionador corresponde de oficio al Director de la Agencia por propia iniciativa o mediante denuncia del afectado. En el acuerdo del Director se designará al instructor y, en su caso, el secretario, así mismo se identificará al presunto responsable y se concretan los hechos imputados, con expresión de las infracciones cometidas, de las medidas provisionales a adoptar y las sanciones que pudieran imponerse.[118]

Dicho acuerdo de incoación de expediente se notifica al responsable y se le informa de su derecho a formular alegaciones y de utilizar los medios de defensa procedentes, citando expresamente los preceptos que son de aplicación. Dentro de los 15 días siguientes a la notificación, el instructor ordenará la práctica de cuantas pruebas y actos de instrucción sean procedentes para esclarecer los hechos y determinar las responsabilidades. En el mismo plazo, el presunto responsable puede hacer sus alegaciones y proponer las pruebas que estime convenientes.

Transcurrido aquél plazo el instructor acordará la practica de las pruebas pertinentes, a cuyo efecto concederá un plazo de 30 días, transcurrido el cual el expediente se pondrá de manifiesto al responsable para que en el plazo de 15 días formule sus alegaciones y aporte los documentos que estime de interés.

■ [117] Cfr. Orden del Ministerio de Justicia de 2 de Febrero de 1995.

■ [118] Cuando las infracciones son cometidas en ficheros de las Administraciones Públicas, el Director de la Agencia debe dictar una resolución estableciendo las medidas que procede adoptar para que cesen o se corrijan los efectos de la infracción. Esta resolución se notifica al responsable del fichero, al órgano del que dependa jerárquicamente y a los afectados si los hubiera.

Cumplidos los trámites se dicta la propuesta motivada de resolución que se notifica al presunto responsable para que formule las alegaciones oportunas, en el plazo de 15 días. Concluido éste, el instructor elevará el expediente al Director de la Agencia, quien puede ordenar la práctica de nuevas actuaciones.

La resolución ha de contener necesariamente los hechos imputados, la infracción cometida, el precepto que la tipifica, el responsable de la misma y la sanción impuesta; igualmente puede contener la declaración de no existencia de responsabilidad. Contra la resolución cabe interponer recurso contencioso-administrativo y ha de ser notificada también al denunciante, si lo hubiera.

Las sanciones pueden ser desde una multa de 100.000 pts hasta los 100 millones para las infracciones muy graves, si bien su cuantía se gradúa en función de los derechos afectados, al volumen de los tratamientos efectuados, a los beneficios obtenidos, al grado de intencionalidad y a la reincidencia.

El artículo 197.2 del Código Penal impone las penas de prisión de 1 a 4 años y multa de 12 a 24 meses "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 o a quien los altere o utilice en perjuicio del titular de los datos o de un tercero".

Si tales datos se revelan, difunden o ceden a terceros se impone la pena de prisión de 2 a 5 años. Se impone la pena de prisión de 1 a 3 años y multa de 12 a 24 meses al que, con conocimiento de su origen ilícito y sin haber tomado parte en su descubrimiento, realice la conducta antes descrita.

Si los hechos antes descritos se realizan por los encargados o responsables de los ficheros, soportes informáticos, electrónicos o telemáticos, archivos o registros, se impone la pena de 3 a 5 años de prisión y se difunden, ceden o revelan, se impone en su mitad superior.

Si tales actos están referidos a los datos especialmente protegidos o la víctima sea un menor o un incapaz, se impondrán las penas previstas en su mitad

superior. Ello se agrava si existe ánimo de lucro, pues la pena puede llegar hasta la prisión de 4 a 7 años.

El artículo 198 agrava la pena, e impone la inhabilitación absoluta por tiempo de 6 a 12 años, cuando el autor de las conductas descritas sea una autoridad o funcionario público que actúa prevaliéndose de su cargo.[119]

Para proceder contra estas conductas se precisa denuncia del agraviado o de su representante legal; no obstante, no se exige denuncia en los casos del artículo 198, ni cuando el delito afecte a los intereses generales o a una pluralidad de personas. Tal sería el caso de que la responsabilidad penal se derivase de hechos probados en una resolución sancionadora de la Agencia de Protección de Datos.

V.2- Derecho de Indemnización:

Las lesiones que se produzcan por incumplimiento de la Ley a los afectados en sus bienes o derechos, originan el deber de indemnizar. La reclamación en el caso de los ficheros de titularidad pública se substanciará según lo previsto en el artículo 139 y siguientes de la Ley 30/92 y legislación concordante. Para calcular la indemnización se atenderá al resultado dañoso, la existencia de intencionalidad, la responsabilidad profesional del personal al servicio de las Administraciones Públicas y su relación con la producción del resultado dañoso.

Las autoridades y personal al servicio de las Administraciones públicas responden de acuerdo a lo establecido en los artículos 145 y siguientes de la Ley 30/92, de suerte que la reclamación del particular se plantea directamente a la Administración, quien debe indemnizar al particular y luego actuar contra la autoridad o funcionario causante de la lesión, siguiendo el procedimiento reglamentario, sin perjuicio de pasar el tanto de culpa a los Tribunales competentes.

■ [119] Es también digno de mención que el artículo 200 del Código Penal extiende su protección a los datos reservados de las personas jurídicas.

Esta llamada a la "responsabilidad profesional" del personal nos induce a realizar una última reflexión: la mayoría de las Universidades han establecido como responsable del fichero al Secretario General, posiblemente por esa competencia de custodia de archivos y registros que posee todo secretario de órgano colegiado, pero ello no ha corrido paralelo con la capacidad de control sobre tratamientos que posee dicho responsable.[120] A menudo en estas cuestiones se exigen unos conocimientos técnicos y jurídicos que no concurren en algunas personas, por lo que se presume una preparación que no se posee y por cuya ausencia se debe responder.

De otro lado, los ficheros automatizados suelen estar adscritos a órganos o dependencias muy concretas: personal, alumnos, acción social, etc... cuyos jefes o responsables actúan con una elevada dosis de autonomía, por lo que el responsable "ex lege" no suele estar en contacto con su gestión diaria. Frente a todo ello, la L.P.A. establece que la responsabilidad civil por estas infracciones se mide según los criterios de la legislación civil, donde prima la responsabilidad objetiva por culpa "in vigilando" o "in eligendo" que hace responder por hechos ajenos.

Por todo ello consideramos necesario formar en la materia a todo el personal relacionado con los ficheros, establecer un adecuado marco normativo que consagre un claro esquema de competencias y responsabilidades y crear un órgano de control y seguimiento de los tratamientos y seguridad de los ficheros.

Con esto damos fin a estas breves y apretadas líneas en las que hemos querido llamar la atención acerca de un problema de cuya magnitud, tal vez, no seamos plenamente conscientes y, que sin embargo, por la gravedad de las consecuencias que pueden derivarse, precisa una mayor atención de las Universidades para evitar que un instrumento positivo como es la informática,

■ 120 No obstante, y a título de ejemplo, algunas Universidades han instituido como responsable al Gerente, caso de Valladolid o Baleares; otras al Director o Jefe del órgano al que está adscrito el fichero, caso de Zaragoza. Granada ha establecido la competencia del Secretario General, bajo la autoridad del Rector, "sin perjuicio de la responsabilidad directa que en la gestión y custodia de los ficheros corresponde al jefe de cada uno de los servicios o unidades".

pueda ser objeto de utilización para fines incompatibles con los servicios que presta la Universidad.

BREVE RESEÑA BIBLIOGRAFICA:

- A.A.V.V. " Jornadas sobre el derecho Español de la Protección de Datos Personales ". Madrid, 1996

- A.A. V.V.:" Banche dati e diritti della persona ". Milano, 1988

- Agencia de Protección de Datos: Memorias de los años 1994, 1995 y 1996

- Davara Rodríguez, M.A.:" Derecho Informático ". Pamplona, 1993

- Frossini, V.:" Informática y derecho ". Bogotá, 1988

- Pérez Luño, A.E.:" Manual de informática y derecho". Barcelona, 1996

- Revista "Informática y Derecho" de la UNED, números 1 al 11, Aranzadi, Pamplona.

La validez jurídica de las comunicaciones por fax y su aceptación en la Administración de Justicia: Incidencia actual y perspectiva de futuro

JULIO JOSE ELIAS BATURONES

Licenciado en Derecho y experto en Criminología

1.- INTRODUCCION.

Los medios técnicos modernos de comunicación están revolucionando de forma vertiginosa las relaciones entre personas y entidades en el mundo entero; es de común conocimiento por todos que el correo ordinario por "carta escrita", constituido por papel suscrito y contenido en un sobre cerrado, se encuentra hoy en día completamente desfasado, en un contexto de espacio-tiempo que se presenta configurado como algo cada vez más cercano y rápido, respectivamente.

En este sentido, el *FAX* por su agilidad y cercanía temporal, es de aceptación y utilización generalizada, en el conjunto de relaciones sociales y comerciales, siendo un buen ejemplo de lo ya dicho con anterioridad; a nadie se le puede escapar la necesidad "social" de este medio de comunicación, sin el cual difícilmente se podría concebir la consecución de acuerdos comerciales y empresariales, tanto a nivel de grandes empresas como incluso en la esfera de las simples relaciones entre particulares.

Sin género de dudas, el factor "tiempo" es la verdadera obsesión en el mundo actual, y los medios para conseguir dicho objetivo es una prioridad casi absoluta en todos los mercados; la tecnología y la industria de las telecomunicaciones y de la infomática (con sistemas multimedia), vienen a responder puntualmente a esta necesidad.

No obstante, a pesar de esta realidad del empleo del *FAX*, no se puede afirmar "cien por cien" un reconocimiento equivalente en el plano de la normativa y jurisprudencia más reciente; el objetivo de este trabajo será el de estudiar los mecanismos legales, especialmente, los procesales para "validar" a este medio de comunicación, y en segundo término comprobar las respuestas más cercanas y cuáles son los requisitos exigibles por los Tribunales de Justicia para conceder al *FAX* un valor jurídico pleno.

En la última parte del trabajo expresaré mis propias conclusiones sobre esta importante materia, haciendo una especial mención a su incidencia en el reconocimiento que el artículo 24 de nuestra Constitución de 1978 se concede al "derecho de todos a un proceso público sin dilaciones indebidas y con todas las garantías".

2.-NORMATIVA VIGENTE.

La Ley Orgánica 6/1985, de 1 de Julio, del Poder Judicial, publicado en el B.O.E número 157 de 2 de Julio, tiene un precepto concreto en su articulado que afirma la aceptación de los medios modernos de comunicación a nivel de las notificaciones de la resoluciones judiciales; me estoy refiriendo al artículo 271, que dice lo siguiente:

"Las notificaciones podrán practicarse por medio de correo, del telégrafo o de cualquier medio técnico que permita la constancia de su práctica y de las circunstancias esenciales de la misma según determinen las leyes procesales".

Hay que tener en cuenta la enorme trascendencia e importancia de este precepto, sobre todo si no olvidamos que este artículo es precedido por el 270 que inicia la regulación del Capítulo VII del Título III de la misma bajo el título "de la notificación" y que dice:

"Las diligencias de ordenación, providencias, autos y sentencias se notificarán a todos los que sean partes en el pleito o la causa, y también a quienes se refieran o puedan parar perjuicios, cuando así se disponga expresamente en aquellas resoluciones, de conformidad con la Ley".

Es decir que desde el momento preciso en que se verifique la notificación de las resoluciones judiciales se producen dos efectos claves en lo que respecta a la protección de los derechos de las personas afectadas o partes en los diferentes procesos judiciales:

1º) Tienen un conocimiento real de la existencia y contenido de tales resoluciones;

2º) Comienza los plazos para su impugnación o recurso si consideran lesivos o perjudiciales el sentido concreto de lo resuelto por el Juez o Tribunal, de tal modo, que si desde la notificación hasta que se cumpla el plazo concreto para su recurso la persona en cuestión no lo interpone, adquiriría tal resolución la condición de firmeza en Derecho, y por lo tanto a partir de ese preciso momento se deberá cumplir estrictamente lo resuelto, ya que en caso contrario, se estaría a la ejecución de lo fallado, en el sentido de lo dispuesto en el artículo 118 de la Constitución, que dice lo siguiente:

"Es obligado cumplir las sentencias y demás resoluciones judiciales firmes de los Jueces y Tribunales, así como prestar la colaboración requerida por éstos en el curso del proceso y en la ejecución de lo resuelto."

Resulta evidente, por lo tanto, tener a ciencia cierta debida constancia de la notificación de la resolución judicial a cada una de las partes y afectados en el proceso, y por ello las leyes procesales vigentes regulan de forma exhaustiva las diversas formas de practicar tales notificaciones en función de la transcendencia e importancia del acto en cuestión.

Comenzando por la Ley de Enjuiciamiento Civil, que constituye la normativa procesal general y común de todas las leyes procesales, se puede comprobar esta materia en los artículos 260 y siguientes.

Para la mejor comprensión de la forma de notificar las resoluciones judiciales en este orden jurisdiccional, se puede explicar con el siguiente esquema:

1º) De forma personal y en la propia sede del Juzgado.

Artículo 260: "Todas las providencias, autos y sentencias se notificarán a quienes sean parte en un juicio, en el mismo día de su fecha o publicación, y no siendo posible, en el siguiente..."

Artículo 264: "Se harán las notificaciones en la Escribanía (hoy se debe entender como "Secretaría" al ser la anterior denominación una reliquia del pasado) o en el local que en cada Tribunal estuviere destinado a este fin, si comparecieran los interesados..."

2º) Para el supuesto de que no sea posible ni conveniente la notificación personal en la sede del Juzgado, supuesto más general, el artículo 261 de esta Ley, en su primer apartado establece, a su vez, un criterio de notificación común:

"Las notificaciones, citaciones y emplazamientos que se practiquen fuera de la sede del Juzgado o Tribunal, se hará por correo certificado con acuse de recibo, dando fe el Secretario en los autos del contenido del sobre remitido, y uniéndose a aquéllos el acuse de recibo."

3º) No obstante, en este artículo de la Ley Procesal Civil, se contempla una excepción al criterio general ya previsto, de la notificación mediante correo certificado con acuse de recibo de este primer apartado, en concreto, en el párrafo cuarto se dice:

"No obstante lo dispuesto en el párrafo primero, los actos de comunicación se realizarán en el modo establecido en los artículos siguientes, cuando su destinatario sea o deba ser parte en el juicio o en cualquiera de sus instancias y dependa de la comunicación su personación en las actuaciones, cuando adopten la forma de requerimiento y en aquellos otros casos en que lo disponga la ley, o así lo acuerde el juzgador, por aconsejarlo las circunstancias personales que concurran."

En estos "supuestos especiales" la Ley de Enjuiciamiento Civil prevé que las notificaciones en sentido amplio (comprendiendo como tales, notificaciones, emplazamientos, citaciones y requerimientos), se verificarán mediante cédula en los términos y modalidades contempladas en los artículos 262 y siguientes de la misma Ley.

Dicho sea lo anterior, y sin perjuicio del interés didáctico de este esquema, lo que resulta auténticamente importante para el objetivo del presente estudio, es que en este articulo 261 de la Ley se admite la posibilidad legal de practicar las notificaciones de las resoluciones judiciales mediante medios técnicos modernos de comunicación, en concreto, me refiero a la redacción de su apartado tercero, que dice lo siguiente:

"Cuando lo aconsejen circunstancias particulares o exigencias de mayor celeridad, se podrá disponer que la comunicación se practique por el servicio de telégrafos o por cualquier otro medio idóneo de comunicación, adoptándose las medidas oportunas para asegurar la recepción del acto comunicado del cual quedará constancia en autos."

También hay que destacar que en el artículo 288 de esta misma Ley, y en lo que respecta a la regulación del llamado "auxilio judicial" (es decir, cuando un órgano judicial necesita de la ayuda de otro de diferente localidad para la práctica de determinadas diligencias, al encontrarse residiendo en la misma el destinatario, evitando su desplazamiento al primer juzgado) se contempla otra posibilidad de empleo de medio técnico distinto del correo ordinario, en los siguientes términos:

"En el caso de que la actuación requerida se considere de urgente práctica, podrá formularse la petición por telex, telégrafo, teléfono o por cualquier otro medio bajo la fe del Secretario, sin perjuicio de confirmarla en despacho ordinario que habrá de remitirse el mismo día o al siguiente."

Por lo tanto, en este orden jurisdiccional civil, cabe la posibilidad de utilizar el *FAX* como medio de comunicación y notificación, siempre y cuando por el Secretario del Juzgado o Tribunal se acredite en los autos suficientemente su constancia, remisión y contenido del texto en cuestión, a semejanza de lo previsto por el conducto del correo ordinario certificado con acuse de recibo.

En el orden jurisdiccional penal, la Ley de Enjuiciamiento Criminal regula esta materia en los artículos 166 y siguientes.

En concreto, el primer apartado, del artículo 166 se dice lo siguiente:
"Las notificaciones, citaciones y emplazamientos que se practiquen fuera de los estrados (refiriéndose lógicamente a la Secretaría) del Juzgado o Tribunal se harán, respectivamente, por un Agente judicial o por un Oficial de Sala. Cuando el Juez o Presidente del Tribunal lo estime conveniente podrán hacerse por correo certificado con acuse de recibo,

dando fe el Secretario en los autos del contenido del sobre remitido y uniéndose el acuse de recibo."

En el párrafo siguiente, o sea en el segundo, se añade por el legislador:

"que este último procedimiento no será de aplicación para las notificaciones previstas en los artículos 160, 501 y 517"

Es decir, para los supuestos de notificaciones para sentencias, autos elevando a prisión de detención o dejándola sin efecto, y auto de prisión o acordando la soltura del preso, respectivamente.

Sin embargo, hay que destacar que a pesar de estas limitaciones o restricciones legales, en la vida diaria de los tribunales penales se utiliza el FAX como medio de comunicación para acordar, por ejemplo, una puesta en libertad de un preso, al afectar la medida a un derecho fundamental como es el de la libertad, aunque exista un vacío normativo en este sentido, que es colmado por la práctica forense.

La Ley de la Jurisdicción Contencioso Administrativa no prevé, especialmente, una normativa propia respecto a las comunicaciones y notificaciones de las resoluciones judiciales, por lo que como consecuencia de la naturaleza supletoria de la Ley de Enjuiciamiento Civil, hay que entender que se aplicarán las normas propias de su regulación en este orden jurisdiccional.

No obstante quisiera mencionar, aunque brevemente, que a pesar de esta falta de regulación, en el procedimiento contencioso administrativo especial previsto en la Ley de Protección Jurisdiccional de los Derechos Fundamentales de la Persona, número 62/1978, de 26 de diciembre (es decir, contra aquellos actos de la Administración Pública, sujetos a Derecho Administrativo, "que afecten al ejercicio de los derechos fundamentales de la persona" que se refiere el artículo 53.2 de la Constitución Española, especialmente por su incidencia en derechos tan básicos como los contemplados en la Carta Magna, en su regulación de la Sección 2ª, artículos 6 a 10) por su carácter de tramitación urgente y preferente, considero que la utilización del *FAX*, como medio técnico de comunicación, notificación e, incluso, remisión del expediente administrativo -que contempla con breve plazo de cinco días en el apartado segundo del artículo 8 -

puede servir a los fines que contempla dicha Ley, sin perjuicio, claro está, de su remisión original por el conducto ordinario.

La Ley de Procedimiento Laboral, en su redacción actual según Real Decreto Legislativo 2/1995 de 7 de Abril por el que se aprueba su Texto Refundido, no solo es la legislación procesal de más reciente factura, sino que además, se puede afirmar sin género de duda alguna, que constituye una auténtica pionera en muchas cuestiones procesales, y en concreto, en el tema objeto de este estudio, es una auténtica "joya normativa", de la que puede servir de ejemplo para futuras reformas legislativas en las otras normas procesales anteriormente estudiadas, por su modernidad.

Así, el artículo 53, que inicia la regulación de "los actos de comunicación", en su primer apartado establece los criterios primordiales que deben seguirse en dichos actos en los siguientes términos:

"Los actos de comunicación se efectuarán en forma que se garanticen el derecho a la defensa y los principios de igualdad y de contradicción. Habrán de practicarse por los medios más rápidos y eficaces que permitan su adecuada constancia y las circunstancias esenciales de la misma".

Los artículos siguientes, es decir, del 54 al 62, contemplan supuestos de notificaciones a las partes con un criterio similar a la Ley de Enjuiciamiento Civil, o dicho de otra forma, siguiendo el mismo esquema a partir del cual se notificarán las resoluciones judiciales:

Artículo 54.1: "Las providencias, autos, sentencias y diligencias de ordenación del Secretario, se notificarán en el mismo día de su fecha, o de la publicación, en su caso, a todos los que sean parte en el juicio, y no siendo posible, en el día hábil siguiente."

Artículo 55: "Las citaciones, notificaciones, emplazamientos y requerimientos se harán por el Secretario o por quien desempeñe sus funciones, en el local del Juzgado o Tribunal o en el servicio común, si allí comparecieren por propia iniciativa los interesados, y en otro caso, en el domicilio señalado a estos efectos."

Artículo 56.1: "Las citaciones, notificaciones y emplazamientos que se practiquen fuera de la sede del Juzgado o Tribunal se harán, cualquiera que sea el destinatario, por correo certificado con acuse de recibo, dando fe el Secretario en los autos del contenido del sobre remitido, y uniéndose en ellos el acuse de recibo."

Artículo 57.1: "Si las diligencias de comunicación no pudieren efectuarse en la forma indicada se practicarán mediante entrega de cédula al destinatario...".

Y en los artículos siguientes se contempla la forma de llevarse a cabo dichas notificaciones por cédula en términos similares a los contemplados en la Ley Procesal Civil.

Sin embargo, en el artículo 56 se regula un último párrafo, el cuarto, que constituye la única vez en que por una norma procesal se admite **expresamente** la posibilidad de utilización de un medio técnico de comunicación moderna, en donde cabe con toda seguridad el *FAX*, ya que tiene este contenido:

"Se podrá disponer que la comunicación se practique por el servicio de telégrafo o por cualquier otro medio de comunicación o de transmisión de textos si los interesados facilitaran los datos indicativos para utilizarlos. Se adoptarán las medidas oportunas para asegurar la recepción del acto comunicado del cual quedará constancia en autos."

Aunque en este precepto no se utilice el término técnico de *FAX*, resulta evidente que en la descripción normativa de "**cualquier otro medio de comunicación o de transmisión de textos**" se encuentra ubicado el mismo, ya que, para su empleo, se requiere que los interesados faciliten los datos correspondientes a sus respectivos números de emisor-receptor, utilizando la línea telefónica para la transmisión del texto que se pretende comunicar, y tanto para uno u otro sujeto de la comunicación, los correspondientes aparatos mecánicos de soporte se deja constancia, no sólo de la hora, sino también de la certeza de la operación realizada.

En este sentido, se acreditaría en los autos mediante una Diligencia de constancia expedida por el Sr. Secretario del Juzgado o Tribunal de lo Social, la hora de la remisión del *FAX*, su número de registro, y se unirá en las actuaciones el recibo acreditativo de tal remisión con el "OK" de su receptor aceptando la comunicación; es decir, con unas garantías similares y de analógica aplicación a lo previsto con anterioridad en el primer párrafo de este importante artículo 56, respecto a las comunicaciones por correo ordinario certificado con acuse de recibo.

Hay que llamar la atención de la gran novedad del contenido del artículo 56. 4 de la L.P.L, ya que además de servir al *FAX* como medio idóneo

de transmisión de textos, considero que abre la posibilidad de otros medios aún más avanzados y rápidos, como podría ser en un futuro cada vez más próximo en el tiempo, el **correo electrónico** vía informática, a través de medios multimedia como el *MODEM-FAX* entre el ordenador central del Juzgado y, por ejemplo, ordenadores personales de procuradores de las partes, del Servicio del Colegio de dichos profesionales especialmente constituído para tales notificaciones, o incluso de particulares, como peritos judiciales, médicos forenses, etc., por lo que abre una puerta importante en el mundo jurídico procesal de las comunicaciones, de unas implicaciones realmente asombrosas para el logro de una justicia auténticamente ágil y segura.

Antes de cerrar este primer apartado del trabajo, con el estudio del orden jurisdiccional laboral de tan especial transcendencia como hemos observado respecto al *FAX*, considero importante destacar otros dos preceptos de dicha normativa que igualmente hacen referencia a los medios técnicos modernos de comunicación, aunque referidos a otros aspectos del proceso, y son los siguientes:

1.- En orden a los principios generales:

Artículo 74: "Los Jueces y Tribunales del orden jurisdiccional social interpretarán y aplicarán las normas reguladoras del proceso laboral ordinario según los principios de inmediación, oralidad, concentración y CELERIDAD."

2.- En materia de régimen probatorio:

Artículo 90.1: "Las partes podrán valerse de cuantos medios de prueba se encuentren regulados en la Ley, admitiéndose como tales los medios mecánicos de reproducción de la palabra, de la imagen y del sonido, salvo que se hubieren obtenido, directa o indirectamente, mediante procedimientos que supongan violación de derechos fundamentales o libertades públicas."

3.- JURISPRUDENCIA SOBRE LA MATERIA.

A la hora de estudiar los criterios concretos de los Jueces y Tribunales de Justicia respecto al *FAX*, lo primero que hay que afirmar es que no existen supuestos muy generalizados en que se hayan contemplado problemas de su aceptación, dada cuenta que es una cuestión tan nueva en el mundo del Derecho y del Proceso que explica la escasa jurisprudencia sobre esta materia.

Sin embargo, he conseguido obtener y localizar cuatro resoluciones de diferentes Tribunales de Justicia, que desde su diferente posición han entrado en el análisis del *FAX* dentro de su validez, y con unos puntos de vista que considero de un gran valor para comprender los requisitos no ya sólo legales, sino también de orden práctico que se exigen para que dicho medio pueda emplearse eficazmente en las relaciones sociales.

Me estoy refiriendo a una sentencia del Tribunal Constitucional, un Auto de la Sala de lo Social del Tribunal Supremo, y otras dos resoluciones de distintas Audiencias Provinciales, que servirán para resumir la postura de la denominada "jurisprudencia menor", cuyo calificativo sirve para diferenciarla de la "mayor", es decir del Alto Tribunal, pero no por ello merece en modo alguno un valor significativo secundario en esta materia, a mi modo de entender.

Sin más preámbulo, entremos en el estudio de estas resoluciones judiciales.

3.1.- Sentencia de 18 de enero de 1993 del Tribunal Constitucional. (Sala Primera). Recurso de amparo número 1.100/1989, publicada en el B.O.E de fecha 12 de febrero de 1.993, siendo su ponente D. Rafael de Mendizabal Allende.

Este recurso lo interpone un militar contra un Auto del Tribunal Militar Central, en una cuestión de personal, ya que al residir éste en una localidad lejana a la sede de dicho Tribunal, pretendía que el expediente administrativo le fuera puesto en su disposición en su localidad, a través del Tribunal Militar de su Zona, para posibilitar así la interposición de la demanda, ya que en caso contrario le supondría indefensión.

Sin ánimo de entrar en el conjunto de las cuestiones y alegaciones, tanto fácticas como jurídicas que rodea este recurso, voy a centrarme en la parte del mismo que especialmente afecta a la utilización del *FAX* dentro del proceso, y para ello, paso a reproducir textualmente algunos de los párrafos contenidos en su fundamento jurídico segundo que no tienen desperdicio:

"Una vez desechados los obstáculos formales, quedan en pie las dos cuestiones que componen la sustancia de esta controversia, una la pertinencia de la petición para que las actuaciones fueran puestas de manifiesto en L.P., donde tiene su domicilio el demandante, y otro

la adecuación al caso de la caducidad declarada al mismo tiempo que se negaba aquella posibilidad...Así como en el procedimiento ordinario se entrega el expediente administrativo a las partes para formular la demanda y la contestación, dentro del procedimiento específico en materia de personal se le pone de manifiesto al demandante...el lugar de la actividad es la sede de la Sala y concretamente la oficina judicial o Secretaría, la Relatoría del Tribunal Militar Central en este caso.

Es evidente que la Ley tampoco prohibe cualquier otra solución al respecto y que las normas jurídicas han de ser interpretadas en el contexto social del tiempo en que hayan de ser aplicadas (Código Civil, art. 3.1), con el apoyo que brinda el progreso tecnológico...

Pues bien, esta perspectiva, nunca contemplada por el Tribunal Militar Central, al cual fue dirigido el interesado por una errónea notificación, converge con la estrictamente formal e instrumental, que afectaba al puro desarrollo del procesamiento....No lo hizo así el Central Militar en el momento de la admisión, ...ni luego cuando se le pidió que el expediente fuera puesto de manifiesto en L.P. Esta petición era razonable y atendible con el auxilio de los medios técnicos que se dispone en nuestros días. En una ponderación pragmática resulta evidentemente más fácil hacerlo así que exigir el desplazamiento del interesado...

Por otra parte, no sólo era posible la remisión del expediente original bajo custodia y con las garantías necesarias, sino que cabía la entrega por fotocopia autenticada, siguiendo el ejemplo que brinda el art. 790 de la Ley de Enjuiciamiento Criminal e incluso la utilización de otros medios de implantación reciente como el FAX, haciendo compatible la buena marcha del procedimiento y la flexibilidad adecuada para facilitar al interesado la defensa en juicio de sus derechos. La negativa de la Relatoría a hacerlo así no puede calificarse como razonable o proporcionada al caso, sino como rutinaria y apegada a la letra pequeña de la norma, sin transcender su significado, su función y, en definitiva, su finalidad..

En definitiva se menoscabó así y se hizo imposible la tutela judicial garantizada constitucionalmente, cuyo contenido normal es conseguir una resolución sobre el fondo, por cuya razón las causas de inadmisibilidad de la pretensión, con un sustrato formal, han de ser utilizadas con un criterio que evite la caída en el formalismo, perversión de la forma si ésta se entiende como garantía, que no otra que su finalidad y su función."

Difícilmente se podría comentar con palabras más certeras el criterio del Tribunal Constitucional en lo que significa el empleo de los medios técnicos como el *FAX* que sirven de instrumento para "**facilitar al interesado la defensa en juicio de sus derechos**", aunque no se encuentre expresamente previsto en

las normas de procedimiento, las cuales no deben entenderse literalmente o rigorísticamente, sino únicamente en su "finalidad y función".

Llamo la atención en este punto a lo que anteriormente, cuando estudiaba en el aspecto normativo de este tema el orden procesal contencioso-administrativo, me refería en los procesos de protección jurisdiccional de derechos fundamentales de las personas, respecto a la forma de cumplir con la urgencia de la remisión en el plazo de cinco días del expediente administrativo, ya que aunque afectando a un procedimiento distinto, como es el de "personal", considero igualmente aplicable a este supuesto en donde el *FAX* respondería a la misma ratio legis; es decir, que su utilización para remitir por el órgano administrativo del expediente, por las posibilidades de rapidez y celeridad en el tiempo, por supuesto dentro del breve plazo contemplado, serviría a la perfección para garantizar la tutela judicial efectiva de los interesados, y conjuntamente, "haciendo compatible con la buena marcha del procedimiento".

3.2.- Auto de la Sala de lo Social del Tribunal Supremo de fecha 20 de diciembre de 1.995.

En este supuesto, la Sala del Alto Tribunal contempla un caso real, y no meramente hipotético, de utilización del *FAX*, a diferencia del carácter hipotético de dicho uso previsto por el Tribunal Constitucional en el supuesto anterior.

Así el antecedente del recurso es el siguiente: Por un Auto de la Sala de lo Social del Tribunal Superior de Justicia de Castilla-León, se tuvo por no preparado en tiempo y forma un recurso de casación para la unificación de la doctrina, ya que la parte recurrente presentó el escrito de preparación de dicho recurso en la Sala de lo Social a través de *FAX*, sin que más tarde lo ratificará ni firmará el original por el Letrado suscribiente del mismo.

El Tribunal Supremo recoge la doctrina defendida en estos supuestos de escritos de preparación dentro del plazo por medio de *FAX*, en los siguientes términos, recogido en su fundamento jurídico segundo:

"El expresado medio de comunicación, aún cuando carezca de los requisitos de fehaciencia para producir los efectos que pretende, es "demostrativo" "prima facie" de la intención de la parte recurrente de preparar su recurso de casación por lo que ha de reconocérsele, por lo menos, la misma eficacia que el escrito que, sin firma de letrado, se presenta con tal

propósito y, en consecuencia, de acuerdo con el principio general establecido en el artículo 243 de la Ley Orgánica del Poder Judicial y con lo dispuesto en el art. 206.3 de la Ley de Procedimiento Laboral, la Sala debió, ántes de tener por no preparado el recurso, conceder a la parte el plazo a que dicho precepto se refiere para subsanar el defecto advertido."

En este sentido, y en su parte dispositivos, el Alto Tribunal acuerda estimar el recurso de queja interpuesto contra la resolución de la Sala de lo Social del Tribunal Superior de Justicia de Castilla-León y, de esa forma:

"conceder un plazo de diez días al recurrente para firmar el escrito de preparación del recurso remitido por FAX con el apercibimiento de tener por no presentado el recurso, continuando su trámite.".

Esta resolución judicial merece, en primer lugar, una llamada de atención al hecho de contemplar un supuesto concreto problemático de la utilización del *FAX*, como hemos visto, respecto a la presentación de escritodeformalización de recursos mediante este medio; pero sobre todo, y en segundo lugar, hay que destacar que si bien rechaza de plano que se deba inadmitir "prima facie", sin embargo tampoco acepta con plenitud de efectos jurídicos su admisión, sino que con un carácter ecléctico, y con analogía a los supuestos de escritos originales presentados por el conducto ordinario pero sin firma de Letrado, se considera que debe concederse un plazo para subsanar tal defecto y de ese modo su ratificación por el Letrado dentro de dicho término le otorgará plenitud de efectos.

Dicho de otro modo, el *FAX* como medio de presentación de escritos, sólo serviría de instrumento urgente para evitar una posible preclusión del plazo para presentar el recurso en cuestión, demostrando su intención de recurrir la resolución, pero con la salvedad de que el recurrente deba, en el plazo que se le conceda por el Tribunal, personarse en la Secretaría del mismo para ratificarlo y firmarlo, si quiere que se le tenga por legalmente interpuesto.

En pocas palabras, que el escrito por *FAX* sería **defectuoso** aunque no **inaceptable**, necesitado de **ratificación**.

3.3.- Auto de la Sección 3ª (penal) de la Audiencia Provincial de Málaga, de fecha 3 de mayo de 1.994.

Esta resolución de un tribunal "menor", que no por ello, merecedor de una inferior importancia, contempla otro supuesto de utilización del *FAX* dentro de la Administración de Justicia, a partir de los siguientes antecedentes:

El Juzgado de Instrucción número 2 de Estepona, valiéndose de las facultades que para notificación de resoluciones judiciales prevé el artículo 166 de la Ley de Enjuiciamiento Criminal, en un sentido amplio, notificó un Auto a una parte mediante *FAX*, lo que aparte de otras cuestiones es puesto en duda su validez por la parte recurrente, a lo que la Audiencia Provincial de Málaga niega su aserto, en el fundamento jurídico Unico, en su primer apartado, con los siguiente términos:

"La notificación realizada por FAX completada por la diligencia de constancia de 2-2-1994 a cargo del Secretario, haciendo constar la remisión de la copia del auto, el número de fax y la recepción por parte del destinatario, reúne todos los requisitos exigidos por el Art.166 Ley de Enjuiciamiento Criminal, cuando el hecho mismo de su emisión y su fidedigna recepción no se discute por la entidad notificada, es decir, se admite la eficacia del medio técnico utilizado por el órgano notificador.".

Por lo tanto nos encontramos con una de las escasísimas resoluciones judiciales que contempla el supuesto concreto de notificaciones por *FAX*, así como resume los requisitos necesarios para su validez, es decir, que se "haga constar el contenido de la resolución que se notifica, el número de *FAX* y la recepción del destinatario, bajo la fe del Secretario judicial, a través de la correspondiente diligencia de constancia".

A pesar de ello, y reconociéndose por la Audiencia su validez al reunir los requisitos del art. 166 de la Ley de Enjuiciamiento Criminal, hay que llamar la atención de que, en primer lugar, es un criterio judicial del todo respetable, pero que en modo alguno se puede afirmar que es compartido por la jurisprudencia en su conjunto, y que en segundo lugar, se apostilla un párrafo que me deja en la duda de la aceptación plena de dicho medio, ya que si en el caso contrario "el hecho mismo de su emisión y su fidedigna recepción se discutiera por la entidad notificada,...", entonces y a contrario sensu de lo razonado por dicho Tribunal, ¿se admitiría la eficacia del medio técnico utilizado por el órgano notificador?.

Entiendo que la plenitud de la **FE PUBLICA** del Secretario Judicial sería de igual valor, que si se hubiera utilizado el medio ordinario de notificación

de resoluciones judiciales contemplados en dicho art. 166, y por lo tanto, no debería haberse condicionado su aceptación por el destinatario a posteriori, una vez interpuesto el recurso, como requisito para conceder a tal notificación de plena eficacia.

A pesar de ello la importancia de este Auto en orden a la aceptación del *FAX* en el presente estudio no puede desconocerse, ya que por lo menos, se equipara en validez a las notificaciones por correo ordinario con acuse de recibo.

3.4.- Sentencia de la Audiencia Provincial (Civil) de Cuenca, de fecha 20 de Julio de 1996, ponente Sr. Vesteiro Pérez.

En este último supuesto se contempla de nuevo la posibilidad de presentación de escritos en un proceso judicial por alguna de las partes intervinientes en el procedimiento; en concreto se trataba de unos autos de juicios ejecutivo, en el que por la parte ejecutada, o demandada, formalizó la oposición a la demanda ejecutiva mediante escrito remitido al Juzgado de Primera Instancia por *FAX*, el cual no fue recibido en dicho Juzgado al no constar adecuadamente su recepción, ni por la parte recurrente haber probado o justificado su transmisión.

Sin ánimo de entrar en la cuestión procesal propia de la tramitación de los juicio ejecutivos en el orden civil, lo que no es objeto de este estudio, voy a reseñar el fundamento jurídico segundo de esta Sentencia en lo que respecta a la cuestión del *FAX*:

"Como enseña el Tribunal Constitucional, el derecho a la tutela judicial efectiva que proclama el art. 24.1 de la Constitución Española comprende la facultad de acceso a la actividad jurisdiccional y a obtener de los Jueces y Tribunales una resolución fundada y razonada en derecho sobre las pretensiones deducidas en juicio, a cuyo fin, por tratarse de un derecho de configuración legal, no se permite la fijación de obstáculos o trabas arbitrarias y caprichosas que obstaculicen aquella tutela; no obstante, obligados como están los Tribunales al cumplimento de los requisitos procesales, ningún criterio antiformalista autoriza a prescindir de las normas establecidas en las Leyes que ordenan el proceso y garantizan el derecho de todas las partes, debiendo ponderarse la entidad del defecto y su incidencia en la consecución de la finalidad perseguida, así como la voluntad y grado de diligencia procesal apreciada en la parte en orden al cumplimiento del requisito procesal omitido o irregularmente observado (STC 19 de diciembre de 1.994). En el caso presente, el recurrente afirma categóricamente que el ida..., y utilizando el medio de comunicación FAX-sistema admitido por el art. 271 LOPJ- remitió al

Juzgado de instancia el escrito de formalización de la oposición- escrito que en su forma original aparece unido a los folios 42 a 44 de las actuaciones y en el que aparece impreso un cajetín de entrada en el propio Juzgado de fecha...-, que no obstante no aparece en el pleito, ni se ha dado razón de su omisión, ante lo cual la Juzgadora a quo dictó la providencia de fecha... en la que, ante la inexistencia de oposición, ordenó traer los autos a la vista para dictar la obligada sentencia; esa falta de prueba de la realidad del FAX que se dice remitido desde Albacete en dicha fecha... impide estimar la oposición que el recurrente intenta...".

Dicho de un modo más asequible, que si bien los Tribunales de Justicia deben interpretar las normas legales de procedimiento de la forma más flexible posible para que se respete el acceso de todos a la Justicia, de reconocimiento constitucional en el art. 24 de la C.E, ello tampoco obliga a los Jueces estirar hasta lo imposible tal "flexibilidad" llegando a extremos de claro incumplimiento de los plazos y reglas establecidas en todos los procesos, y por ello, en este supuesto concreto, ante la falta de prueba por parte del recurrente de haberse efectivamente remitido el *FAX* que contenía el escrito de formalización de la oposición a la demanda ejecutiva, dentro del plazo establecido por Ley de cuatro días, y en cambio, sí existir un escrito original de dicha formalización de fecha posterior al término legal, todo ello conllevaría a las consecuencias jurídicas ya vistas en la anterior reseña judicial.

Por lo tanto, y a contrario sensu, si se hubiera acreditado fehacientemente tanto la remisión del *FAX*, su contenido, y su recepción por el Juzgado en cuestión, tal medio de presentación de escritos hubiera sido de aceptación por el mismo, lo que indudablemente merece un comentario muy positivo en esta parte del estudio.

Resumiendo esta breve síntesis jurisprudencial, podemos decir, que se observa una clara tendencia a la aceptación del *FAX*, tanto como medio de notificación de resoluciones como de presentación y remisión de escritos por las partes, aunque condicionado así en un caso como en otro, a que se acredite su remisión y recepción, con carácter fehaciente, es decir, mediante la debida constancia en autos bajo la fe pública judicial del Secretario Judicial; aunque si bien es cierto que es más fácil entrever que tal criterio es de mayor coincidencia por los Tribunales de Instancia, ya que en lo que respecta al Tribunal Supremo, es más escrupuloso con los medios ordinarios, por lo que se exigiría una ratificación posterior por el remitente, en el caso de los escritos de las partes.

4.- CONCLUSIONES PERSONALES.

La verdad es que como se habrá observado, a medida que he estudiado cada uno de los diferentes apartados de este estudio, he dejado sentado consideraciones particulares sobre cada aspecto en cuestión; sin embargo, y con el fin de resumir brevemente mi postura personal en este tema, voy a destacar las siguientes claves:

Primera.- La necesidad de los medios modernos de comunicación y transmisión de textos como es el *FAX*, es una realidad incuestionable, en un mundo como el actual.

Segunda.- La legislación procesal en este sentido aún es un poco atrasada, sin embargo, se observa una línea de clara aceptación de estos medios, siendo un magnífico ejemplo la redacción de la actual Ley de Procedimiento Laboral, en su Texto Refundido de 1.995.

Tercera.- De igual forma, la jurisprudencia, aunque también avanza poco a poco, teniendo en cuenta que se encuentra obligada, en la aplicación y solución de los casos, a la regulación legal que se encuentre vigente en cada momento, no por ello desconoce este tema, sino que viene aceptando en la fecha con regularidad la existencia del *FAX*, especialmente en orden a las notificaciones de resoluciones judiciales, siempre y cuando se acredite con exactitud en los autos, teniendo un papel primordial en este sentido la Fe Pública de los Secretarios Judiciales, que son, no nos olvidemos, los únicos depositarios de la misma en los términos recogidos en el art. 279 y siguientes de la Ley Orgánica del Poder Judicial.

Cuarta.- Y terminando, que en nuestra Constitución se reconoce en el artículo 24, en su primer apartado, "que todas las personas tienen derecho a obtener la tutela judicial efectiva de los jueces y tribunales en el ejercicio de sus derechos e intereses legítimos sin que, en ningún caso, pueda producirse indefensión", pero que asimismo, en su segundo apartado se observan dos concreciones concretas para la consecución de esta tutela judicial efectiva, a saber, por un lado, el derecho constitucional a "un proceso público sin dilaciones indebidas", en el que el *FAX* sería un buen instrumento para su realización, pero por otro lado, el derecho a que en ese proceso se guarden "todas las garantías", por lo que es necesario que se cumplan adecuadamente los requisitos que por la

jurisprudencia se exigen, en orden a lo ya observado por los dos casos concretos antes examinados, es decir, "constancia y recepción de todo aquello que se comunica o transmita por *FAX*.".

Notas acerca de la relación entre Informática y Propiedad Intelectual

GUILLERMO OROZCO PARDO

Profesor Titular del Departamento de Derecho Civil.
Universidad de Granada.

1- **Introducción.**

La informática es un fenómeno que posee múltiples facetas y diversidad de consecuencias de orden técnico, cultural y jurídico; ello quiere decir que estamos ante un importante fenómeno social cuyo estudio atañe a distintos campos del conocimiento humano. Es ya tradicional comparar la aparición de la informática con la invención de la imprenta lo cual, a nivel de ejemplo, es admisible, pero las consecuencias de todo orden que ha producido la informática superan, con mucho, las de esta. Uno de los efectos fundamentales que se asignan al ordenador es el de haber roto con la identificación de cada máquina con una función concreta y determinada, es decir, ese monólogo exclusivo entre una máquina y su utilidad o tarea única, ha sido superado por unos equipos que pueden asumir diversidad de funciones. No estamos ante una simple computadora que procesa información de forma automatizada, sino que nos dirigimos hacia aparición de equipos capaces de pensar y decidir que constituyen lo que se ha denominado "la informática decisional".[1]

■[1] Vid. Bretón, Ph.:" Historia y crítica de la informática". Trad. V. Villoria. Madrid, Cátedra, 1989 y "Revista de Occidente". "La mente y sus representaciones: cognición e inteligencia artificial". Número 119 de 1991.

Esto quiere decir que la capacidad de trabajo de los ordenadores aumenta progresivamente a un ritmo casi vertiginoso, tanto en lo que se refiere a la "potencia" de los equipos o sistemas, como en lo referido a las tareas que se les asignan. En consecuencia su importancia política y económica se ha multiplicado paralelamente ya que la "informatización" de la vida social es un fenómeno imparable y afecta a muy diversos aspectos de las relaciones sociales: reservar un billete de avión, retirar dinero de un cajero, diseñar un edificio o escribir un trabajo de investigación, son algunas de las múltiples tareas cotidianas que realizamos por medios informáticos. Ello ha conducido a una nueva y más peligrosa dependencia tecnológica ya que el mercado de la informática está "dominado" por unos cuantos países que producen y exportan equipos y programas a terceras naciones cuyo desarrollo depende en gran parte de la posibilidad de adquirir los nuevos productos capaces de realizar nuevas y más eficaces tareas.

En definitiva, estamos ante la que podemos calificar como gran innovación del siglo XX cuya verdadera proyección se manifestará en el siglo venidero. La informática ha propiciado, a nuestro juicio, un gran "salto cualitativo" en nuestra civilización muy superior en su alcance y consecuencias a cualquiera otro producido en la Historia de la humanidad.[2] Como afirma Bertrand, la conjunción de la informática y los modernos medios de comunicación ha provocado que entremos en una sociedad donde la información se ha constituido en una realidad independiente y un elemento básico que posee la misma importancia que el trabajo, la energía o las materias primas.[3]

■[2] Sobre el impacto de la Informática en el Derecho véase Pérez Luño, A.E.:" Nuevas tecnologías, Sociedad y Derecho". FUNDESCO, Madrid, 1987 y " Manual de informática y derecho". Ariel, Madrid, 1996.

■[3] Vid. " Le droit d'auteur et les droits voisins ". Masson, Paris, 1991. Este autor pone de manifiesto que en los Estados Unidos, para el principio de la década de los noventa, el sector de la informatización empleaba más del 50% de la mano de obra, frente al 25% de la industria tradicional o el 3% de la agricultura. La Unión Europea estima que hacia el año 2000, más del 80% de los empleos estarán ligados a las tecnologías de la información.

2- Derecho e Informática.

Hemos puesto de manifiesto cómo la informática afecta a las relaciones sociales planteando una variada gama de problemas que poseen trascendencia jurídica. Cuestiones tales como el tratamiento de la información relativa a datos personales, la comercialización de los productos informáticos, los delitos perpetrados por estos medios, las consecuencias de su aplicación en el ámbito laboral, la contratación electrónica o su aplicación en el campo administrativo y judicial, integran esa variada panoplia de manifestaciones de este fenómeno social ante las que el Derecho no puede quedar silente. Si entendemos al Derecho como un instrumento de coordinación ética de la vida social para ordenar la convivencia, podremos comprender la íntima vinculación que existe entre ambos pues es imprescindible asegurar la presencia de un "condicionante ético" en la aplicación de los medios informáticos a la vida social. El desafío que la Informática ha planteado al Derecho se ha caracterizado, hasta ahora, por dos notas muy marcadas: el "retraso" del Derecho con respecto a la evolución de aquella y la fragmentaria respuesta que se han dado a los distintos problemas. Efectivamente, tratamos de poner coto a la invasión de la privacidad de las personas por medio de la recogida y tratamiento de datos personales cuando ello ya se ha producido, lo cual pone de manifiesto la pervivencia del mito hegeliano del "búho de Minerva". De otro lado, al analizar esta problemática, los juristas se encuentran con un campo de estudio cuya jurisdicción científica no está claramente establecida. Aún hoy pervive la idea de que estos problemas afectan "transversalmente" a diferentes áreas según la cuestión a tratar: el Derecho Civil, Penal, Laboral, Procesal y Mercantil, son alguna de las disciplinas "implicadas" en la materia y, según la índole del problema, será una u otra la que posea la "jurisdicción" científica sobre el mismo. Esto origina un tratamiento fragmentario e incompleto de la problemática jurídica de la Informática, con las perniciosas consecuencias que de ello se derivan.

Actualmente, los juristas que estudian estas materias propugnan la necesidad de ordenar su estudio desde una perspectiva que unifique los principios, los métodos y las fuentes, para construir así una nueva disciplina científica que vendría a denominar "Derecho Informático o Derecho de la Informática", pues del mismo modo que otros fenómenos sociales, de menor

trascendencia, han conducido a la consagración de disciplinas autónomas, la Informática y sus múltiples efectos jurídicos demandan esa misma solución.[4] Sólo desde un análisis coherente basado en unos principios y métodos coordinados se podrá dar solución de la pluralidad de problemas que la Informática está planteando, y planteará, a la sociedad. Con ello estableceremos los cauces éticos por los que habrá de discurrir la evolución futura de una innovación muy beneficiosa pero que puede prestarse a abusos de muy variada índole.

3- La Informática y la Propiedad Intelectual.

Una de las dialécticas más interesantes que la materia plantea es la que se deduce de la relación entre la creación intelectual de productos informáticos y las normas que el Derecho ha arbitrado para proteger los derechos de sus autores. Como dice nuestro Legislador, la propiedad intelectual es un "supraconcepto" que engloba los derechos personales y patrimoniales que la Ley reconoce en exclusiva al autor sobre su obra. Con ello se asegura al creador toda una variada gama de posibilidades de actuación sobre las distintas vertientes de su obra, pues le permite adoptar toda una serie de "decisiones" con respecto al destino y explotación del objeto de su derecho. No obstante, hemos de tener muy presente la función social que cumplen las obras artísticas, literarias y científicas, razón por la cual son muy diversas las limitaciones que la Ley impone en este campo de actuación de la voluntad humana.

De otro lado, a nadie escapa hoy la relevante dimensión económica que estas obras poseen en muchos casos y que se acentúa en el campo de las creaciones de productos informáticos. Efectivamente, el "mercado de la cultura" forma parte de los sectores más dinámicos y crecientes de nuestros días. Ello se debe, entre otras razones, a la pluralidad de objetos en que puede plasmarse tal y como las leyes sobre la materia se encargan de reflejar con una encomiable visión de futuro. Libros, impresos, obras dramáticas, musicales, audiovisuales, fotografías, esculturas, mapas, proyectos, planos, etcétera, forman parte de ese versátil y flexible conjunto de obras originales "expresadas por cualquier medio o soporte, tangible o intangible, actualmente conocido o que se invente en el

[4] En nuestro país existe ya un digno ejemplo de sistematización científica de la disciplina en la obra de Davara Rodríguez, M.A.:" Derecho Informático". Aranzadi, Pamplona, 1993.

futuro", a las que la Ley protege atribuyendo a los autores la propiedad sobre las mismas.

Estamos pues ante una realidad material o inmaterial que es producto de la actividad creadora de la persona, plasmado en un soporte material o inmaterial que le hace perceptible, que aporta un "quid novi" al patrimonio artístico, literario o científico precedente y sobre el cual la Ley confiere una serie de derechos, "ab origine", a su autor. Tal protección se dispensa con independencia de factores como su valor o mérito, de su utilidad o de que se comunique públicamente o no. Como puede deducirse de la legislación sobre la materia, el campo de actividades humanas en las que pueden producirse obras protegidas es muy diverso, pues abarca desde las "tradicionales" como pintura, literatura, escultura, música, docencia, dramaturgia, cinematografía o fotografía, hasta otras propias de las ciencias empíricas o de la técnica como ingeniería, arquitectura, topografía o geografía.

Lógicamente, la Informática como campo de la actividad humana en la que se producen creaciones intelectuales, no podía quedar ajena a este fenómeno pues era necesario proteger los derechos de las personas y empresas dedicadas a la investigación y desarrollo de nuevos productos. Sin embargo, se planteaba el problema de que, inicialmente, los productos informáticos poseían una aplicación básicamente industrial o militar. Así lo afirma Bretón: "La segunda guerra mundial y la posterior guerra fría constituyeron sin ninguna duda el factor decisivo que permitió la invención del ordenador moderno y la entrada en la era de la informática. Todo lo relacionado con la carrera nuclear, la guerra y los imperativos de la defensa nacional, permitió el encuentro entre los sueños más avanzados de los mejores científicos y las amplias posibilidades de financiación y de experimentación que ofrecía la armada de un país altamente industrializado: los Estados Unidos. De esta conjunción nació el ordenador".[5]

En consecuencia, es lógico pensar que los primeros equipos tenían unas aplicaciones muy claras y determinadas por lo que se atendió a protegerlos atendiendo a su dimensión industrial, razón por la cual su tutela quedó adscrita al campo de las normas de la Propiedad Industrial. En principio, el centro de atención lo integraban los equipos ("Hardware") cuyo coste y limitaciones hacían

■[5] Vid. "Historia y crítica..."cit. página 117 y siguientes.

muy restringida su utilización a determinados ámbitos y tareas. Sin embargo, con la difusión de los ordenadores por su aplicación a otros distintos ámbitos de la actividad humana, se acentuó su capacidad multifuncional pues un mismo equipo podía ya realizar muy diversas tareas en función de las instrucciones que se le facilitaran. Emerge así la importancia de un nuevo elemento que permite adaptar el ordenador a muy diversos usuarios y destinos: los programas o soporte lógico ("Software"). [6] Ellos permiten que personas no preparadas específicamente para programar un ordenador puedan obtener de estos toda una diversidad de utilidades: laborales, de ocio y recreo, de comunicación y de tratamiento de información. He aquí pues un nuevo y relevante elemento, producto de la capacidad creadora del ser humano, que aporta nuevas metas y soluciones y que ha de ser protegido adecuadamente: el programa de ordenador.

Por otra parte, es de sobra conocido que nuestra época es conocida como la de la "sociedad de la información" dado que ésta se ha erigido como el más deseado instrumento de poder económico y político. Pero el problema no es sólo adquirir la información, sino saber sistematizarla y relacionarla adecuadamente según la finalidad perseguida. Ello quiere decir que no basta con almacenar información, sino que hemos de contar con un instrumento que permita al ordenador poder tratarla adecuadamente para las distintas finalidades que se puedan perseguir. La eficacia de una base de datos reside tanto en su capacidad de almacenar, cuanto en la posibilidad de tratar la información que contiene. Es por ello que las bases de datos poseen hoy tal relevancia que se hace necesario dotarlas también de protección jurídica adecuada en su faceta de objeto de propiedad intelectual.

Veamos seguidamente cuáles son las líneas maestras de esta tutela jurídica en nuestro Ordenamiento y en las normas comunitarias e internacionales. No obstante, dejamos fuera de este estudio la problemática de los productos

[6] "Hardware" es el término que hace referencia a los componentes físicos que configuran un sistema de ordenador. El "Software" es el soporte lógico que contiene las instrucciones y órdenes, es decir los programas, que se cursan al ordenador para que realice un determinado proceso. Puede ser "de base o sistema", integrado por el conjunto de programas que controlan y ordenan las funciones del sistema; de "utilidad", referido a diversos programas de utilidades; y de "usuario" o de aplicaciones. Vid. Actualidad Informática Aranzadi nº 1 de octubre de 1991.

semiconductores pues, por su propia naturaleza, quedan fuera del objeto de nuestro estudio.

4- La protección de los programas de ordenador en nuestro Ordenamiento.

A) Su régimen jurídico.

Una de las primeras dificultades con la que nos encontrábamos al abordar la materia, era la fragmentación de esta normativa que se ponía de manifiesto en la existencia de una panoplia variada de normas aplicables, que perduró hasta la aparición del tantas veces prometido Texto Refundido de la Ley de Propiedad Intelectual aprobado por el R.D. Legislativo 1/1996 de 12 de Abril. Sintetizando mucho la cuestión, podemos decir que existían unas normas especiales, que conformaban un régimen especifico, y otras generales, que integraban el substrato básico. De entre esas normas asumidas por la actual Ley cabe citar:

- La Ley de Propiedad Intelectual de 1987, sobre todo los artículos 95 a 100, como normas especiales, y demás preceptos aplicables de la misma, en cuanto régimen general aplicable al programa como obra literaria.

- El Reglamento del Registro General de la Propiedad Intelectual de 14 de Mayo de 1993.

- La ley de 23 de Diciembre de 1993 que incorporó la Directiva 91/250/CEE, sobre protección jurídica de programas de ordenador, como norma especial.

- La Ley de 30 de Diciembre de 1994 que incorporó la Directiva 92/100/CEE sobre derechos de alquiler y préstamo y otros derechos afines a los derechos de autor en el ámbito de la propiedad intelectual.

- la Ley de 11 de Octubre de 1995 de incorporación de la Directiva 93/98/CEE relativa a la armonización del plazo de protección del derecho de autor y determinados derechos afines.

De esta amplia panoplia de normas se deducía ya la importancia que los programas de ordenador poseían para el Derecho en cuanto objeto del tráfico jurídico económico, lo cual hacía más necesario que se unificara definitivamente su tratamiento legal, pues esta fragmentación podía ocasionar disfunciones

perjudiciales para la eficacia de su tutela legal, tal y como venia denunciando la Doctrina. Para asumir esta normativa dispersa sobre Propiedad Intelectual, en los diversos campos de la materia, surge el Real Decreto Legislativo antes citado, que se elabora como anexo al Texto Refundido de la Ley de Propiedad Intelectual, con una finalidad expresa que anuncia su artículo único: "*Se aprueba el texto refundido de la Ley de Propiedad Intelectual, regularizando, aclarando y armonizando las disposiciones legales vigentes sobre la materia, que figura como anexo al presente Real Decreto Legislativo* ".

La entrada en vigor de esta norma, el martes 23 de abril de 1996, supuso la derogación, en su mayor parte, de la panoplia normativa antes relacionada, excepto en lo relativo al Registro de la Propiedad Intelectual, según establece su disposición derogatoria única. No obstante, junto a esta norma especial hemos de atender a otras normas generales o especiales que regulan aspectos relacionados con esa protección. Tal sería el caso de textos como el Código Penal, el Código Civil o las leyes procesales, cuando sean aplicables al supuesto planteado.[7] Esta contingencia estaba expresamente prevista en la disposición adicional única de la Ley 16/93 que establecía: "Lo dispuesto en la presente Ley se entenderá sin perjuicio de cualesquiera otras disposiciones legales tales como las relativas a los derechos de patente, marcas, competencia desleal, secretos comerciales, protección de productos semiconductores o derecho de obligaciones".

■[7] Así lo prevé el mismo Texto refundido cuando acepta la aplicación del sistema de Derecho transitorio del Código civil, según establece su disposición transitoria decimocuarta. El Código Penal trata los delitos contra la propiedad intelectual en su artículos 270 y siguientes, junto a los relativos a la propiedad industrial, al mercado y a los consumidores, lo cual entraña un posicionamiento "patrimonialista" en el "espíritu" de la norma, si bien la interconexión de las materias es evidente, sobre todo en los programas de ordenador. En concreto, el último párrafo del artículo 270 prevé el castigo con la pena de prisión de 6 meses a 2 años o de multa de 6 a 24 meses para quienes lleven a cabo ".. la fabricación, puesta en circulación y tenencia de cualquier medio específicamente destinado a facilitar la supresión no autorizada o la neutralización de cualquier dispositivo técnico que se haya utilizado para proteger programas de ordenador ". El artículo 272.1 C.P. remite a la misma Ley de Propiedad Intelectual para establecer el alcance de la responsabilidad civil derivada de estos delitos.

B) El programa de ordenador como objeto del derecho de propiedad intelectual.

Ya hemos aludido antes a la flexibilidad y visión de futuro que nuestra Ley de Propiedad Intelectual (LPI) consagra a la hora de definir el objeto de este derecho. En su artículo 10 recoge una definición genérica y elástica:"... todas las creaciones originales literarias, artísticas o científicas expresadas por cualquier medio o soporte, tangible o intangible, actualmente conocido o que se invente en el futuro". Sentado esto, a continuación hace una enumeración abierta dentro de la cual cita expresamente a los programas de ordenador en apartado 1.i) del precitado artículo.

Hemos de recordar que el Convenio de Berna consagra ya a los programas de ordenador como obras literarias y debe atenderse a su protección siguiendo esta premisa inicial. Siguiendo esta línea general, podemos citar el texto del artículo 4 del Proyecto de Tratado sobre ciertas cuestiones relativas a la protección de las obras literarias y artísticas (OMPI, 1996) a cuyo tenor " los programas de ordenador están protegidos como obras literarias en el marco de lo dispuesto en el artículo 2 del Convenio de Berna. Dicha protección se aplica a las expresiones, en cualquier forma, de un programa de ordenador".(cfr. art 10 del Acuerdo sobre los ADPIC)

En tal sentido, el artículo 1.1° de la Ley 16/93 de 23 de Diciembre estableció expresamente que "los programas de ordenador serán protegidos mediante los derechos de autor como obras literarias, tal como se definen en el Convenio de Berna para la protección de las obras literarias y artísticas". Esta misma línea se mantiene en el Texto Refundido, cuya disposición derogatoria establece la derogación de todas las disposiciones que se opongan a lo establecido en esta Ley, razón por la cual no cabe ya la menor duda de que el programa es una obra literaria más de las protegidas por la Ley, sin que quepan interpretaciones restrictivas a la hora de aplicarle la tutela legal.

El programa en cuanto bien susceptible de protección legal es un fenómeno reciente, razón por la cual inicialmente se le protegía mediante una vía indirecta. Toda vez que normalmente se adquiría unido al equipo al que servía en régimen de accesoriedad como sistema operativo, su tutela se operaba mediante la aplicación de las normas de la propiedad industrial en la medida en que ello era posible. En consecuencia, la adquisición de programas se realizaba mediante un

contrato "accesorio" de venta de "software". Sin embargo, el auge del mercado de programas y su "independencia" del equipo demandaron la necesidad de brindarle una protección autónoma pues su adquisición no siempre va unida al equipo ya que actualmente los programas pueden cubrir muy diversos campos de aplicación, y tal vez por ello la contratación de "software" sea hoy un fenómeno de contratación conexa o coligada, sin aquél matiz de accesoriedad antes citado.[8]

Hoy está plenamente superada la duda de si se debió optar por regular esta materia en el campo de la propiedad industrial, pues dadas las características de los programas es lo más lógico y práctico incluirles dentro de las normas que protegen a la propiedad intelectual, ya que su dimensión industrial no es generalizada y presenta aspectos "personalistas" no previstos en la propiedad industrial. De otro lado, el dotarle de una normativa "sui géneris" habría debilitado su protección. Por tanto, lo más operativo era incluirle dentro de las normas de la propiedad intelectual y así lo concluye Galán Corona cuando afirma:" En cualquier caso, está fuera de toda duda la opción adoptada y ciertamente existen sólidas razones pragmáticas para ello. Por una parte, la protección que confiere el derecho de autor presenta indudables ventajas: no se requiere novedad ni actividad inventiva, sino solamente originalidad y tampoco es preciso registro conforme a la Convención de Berna. Todo ello supone una protección inmediata, barata y geográficamente generalizada, gracias al juego de los Convenios internacionales sobre la materia".[9]

Estas razones de orden pragmático son incuestionables si reparamos en el aumento de la llamada "piratería informática" que conlleva la copia y comercialización de programas ilícitamente obtenidos. Este fenómeno no sólo

■[8] Davara considera que este tratamiento diferenciado tiene su origen en la práctica de IBM de facturar independientemente los equipos de los programas a causa de las imposiciones legales en USA, para evitar monopolios que falsearan la competencia. Vid. "Derecho Informático".cit. página 107. Sobre el tema de los contratos conexos véase la obra de López Frias, A."Los contratos conexos "Barcelona, 1994, donde se hace un profundo estudio de esta materia y, en concreto, las páginas 233 y siguientes; véanse también A.A.V.V.: "Les contrats de dévelopement de logiciel sur mesure 2. Bruselas, 1986 y A.A.V.V.: "I contratti di utilizzazione del computer ". Dir. G.Alpa. 1984

■[9] Vid. "Comentarios al Código Civil y Compilaciones Forales". Dir. M. Albaladejo y S. Díaz Alabart. Madrid, EDERSA, 1995. Tomo V, vol. 4° B, donde hace un extenso análisis sobre la materia.

supone pérdidas económicas para los autores, sino que sus consecuencias perniciosas se proyectan sobre toda la comunidad.[10]

Ya hemos aludido antes a la creciente importancia de la industria del "software" y a su papel "estratégico" a nivel político. [11] Los estados más desarrollados tratan de fomentar la industria de este campo incentivando la creatividad, de manera que la "piratería" supone un grave quebranto para la industria y la economía de los países productores de programas para ordenador, pues supone menores exportaciones, disminución de empleo y competencia desleal. La necesidad de hacer frente a este problema impuso la política de coordinar las medidas legales de protección a la vez que la aplicación de la doctrina de la reciprocidad: sólo los países que disponen de una protección legal adecuada tienen acceso lícitamente al intercambio del "software". Prueba de todo ello son los textos internacionales suscritos por los Estados y los que la Unión Europea ha dictado para armonizar la protección de estos derechos en el seno de sus Estados miembros.

No obstante, siguen existiendo casos en los que un programa va ligado a un proceso industrial, en cuyo caso se le brinda una protección complementaria. Así lo recoge el artículo 96.3 LPI: "Cuando los programas de ordenador formen parte de una patente o un modelo de utilidad gozarán, sin perjuicio de lo dispuesto en la presente Ley, de la protección que pudiera corresponderles por aplicación del régimen jurídico de la propiedad industrial ".

■[10] Paralelamente al auge de este mercado, se ha producido un aumento de la "piratería" en dicho sector, tal y como lo demuestra el hecho de que en nuestro país sólo 12% de los programas de ordenador estándar utilizados es legal. Ello quiere decir que el 88% restante se está utilizando de manera fraudulenta por vía de comercialización ilegal y copias indiscriminadas. Ello ha significado unas pérdidas en el sector, sólo para el año 1994, de 100.000 millones de pesetas. En 1996, las pérdidas globales se cifran en 11.200 millones de dólares (1'5 billones de pesetas) y los fabricantes españoles perdieron a causa de la piratería, en este mismo año, 22.000 millones de pesetas. Lo que se ha traducido, además, en pérdida de empleo y productividad. Vid. "La campaña contra la piratería informática", en Actualidad Informática Aranzadi, nº 15 de abril de 1995. Véase también la revista "Despacho de abogados". nº 6 de 1995, donde se afirma que España ocupa el segundo lugar en cuanto a utilización ilegal de "software".

■[11] Véanse los datos que aporta Racicot sobre la magnitud económica del mercado del "software" en: "Software protection". En: "L'informatique et le droit d'auteur". Ed. Y. Blais Inc. Montreal, 1990.

A la hora de definir un concepto podemos entender el "Software", según afirma Davara, como "el soporte lógico de las instrucciones y órdenes que forman los programas que se dan a un ordenador para que realice un proceso".[12] Nuestro Legislador ha definido con claridad, en al artículo 96.1, cual es el concepto de programa como bien protegido por la Ley: "toda secuencia de instrucciones o indicaciones destinadas a ser utilizadas, directa o indirectamente, en un sistema informático para realizar una función o una tarea o para obtener un resultado determinado, cualquiera que fuere su forma de expresión y fijación". Es decir, el programa es una creación intelectual integrada por un conjunto de instrucciones que se dirigen al ordenador para que éste realice una tarea u obtenga un resultado, siendo así que se le compara con una "partitura" que el ordenador lee y ejecuta. Estamos ante un elemento instrumental que dirige y da sentido a la "tarea" que se asigna a la máquina y posibilita la obtención de un resultado; en razón de ello no podemos admitir que se la vincule al ordenador mediante un criterio de accesoriedad, toda vez que posee su propia entidad independiente de la máquina quien, realmente, "depende" del programa para realizar adecuadamente su función.

Así concebido, el programa es una expresión autónoma del pensamiento creativo de su autor, que una vez plasmado en un soporte suficiente sirve para que el ordenador realice una tarea prevista. Edelman lo define como el conjunto de secuencias de instrucción que permiten hacer realizar una función determinada a una máquina de tratamiento de información llamada ordenador.[13]

Estamos ante uno de los llamados "bienes inmateriales", concepto que la Doctrina científica actual utiliza para referirse a un conjunto de bienes que comportan creaciones humanas que mediante su plasmación en un medio o soporte son susceptibles de percepción, aprovechamiento o utilización por los destinatarios o usuarios. De entre sus características, nosotros queremos destacar su "fragilidad esencial" y su "relevancia económica", pues su importancia como

■[12] Vid. " Introducción a la informática".Revista Actualidad Informática Aranzadi, nº 1 de 1991.

■[13] Vid. "Actualité Législative Dalloz". Número especial de 1987.

bienes de consumo o explotación económica corre paralela a la facilidad para copiarlos u obtener ilícitamente ejemplares de los mismos.[14]

Racicot explica el proceso de creación del programa que parte de la idea de su autor de lograr la solución a un problema o de cumplir una función. En esta primera fase se establecen los objetivos, se definen los problemas y se determinan las especificaciones funcionales. En la siguiente fase, la obra se segrega en módulos que a su vez se subdividen y se determinan las relaciones y los "interfaces" entre componentes (interfaz es un dispositivo físico o lógico que permite establecer la conexión facilitando el intercambio de información entre dos equipos o entre equipo y usuario). Todas estas fases conforman la etapa de "arquitectura del programa".

A continuación, el autor establece cuál ha de ser el método de resolución del problema, siendo esta segunda etapa la de la lógica o algoritmo del programa en la cual se pueden utilizar los ordinogramas donde la lógica del programa es descrita gráficamente por unidades interrelacionadas que desarrollan las diferentes etapas y los flujos de datos. Seguidamente, el autor elige, si no lo ha hecho ya, el lenguaje de programación y codifica el programa en ese lenguaje mediante una serie de instrucciones. Este es el programa fuente. Este lenguaje, que recuerda vagamente al humano, sólo puede ser comprensible por un informático y el propio ordenador. En consecuencia, el programa en lenguaje fuente ha de ser traducido a lenguaje objeto para que se adapte al ordenador. Este suele ser un lenguaje binario formado por una serie de ceros y unos, o por un lenguaje hexadecimal formado por la combinación de números y letras. Las series de unidades de tales códigos se representan en el ordenador en dos estados: existencia o ausencia de corriente eléctrica o bien alto o bajo voltaje de corriente.

Este programa traducido a lenguaje objeto se plasma o fija en un soporte material fijo (tarjeta, papel, cinta) mediante la presencia de agujeros, perforaciones o espacios. Este soporte puede ya ser "leído" por una fuente luminosa o eléctrica que envía las señales a la memoria interna del ordenador. Este sistema es similar en los casos en que se fija el programa en un disco o circuito impreso, aunque en

■[14] Vid. Chateau,B.: "L'evolution de la propiété litteraire et artistique". En: "L'evolution contemporaine du Droit des biens". París, 1991. Así mismo, Galán Corona en: "Comentarios...". cit. página 218 y siguientes.

este caso los agujeros o perforaciones se sustituyen por la presencia o ausencia de una carga magnética.

He aquí la realidad material o soporte físico del bien inmaterial llamado programa de ordenador, que sirve para plasmar y hacer perceptible la obra creada por su autor. Se entiende más fácilmente si empleamos la distinción que hace Baylos entre el programa fuente constituido por la formulación de las instrucciones a través de enunciados representados por signos escritos, símbolos, diseños y ordinogramas; y el programa objeto que supone su traducción a tablas numéricas y a elementos electromagnéticos que operan sobre el ordenador y que se plasma en distintos soportes: discos, cintas o memoria.[15]

Cuando el programa ha sido terminado se realizan las fases de prueba y control y se elabora la documentación que le acompaña y como ya es un objeto material susceptible de explotación se inscribe en el Registro. Nuestra Ley extiende su protección tanto al programa fuente, como al programa objeto y a la documentación técnica y manuales de uso que le acompañan. Ello se justifica, según Baylos, porque el programa fuente supone "la transformación de un soporte integrado por signos semánticos en otro soporte por señales electromagnéticas combinadas en forma que realizan la concepción de los creadores del programa". Y ello teniendo en cuenta además que ambas versiones son intercambiables ya que pueden obtenerse por medio de mecanismos automáticos de reversión.[16]

En conclusión, la concepción del programa como objeto de tutela por las normas de propiedad intelectual que mantiene nuestra Ley es muy amplia pues se extiende a diversas posibilidades, ya sean programas operativos, de aplicación o usuario y a la documentación auxiliar. Así lo ha expresado la sentencia de la A.P. de Madrid, sección 13ª, de 12 de Mayo de 1992: "La legislación española en cuestión de la protección de las obras consistentes en programas de ordenadores ha adoptado un carácter amplio y extensivo, como se desprende del artículo 96 de

■15 Vid. Racicot: op.cit. loc.cit.

■16 Vid. "Tratado de derecho Industrial". Cívitas, Madrid, 2ª edición de 1993. También Paz Soler": Una aproximación a la terminología básica en materia de programas de ordenador". RGDº de 1992.

la LPI". Una vez que el programa reúne los requisitos de licitud, forma suficiente y originalidad, se considera protegida como obra literaria y su autor adquiere los derechos que a su estatuto confiere la Ley.

Así lo sancionaba ya el artículo 1 de la Ley 16/93 que exigía que el programa fuera una obra original producto de la creación intelectual, aplicando esta protección "a cualquier forma de expresión de un programa de ordenador, salvo aquellas creadas con el fin de crear efectos nocivos a un sistema informático. Las ideas y principios en los que se basa cualquiera de los elementos de un programa de ordenador, incluidos los que sirven de fundamento a sus interfaces, no estarán protegidos mediante los derechos de autor con arreglo a la presente Ley".

Todo ello ha sido asumido por la actual Ley toda vez que reconoce estos elementos esenciales de la obra intelectual llamada programa de ordenador (v.gr. creatividad y originalidad) como condicionantes para reconocerlo como objeto autónomo digno de protección legal. Ello se deduce de lo establecido en al artículo 96.2 cuando afirma: "El programa de ordenador será protegido únicamente si fuese original, en el sentido de ser una creación intelectual propia de su autor". Siguiendo las líneas directrices de la materia, la LPI protege "cualquier forma de expresión de expresión de un programa de ordenador" (art. 96.3) sin vincular la obra al soporte "natural" como objeto protegido, tal y como sucede con una obra literaria o musical. Igualmente, se protegen las versiones sucesivas y los programas derivados, exceptuando aquellas que se crean con la finalidad ¿exclusiva? de ocasionar efectos nocivos a un sistema informático. Esto supone que en el caso de los programas la licitud se convierte en un requisito esencial para reconocer al programa como obra protegida, lo cual no está tan claro en otras obras recogidas en la Ley.

Dentro de esta misma tónica general avanzada por la Directiva y su Ley de transposición, se excluyen de la protección las ideas y principios en los que se

basan los elementos de un programa (algoritmos, etc...) incluídos los que sirven de fundamento a sus interfaces.(art.96.4)[17]

C) El régimen legal a partir de la Ley de Propiedad Intelectual y su legislación complementaria.

Ya hemos hecho alusión a la panoplia de normas que nuestro Ordenamiento contenía en relación con la materia que nos ocupa y, si bien se ha "aclarado" en parte por el papel que juega el texto refundido, podemos afirmar que el régimen jurídico de la propiedad intelectual no se agota con la Ley especial pues siguen existiendo normas generales y específicas de obligatoria aplicación, ya sea de forma directa y específica o por remisión a instituciones generales aplicables al caso; basta para ello con leer el párrafo segundo de la disposición derogatoria única. Partiendo del "eje central" del sistema, la Ley de Propiedad Intelectual, nos encontramos con el hecho de que la deficiente redacción de su artículo 95 que, cuando menos, puede inducir a error": El derecho de autor sobre los programas de ordenador se regirá por los preceptos del presente Título y, en lo que no esté específicamente previsto en el mismo, por las disposiciones que resulten aplicables de la presente Ley". Haciendo una "rígida" interpretación literal de este precepto podríamos concluir que el régimen general que regula a los programas de ordenador sería el establecido en el Título VII, siendo supletorio y complementario el resto de la Ley. No hemos de olvidar el criterio interpretativo que sostiene que la norma especial o excepcional se aplica con preferencia a la general. Pero a nuestro juicio, que venimos manteniendo desde que se dictó la Ley en 1987, la interpretación del artículo 95 LPI es otra: el régimen general aplicable a los programas, como obras literarias que según el Convenio de Berna, es el mismo que se aplica a éstas, es decir el régimen general establecido en el Libro I de la Ley, salvo determinadas normas específicas establecidas en el Título VII y leyes especiales complementarias en atención a ciertas características especificas de los programas.[18] Este espíritu preside, a nuestro entender, al Texto

■[17] Ello es lógico en cuanto que no cabe un "monopolio" sobre las ideas o conceptos básicos en que se basan las creaciones intelectuales, ya que nadie puede pretender "apropiarse" de las palabras, las letras, las cifras o las notas musicales. Vid. Orozco Pardo,G.": Acerca de la protección de las ideas por el derecho de autor". Rev. Actualidad Civil, nº 12 de 1993.

■[18] Vid. Dietz,A: "El derecho de autor en España y Portugal". Trad. López Sáez, Mº Cultura, Madrid, 1992. Delgado Echeverría,J.: "Comentarios a la Ley de Propiedad Intelectual". Dir. Bercovitz, Técnos, Madrid, 1989 y Galán Corona: "Comentarios...". cit. página 231.

refundido pues atiende a las mismas condicionantes básicas de originalidad y creatividad para reconocer a un programa como obra, aunque exige "funcionalidad lícita" para desplegar su protección, tal y como antes vimos, si bien se ha perdido una excelente ocasión para mejorar el texto del artículo 95.

Es indudable que el autor de los programas ha de poseer el mismo estatuto jurídico que le asegure igual protección que el resto de los autores. En consecuencia, es titular de las facultades contenidas en el derecho moral, del artículo 14 LPI, de los derechos de explotación, de los artículos 17 y siguientes del mismo texto legal, aunque con ciertas matizaciones que luego veremos, y de los medios de protección establecidos en la Ley. Así lo disponían ya los artículos 2 y 3 de la Ley 16/93 que aseguraban la protección a todas las personas físicas que hubieran creado el programa o a la persona jurídica que sea contemplada como titular de los derechos según los casos previstos en la LPI. Este criterio ha sido asumido por la actual Ley en su artículo 97, donde se prevé la titularidad de las personas físicas o jurídicas, así como la posibilidad de que se creen programas como obras colectivas o en colaboración, en sintonía con lo establecido en los artículos 5 a 9 de su Título Primero. No obstante, el Título VII no alude a la obra "compuesta" del artículo 9 que es aquella obra nueva que incorpora otra preexistente, sin la colaboración del autor de esta última, lo cual estimamos posible en el campo de la informática en cuanto a programas que contienen obras de otros autores y que deben contar con la respectiva autorización de estos.

No obstante, caben ciertas modificaciones de ese régimen adaptadas a las especiales características de los programas. Tal sucede con determinados preceptos que no serían aplicables al caso de entre los cuales destacamos:

- Las normas del Libro II de la Ley, relativas a los derechos conexos.

- El derecho de acceso al ejemplar único del artículo 14.7.

- El cómputo del plazo de protección para obras publicadas por partes, del artículo 29.

- La reproducción en Braille, del artículo 31.3.

- La parodia, del artículo 39.

- Lo establecido en el artículo 43 LPI sobre la transmisión "inter vivos" de los derechos de explotación.

- La publicidad registral en todo su alcance, según el artículo 32 del Reglamento del Registro General de la Propiedad Intelectual en conexión con el 101 de la Ley, para evitar que el registro sirva indirectamente de fuente para la defraudación de estos derechos.[19]

- La participación en la remuneración compensatoria por copia privada del artículo 25, cuyo párrafo tercero que excluye expresamente a los programas de ordenador.(ex Ley 43/94 de 30 de Diciembre) Esto no parece tan claro en la medida en que los ordenadores, sobre todo los personales, son un instrumento muy utilizado para realizar copias no autorizadas de programas, sobre todo ahora cuando los lectores de discos compactos (CDROM) permiten grabar en estos soportes y tienen un precio muy asequible.

En general, se excluyen todos aquellos preceptos que sean relativos a aspectos o contenidos que no se prediquen del programa de ordenador, ni aún considerado como una obra literaria.

Más dudosas son otras normas como las relativas a la participación en el precio de reventa de obra plástica cuando se trata de obras creadas por ordenador, del artículo 24 o la autorización legal para la reproducción de obras por bibliotecas del artículo 37 LPI.

Del Título VII podemos deducir algunas especialidades interesantes a destacar:

- A los efectos previstos en la Ley, la expresión "programas de ordenador" comprende también su documentación preparatoria.(96.1 LPI)

■[19] El problema se ha creado toda vez que no están claros cuáles son aquellos elemtos susceptibles de consulta que menciona el artículo 101 L.P.I. Actualmente, se inscribe el programa con el modelo B-7, que contiene ciertas partes criticables, presentando, por parte de los solicitantes, la totalidad del código fuente del programa en papel lo que representa, en muchos casos, un volumen considerable de folios, tiempo y dinero, lo que puede surtir efectos "disuasorios" indeseables en un sector tan necesitado de protección.

- La compatibilidad de la protección por vía de la propiedad intelectual para los programas que formen parte de una patente o modelo de utilidad a la que aludimos en páginas precedentes. Ello se debe a que el programa puede conciliar perfectamente sus facetas como obra intelectual e instrumento industrial, a la vez que las lesiones a estos derechos pueden provenir de ambos cauces.(art.96.3 LPI)

- La protección se extiende a la documentación técnica y manuales de uso.((96.1 LPI)

- Se consideran protegidos también las versiones sucesivas y los programas derivados, salvo los creados con finalidades lesivas.(96.3 LPI)

- Cuando el programa se crea en el marco de una relación jurídica de carácter laboral, actuando el autor en ejercicio de las funciones que le han sido confiadas o siguiendo instrucciones de su empresario, la titularidad de los derechos económicos, tanto del programa fuente como del programa objeto, corresponden exclusivamente al empresario, salvo pacto en contrario. (ex art.2.4 Ley 16/93 de 23 de Diciembre, recogido en los artículos 51.5 y 97.4 LPI). Esta atribución legal supone una importante excepción al principio general según el cual, en actos "inter vivos", no se transmiten más derechos de explotación sobre la obra al cesionario que los expresamente pactados.(Cfr.arts 43 y siguientes LPI) Con ello se da prioridad a los intereses empresariales, frente a los de los trabajadores en aras, tal vez, de fomentar la inversión de las empresas en el campo de la creatividad del "software" y de su industria.

Hemos de recordar que el artículo 43.5 de la Ley prevé que la transmisión de estos derechos no alcanza a las modalidades de utilización o medios de difusión inexistentes o desconocidos al tiempo de la cesión. No obstante, aunque la Ley no presume una cesión, sino que establece una atribución directa al empresario, adquisición originaria, merced a que es quien aporta los medios y las instrucciones para realizar el programa, cabe pensar en la posibilidad de aplicarle esta restricción. Desde luego, hemos de atenernos a lo previsto en el contrato, donde puede haber pacto en contrario, y pensar que lo establecido en el artículo 51 LPI es también aplicable como limites a esta atribución presunta: se atribuyen con el alcance para el ejercicio de la actividad habitual del empresario en el momento de entrega de la obra realizada en virtud de esa relación laboral, este no puede utilizar o disponer de ella para un sentido o fin diferente a lo establecido en los párrafos anteriores. Y ello porque la remisión que hace el párrafo 5 del

artículo 51 no permite pensar que su texto no pueda ser aplicado al programa en lo que no sea contrario a las normas del Titulo VII, ya que el 97.4 nada dice en cuanto a ello. Esta precisión es similar a la establecida por el artículo 110 LPI en favor de los artistas, interpretes o ejecutantes.

Desde luego los derechos morales del creador corresponden a éste, aunque en caso de conflicto con los del empresario, deberemos atender a la prioridad de aquellos. Tal sería el caso de la prohibición al trabajador de crear otros programas en el futuro que puedan competir con el que explota el empresario, pues se produce un conflicto entre el derecho de creación intelectual (art.20.1-B CE) que se vierte en el artículo 43.4 LPI que decreta la nulidad de las estipulaciones por las que el autor se compromete a no crear obras en el futuro, y el deber de no competir dimanante del principio de buena fe contractual. [20]

Finalmente, el artículo 97.5 impone una condición para dispensar esta tutela: que los pretendidos titulares cumplan con los requisitos establecidos en la Ley para la protección de los derechos de autor y que se predican de la obra y los sujetos.

- En cuanto al programa creado merced a un contrato de obra la Ley no hace una regulación expresa, razón por la cual habremos de acudir al Código civil y aplicar los principios generales relativos a este contrato. En consecuencia, sino se ha pactado la cesión de estos derechos de explotación, pertenecerán al autor del programa. Así lo sancionó el Tribunal Supremo en la sentencia de 12 de Diciembre de 1988: "La prestación de técnicas informáticas no tiene, necesariamente, una calificación uniforme, puesto que puede consistir en un contrato de actividad, asimilable al arrendamiento de servicios o de resultado, dentro del concepto genérico de arrendamiento de obra y puede concertarse la concesión de la propiedad de los programas". En razón de ello, no admite que la cesión sea automática porque se pueda considerar una "consecuencia natural del contrato", sino que alcanza sólo a los objetos confeccionados según esa

[20] Vid. González de Patto, R.Mª:" Especialidades en el régimen jurídico de la protección cuando el autor del programa de ordenador es un trabajador asalariado". Actas del II Congreso Iberoamericano de Informática y Derecho. Guatemala, 1989 y Galán Corona "Comentarios..." cit. pág. 258 y sig.

disposición, porque la transmisión de la propiedad depende de lo pactado en cada caso.(Cfr. A.P. Madrid, sección 13ª, de 12 de Mayo de 1992)[21]

En el caso de que el titular sea una persona jurídica, según lo previsto en el artículo 97, la duración de la protección será de 70 años computados desde el día 1 de enero del año siguiente a la divulgación lícita del programa o al de su creación, si no se hubiese divulgado. En caso de ser una persona física, se mantiene el criterio general establecido en el artículo 26 de la Ley: vida del autor y 70 años "post morten".(art.98 LPI)

- Cuando se produce la cesión del derecho de uso se presume, salvo prueba en contrario, que se hace de forma no exclusiva e intransferible y únicamente para satisfacer las necesidades del usuario. Ello permite a éste utilizar el programa, conservando el cedente la propiedad del mismo, pero sólo en la medida en que es preciso atendiendo a las necesidades del usuario.(art.99 final LPI) Según este mismo precepto, la primera venta en la Unión Europea de una copia de un programa por el titular de los derechos o con su consentimiento, agotará el derecho de distribución de dicha copia, salvo el derecho de controlar el subsiguiente alquiler del programa de una copia del mismo.

- El derecho de reproducción, que faculta para fijar la obra en un medio que permite su comunicación al público y la obtención de copias, está recogido en el artículo 99.a de la Ley. A tenor de este, la reproducción del programa, incluso para uso personal, precisa la autorización del titular del derecho de explotación. No obstante, la misma Ley, en su artículo 100.2, exceptúa la copia de seguridad por parte de quien tiene derecho a utilizar el programa, que no podrá prohibirse por contrato cuando resulte necesaria para la utilización del mismo.

El artículo 99 aborda el contenido de los derechos de explotación y a su tenor el titular de los derechos exclusivos de explotación de un programa puede realizar o autorizar:

- La reproducción total o parcial del programa, incluso para uso personal, por cualquier medio y bajo cualquier forma, ya sea permanente o transitoria. Si la carga, presentación, ejecución, transmisión o almacenamiento del programa

■[21] Vid. Galan Corona en op. cit. pág. 264.

precisan tal reproducción, deberá disponerse de la autorización al efecto del titular.

- El derecho de distribución pública definido en el artículo 19 LPI como la puesta a disposición del público del original o copias de la obra mediante su venta, alquiler, préstamo o cualquier otra forma. Atendiendo a ello, podemos afirmar que el autor ostenta los derechos de autorizar o prohibir el alquiler y préstamo de su programa, en los términos ya establecidos en el artículo 4.c) de las derogadas leyes 16/93 y 43/94 de 30 de Diciembre. A tenor de esta norma se entiende por alquiler la puesta a disposición del programa para su uso por tiempo limitado y con un beneficio económico o comercial directo o indirecto. El préstamo supone la misma operación pero sin un beneficio comercial o económico directo ni indirecto, siempre que dicho préstamo se lleve a cabo a través de establecimientos accesibles al público. La Ley presume que no existe tal beneficio cuando el préstamo efectuado por un establecimiento accesible al público dé lugar al pago de una cantidad que no exceda de lo necesario para cubrir sus gastos de funcionamiento. No se considera a estos efectos como alquiler o préstamo la puesta disposición con fines de exposición, la que se hace para consulta "in situ" o la que se realice entre establecimientos accesibles al público. No se precisa autorización, ni origina remuneración, para los préstamos que realicen determinados centros culturales de titularidad pública o de entidades de interés general o centros educativos tales como museos, bibliotecas, etcétera.

- El derecho de transformación que comprende la realización o autorización de la traducción, adaptación, arreglo o cualquier transformación del programa y la reproducción de los resultados de tales actos. Todo ello sin perjuicio de los derechos de la persona que realice la transformación. Ello fue introducido por el art. 4.b Ley 16/93.

No obstante, existen unas limitaciones a estos derechos de explotación y son aquellas que la Ley consagra en su artículo 100 en base a diversas razones:

En primer lugar, el mismo usuario puede realizar la reproducción o transformación del programa que sea necesaria para su utilización exclusiva, sin que ello constituya transformación a los efectos previstos en el artículo 21 de la Ley, por lo que no adquiere derecho de ningún tipo sobre el resultado de su actividad. No obstante ha de ser conforme a una finalidad propuesta y salvo estipulación contractual en contra; esto fue introducido por el artículo 5.1 Ley 16/93. Con ello se admite un "uso leal" por parte del usuario del programa al que

se le reconoce una esfera de actuación que le permite obtener unos rendimientos del programa que no lesionan en absoluto los derechos del autor y el cesionario.

En segundo lugar, el usuario legítimo de la copia de un programa está autorizado por la ley para observar, estudiar o verificar su funcionamiento con el fin de determinar las ideas y principios implícitos en cualquier elemento del programa, siempre que ello se haga durante las operaciones de carga, visualización, ejecución, transmisión o almacenamiento del programa que esté autorizado a hacer.(art.100.3 LPI)

En tercer lugar, el artículo 100.4 contiene una norma que confiere al cesionario titular de los derechos de explotación la facultad de realizar o autorizar la realización de versiones sucesivas y programas derivados, salvo pacto en contra. De nuevo la remuneración de la inversión empresarial es protegida por la Ley, pero hemos de entender que ello tiene como límite el posible conflicto con intereses del autor que se tutelen en los derechos que le confiere el artículo 14. Además, es exigible al cesionario que ejercite este derecho conforme a la buena fe y sin hacer un ejercicio abusivo del mismo. Tampoco el cesionario podrá prohibir la creación de obras derivadas pues ello lo veda expresamente la Ley en el artículo 43.4, aunque si con ello se hace una competencia desleal que lesiona los intereses del cesionario se crea un conflicto que se ha de resolver por las normas del Derecho de la Competencia.

Es digna de resaltar una limitación recogida en el artículo 100.5 LPI que se estableció en aras de fomentar la coherencia y desarrollo de los programas y su interoperatividad. El artículo 6 de la ley 16/93, consagraba la descompilación como un procedimiento de "fair use" en favor del desarrollo y compatibilidad de programas. Ya hemos dicho antes que lo que la Ley protege es la expresión de las ideas del autor una vez plasmadas en la obra como resultado "tangible" y unitario de su actividad. Es por ello que las ideas y principios implícitos en los elementos del programa no pueden acogerse a una protección excluyente, lo mismo que no cabe "adueñarse" de las palabras o las notas musicales. Por lo tanto, en la medida en que la lógica, los algoritmos y los lenguajes de programación comprendan ideas y principios, quedarán excluídos de la protección, pues se trata de proteger la expresión de tales ideas plasmada en el programa.

En la Directiva de la que trae causa el artículo 100.5 la Ley, quedaba ya muy claro que la función de todo programa es comunicarse y trabajar con el resto de los componentes del sistema, con el usuario y con los demás programas y

sistemas. Para ello se precisa contar con un sistema lógico, e incluso físico, de interconexión e interacción, que asegura la interoperatividad, es decir, la capacidad de los programas de intercambiar información y de utilizarla adecuadamente. Supone romper el aislamiento entre equipos, programas y usuarios. Las partes del programa que realizan esa interconexión e interacción entre "software" y "hardware" son los "interfaces" que, como hemos podido constatar, quedan fuera de la protección legal. Para lograr esa interoperatividad se establecen unas excepciones al derecho a oponerse a la reproducción y traducción del código en el que se suministra al adquirente la copia del programa, siempre que ello se haga para lograr la interoperatividad con otro programa creado independientemente. Esa actividad la puede realizar sólo la persona legalmente facultada para utilizar la copia del programa y con arreglo a los fines antes enunciados.

La operación mediante la cual se realiza es la llamada "descompilación", que es el proceso mediante el cual un técnico en informática accede a la estructura interna del programa y conoce así las soluciones aplicadas en la gestión del mismo y otros elementos que no son visibles en el código objeto.[22] Hemos de insistir en el requisito de que la descompilación únicamente puede llevarse a cabo para obtener la información necesaria para la interoperatividad con otros programas, y no con otra finalidad. Tampoco puede facilitarse la información obtenida a terceros, máxime si son competidores y persiguen crear un programa sustancialmente idéntico. Con ello se ha pretendido evitar posiciones dominantes o cuasi monopolísticas en el mercado del "software", promocionando el desarrollo de la creatividad y de la técnica, en beneficio de los usuarios y del rendimiento de los sistemas.

No obstante, hemos de recordar que el programa fuente y el programa objeto están protegidos por la Ley por lo que, "ab initio", la descompilación sería un acto ilícito si no está "legitimada" por una finalidad social relevante que la norma toma en cuenta como fundamento de una excepción: la interoperatividad. Para asegurarse de ello, el artículo 6 de la Ley 16/93, siguiendo a la Directiva, establecía esos requisitos de licitud, luego consagrados en el artículo 100.5 de la Ley:

■[22] Vid. Ribas, J: "Actas del I Congreso Iberoamericano de Propiedad Intelectual". Madrid, Mº Cultura, 1991, Tomo 1º; más extensamente en Galán Corona: "Comentarios...". cit. páginas 314 y siguientes.

A - Que se realice a partir de una copia lícitamente obtenida por el usuario legítimo o, en su nombre, por persona autorizada para ello.

B - Que esa información no haya sido ya puesta a su disposición previamente de manera fácil y rápida.

C - Que las operaciones se limiten a las partes del programa original que sean precisas para conseguir la interoperatividad.

Una vez obtenida esa información, sólo puede utilizarse de acuerdo a unos límites que la Ley establece en el artículo 100.6:

- Ha emplearse exclusivamente para conseguir la interoperatividad del programa creado de forma independiente.

- Sólo puede comunicarse a terceros si es preciso para la finalidad arriba expresada.

- No puede utilizarse para desarrollar, producir o comercializar un programa sustancialmente similar en su expresión, o para cualquier otro acto que infrinja los derechos de autor.

En definitiva, se trata de flexibilizar el régimen de exclusión que el derecho de autor comporta en aras de dinamizar el mercado, fomentar la coherencia y coordinación de programas e incentivar la creatividad del sector. No obstante, esta limitación se basa en un "uso leal" que no puede servir para amparar el plagio, la competencia desleal o lesiones injustificadas a los titulares de tales derechos.

En cuanto a la duración de la protección, tema al que aludimos brevemente en líneas anteriores, hemos de decir que el panorama ha cambiado merced a la armonización comunitaria y como consecuencia del principio "igualitario" asentado en el Convenio de Berna. Originariamente, el artículo 97 de la Ley de 1987 establecía un plazo de protección de 50 años a contar desde el 1º de Enero del año siguiente a su publicación, o desde su creación si no se hubiera publicado. Inicialmente, el Proyecto de Ley preveía un plazo de 20 años, pero merced a una enmienda se amplió a 50 años. La Doctrina nunca aceptó este criterio discriminatorio basado en la idea de impedir que una protección extensa paralizase el desarrollo de los programas. Ello no tenía lógica ya que se permite al

cesionario o adquirente "ex lege" de los derechos de explotación autorizar o realizar versiones sucesivas y programas derivados y se impone la compatibilidad de programas. El artículo 7 de la ley 16/93, hoy derogado, vino a paliar parcialmente la situación pues estableció varios criterios según cada caso atendiendo al plazo general del anterior artículo 97 LPI:

a) Cincuenta años a contar desde las fechas antes citadas en el caso de que el autor sea una persona jurídica. Técnicamente la expresión no es adecuada pues las personas jurídicas no tienen capacidad creadora, pero el artículo 8 prevé la posibilidad de que una de estas personas asuma la iniciativa y coordinación de la obra y que la edite y publique bajo su nombre.

b) Cuando el autor sea persona física el plazo era de su vida y 50 años después de su muerte o declaración de fallecimiento.

c) Si es anónimo o se edita bajo seudónimo, el plazo era de 50 años desde que se puso a disposición del público por primera vez, iniciando el cómputo el 1º de Enero del año siguiente a tal hecho.

Sin embargo, y merced al principio de igualdad de trato a los autores de programas antes mencionado, la disposición derogatoria de la Ley 28/95 de 11 de Octubre, también derogada, modificó el criterio anterior pues pretendía armonizar el plazo de duración de los derechos de explotación en el ámbito de los derechos de autor, adaptando la Directiva 93/98 CEE. En consecuencia, su artículo 2º estableció un plazo de duración que se extiende a la vida del autor y 70 años después de su muerte o declaración de fallecimiento. Si hay varios coautores, el plazo se computa a partir de la muerte del último de ellos que sobreviva. Este mismo plazo general se aplica en los casos de obras bajo seudónimo y anónimas y las atribuidas a personas jurídicas. Cuando la obra no sea divulgada lícitamente, el plazo es de 70 años desde su creación, cuando no sea computado según el criterio general.

Tal y como antes dijimos, el actual artículo 98 LPI ha dejado las cosas en "sitio" al terminar con los criterios discriminatorios, pues a su tenor el plazo de duración es el siguiente:

A - Cuando el autor sea una persona natural el plazo de duración de estos derechos de explotación será el establecido en el artículo 26 como criterio general: la vida del autor y 70 años después de su muerte. No obstante, pueden plantearse

otros supuestos previstos en el Capítulo Primero del Título III, del Libro 1° para las obras póstumas, anónimas y seudónimas(art.27), así como para los casos de obras colectivas, en colaboración (art.28) y las publicadas por partes (art.29).

B - Cuando el titular sea una persona jurídica, en los términos previstos en el artículo 97, la duración de los derechos será de 70 años, computados desde el 1 de enero del año siguiente al de la divulgación lícita del programa, o al de su creación si no se hubiera divulgado.

D - Las infracciones del artículo 102 L.P.I.

Dejando al margen otras posibles conductas lesivas derivadas de los daños personales y patrimoniales previstos en la "parte general" de la Ley y en el Código Penal, podemos afirmar que, como norma general, las infracciones son aquellas conductas contrarias al derecho moral y a los derechos de explotación del programa. No obstante, el artículo 102 de esa misma norma recoge algunos actos en particular:

1- Poner en circulación una o más copias del programa, conociendo o pudiendo presumir su naturaleza ilegítima. Por tanto, no sólo se infringe este derecho cuando se obtiene un rendimiento económico y se es consciente del origen ilícito del programa que se circula, sino que basta con poner en circulación el programa en base a unas circunstancias que permiten presumir su origen "espúreo". Ello deja sin base a la argumentación de la defensa en el conocido caso "La Macchia" en el que la ausencia de ánimo de lucro sirvió de fundamento para absolver al autor de la distribución gratuita de software sin autorización de su titular.

2- Tener con fines comerciales una o más copias del programa, conociendo o pudiendo presumir su naturaleza ilegítima. Ello pretende acabar con los distribuidores de copias ilegítimas de programas que tanto abundan en la actualidad, merced a la comercialización de unidades de "C.D. Rom" que permiten copiar el programa original. A este respecto volvemos a insistir que este tipo de aparatos deberían ser objeto de remuneración compensatoria en favor de los titulares de los derechos sobre los programas, que son excluídos por el artículo 25.3 de la Ley sin causa que lo justifique pues estamos ante una obra literaria.

3- Poner en circulación, con fines comerciales instrumentos cuyo único uso sea facilitar la supresión o neutralización no autorizada de los dispositivos

técnicos de protección del programa. Ello se refiere, por ejemplo, a los "copiones" que permiten destruir las "defensas" del programa y saltarse las claves o cualquier otro dispositivo que el programa posea para evitar copias o utilizaciones no autorizadas.

Es digno de mencionar aquí la detención, en diversas ciudades españolas, de 26 supuestos clientes de una red de venta ilegal de software "pirateado" a través de INTERNET, que fueron puestos a disposición judicial. La acusación se basa en el artículo 102.1 L.P.I y el artículo 298 del Código Penal pues se les considera autores de un delito de receptación y las pruebas se obtuvieron al interceptar el correo electrónico del sujeto que se encargaba de la distribución de las copias ilegales.

E - Las medidas de protección.

Como norma general, los titulares de estos derechos están tutelados igualmente por los instrumentos de protección que la Ley consagra: el Registro de la Propiedad Intelectual, los símbolos de reserva de derechos, las entidades de gestión, acciones y procedimientos y el régimen de sanciones. Ello se debe a que estamos ante una obra literaria con ciertas especialidades que la ley ha tenido en cuenta a la hora de establecer esa protección. En lo que aquí interesa es de destacar la necesidad de fomentar que los autores de programas se integren en una entidad de gestión dado que uno de los problemas de los titulados en informática estriba en la falta de un Colegio Oficial y ésta puede ser una vía indirecta de coordinación y unión entre ellos.[23]

Haciendo un breve recorrido concreto por los medios de protección que más nos interesan podemos precisar:

■[23] Este régimen protector se completa con el Código Penal del cual destacamos los artículos 264.2, relativo a los daños; el 271 y siguientes que sanciona los delitos relativos a la propiedad intelectual e industrial; el 278.3 sobre apoderamiento o destrucción de soportes informáticos y el 400 sobre la tenencia o fabricación de útiles o programas de ordenador específicamente destinados a la comisión de los delitos antes mencionados.

1) Las acciones y procedimientos del Libro III, Título 1°, artículos 133 y siguientes, de la Ley que consagran:

- El cese de la actividad ilícita.

- La posibilidad de desplegar las acciones y medidas cautelares del artículo 133 y las medidas cautelares de protección urgente del artículo 136 que prevé la intervención y el depósito de los ingresos obtenidos en la actividad ilícita de que se trate, la suspensión de la actividad, el secuestro de ejemplares e instrumentos que posibilitan la defraudación y el embargo de equipos y aparatos.

- El artículo 134.2 prevé la posible destrucción o inutilización de los mismos ejemplares, materiales o instrumentos de defraudación.

- El artículo 135 prevé la indemnización de los daños materiales, patrimoniales y morales. A tal efecto, el perjudicado puede optar porque se le repare el beneficio que hubiera obtenido de no mediar la actividad ilícita o que se le pague la remuneración que hubiera percibido de haber autorizado la explotación. En el caso del daño moral procede su indemnización, aún no probada la existencia de un daño económico. Para su valoración se atenderá a las circunstancias de la infracción, la gravedad de la lesión y el grado de difusión ilícita de la obra.[24]

- Cabe también la puesta en práctica de los procedimientos del artículo 137 del que cabe destacar una novedad interesante en su párrafo 3° pues, al solicitar al juez la adopción de las medidas cautelares, éste antes de dar traslado del escrito a las partes, puede requerir los informes y ordenar las investigaciones que estime oportunas. Ello implica el posible "registro por sorpresa" que impide que el infractor sea "preavisado" y pueda ocultar o destruir pruebas de la actividad infractora.

■[24] Ello nos recuerda, a título de ejemplo, el caso del Beato Juan de Avila al que un impresor de Alcalá de Henares le publicó, sin su autorización, una biblia con sus anotaciones y comentarios personales, lo cual le provocó un serio "tropiezo" con la Inquisición.

Es de destacar la "importación" a nuestro país de una "técnica" procedente del mundo anglosajón que, junto al "registro sorpresa", se está mostrando muy eficaz: se prima a los denunciantes de las infracciones con el 10% de la indemnización obtenida si prospera la pretensión del afectado. Así, en 1994 se presentaron 236 denuncias en nuestro país, llegándose a un total de 191 acuerdos extrajudiciales.

2) La protección registral:

El artículo 101 L.P.I. sanciona que los derechos sobre los programas de ordenador, así como sobre sus versiones sucesivas y los programas derivados, pueden ser objeto de inscripción en el Registro de la Propiedad Intelectual. No obstante, el propio precepto ya prevé que se dicten normas para evitar que el Registro se convierta en una fuente de acceso al conocimiento de aquellas partes o elementos del programa que permitieran su plagio. Esta materia se regula en los artículos 139 y siguientes de la propia Ley, el R.D. 1694/94 de 22 de julio de 1994 y el Reglamento del Registro de la Propiedad Intelectual, R.D. 733/93 de 14 de mayo de 1993. A tenor del artículo 8.1 del Reglamento se crea la sección 7ª en el Registro sobre programas de ordenador.

Dicho precepto exige para practicar la inscripción de programas que se plasmen en soportes que garanticen la durabilidad y permanencia de los inscritos y el artículo 14.7 exige que se describa la obra mediante la presentación en papel de las 10 primeras y últimas hojas del código fuente o un resumen, de 20 folios máximo, del manual de uso, siempre que contenga y reproduzca los elementos esenciales del programa. Si este fuera inédito, deberá presentarse la totalidad del código fuente.

El artículo 32 del mismo texto sólo permite la consulta pública del nombre o denominación social del solicitante, nombre, nacionalidad y residencia del autor del programa, naturaleza y condiciones del derecho inscrito y título y fecha de publicación.[25]

■[25] Para verificar la inscripción se han de rellenar unos modelos de documentos que facilita el propio Registro, unos genéricos para todo tipo de obras y otro, el B-7, específico para programas de ordenador. La queja que más se formula en el caso de los programas es la relativa a la obligatoriedad de presentar la totalidad del código fuente en papel, por los gastos y molestias que ello genera, pues en algunos programas ese documento puede llegar a ser muy extenso y ocupar

Pese a todo lo anterior, queremos también resaltar que es muy "difícil" dotar a esta materia de un régimen equilibrado que permita, a la vez, proteger adecuadamente los derechos excluyentes en este campo, tan dinámico y necesitado de desarrollo, en el que se han de armonizar tales derechos con los intereses de las empresas y los usuarios. Combinar adecuadamente Propiedad Intelectual, Derecho Civil en aras de los titulares, Derecho Mercantil y derechos de los consumidores es una tarea complicada que, sin duda, seguirá planteando nuevos problemas conforme avancen la creatividad de los programas y los medios de defraudación.

5- La protección de las bases de datos.

Es indudable que una documentación compuesta por datos informatizados es un producto menos tecnificado que un programa de ordenador, en razón de ello su protección por el derecho autor debe ser, en principio, menos "complicada". Como norma general, volvemos a utilizar el Proyecto de Tratado antes aludido (OMPI, 1996) en cuyo artículo 5 se ponen de manifiesto las directrices de esta materia cuando se refiere a estas como "colecciones de datos". A tenor de este artículo "las colecciones de datos o de otros materiales, en cualquier forma, que por razones de la selección o disposición de sus contenidos constituyen creaciones de carácter intelectual, están protegidas como tales. Esta protección no abarca los datos o materiales en sí mismos y se entiende sin perjuicio de cualquier derecho que subsista respecto de los datos o materiales contenidos en la colección". (cfr. 2.5 C. de Berna y 10.2 ADPIC)

Hemos de anticipar que nuestro ordenamiento jurídico no posee un apartado específico en el artículo 10, dedicado al objeto del derecho de autor, que aluda de forma expresa a esta cuestión, pero el artículo 12 sí se ocupa de ellas, a

varios volúmenes encuadernados. Hemos de tener en cuenta que el papel es el único soporte admitido a efectos de registro, salvo ciertas excepciones en que se admite el cassette para obras musicales. También se fromulan algunas quejas en relación a le necesidad de consignar algunos datos que se deducen del programa y que incluso la solicitud de alguno de ellos ya está anticuada, por ejemplo el diagrama de la aplicación.

nuestro entender, cuando regula las colecciones.[26] A tenor de este precepto, "también son objeto de propiedad intelectual, en los términos de la presente Ley, las colecciones de obras ajenas, como las antologías, y las de otros elementos o datos que por la selección o disposición de las materias constituyan creaciones intelectuales, sin perjuicio, en su caso de los derechos de los autores de las obras originales". La Ley alude expresamente al concepto bases de datos en el artículo 20.2 (i cuando define como acto de comunicación pública "el acceso público a bases de datos de ordenador por medio de telecomunicación, cuando éstas incorporen o constituyan obras protegidas". Esto quiere decir que para nuestra Ley las bases de datos son una creación intelectual digna de protección legal siempre que cumpla los requisitos exigidos para ello y en conciliación con los derechos de los titulares de las obras o informaciones incluidas en la base o colección. La base o colección se nos aparecerá así como un tercer género donde se pueden conciliar aspectos de la obra compuesta, la colectiva y la obra en colaboración, aunque suele aparecer como una obra compuesta, comercializada bajo la apariencia de obra colectiva que coordina una persona física o jurídica que la edita y divulga bajo su nombre. (ej. B.D. Aranzadi o La Ley Actualidad)

No hay una normativa particularizada, como para los programas de ordenador, y es por esto que habremos de considerar que ello se debe a que las bases de datos están sometidas al régimen general de la LPI, en la medida en que se les considera objeto de la propiedad intelectual como obras literarias, según los flexibles términos de los artículos 10 y 12 de la Ley de Propiedad Intelectual. Ya hemos hecho referencia anteriormente a la importancia de la información en nuestra sociedad así como al hecho de que tan importante es la "cantidad y calidad" de la misma, como el que se encuentre depositada de forma sistemática y organizada que permita su rápida localización y tratamiento. Sistematización, coordinación e interrelación son exigencias que toda colección o conjunto organizado de información precisa para ser útil y valorada. A ello vienen a responder las bases de datos en sus distintas clases.

A la hora de fijar su concepto debemos partir de la idea general de que una base de datos es un conjunto de unidades de información informáticamente

■[25] Sobre el artículo 12 de la L.P.I. véase Rogel Vide, Carlos: "Comentarios al Código Civil y Compilaciones Forales". Dir. Albaladejo y Díaz Alabart. EDERSA, Madrid, 1994. Tomo V; vol.4° A, Páginas 275 y siguientes.

organizadas susceptibles de protección legal. El artículo 1.2 de la Directiva 9/96 CE considera como bases de datos "las recopilaciones de obras, de datos o de otros elementos independientes, dispuestos de manera sistemática o metódica y accesibles individualmente por medios electrónicos o de otra forma". Dentro de este concepto general podemos distinguir:

- Base de datos "strictu sensu": Es el "depósito común de documentación, almacenada y organizada de una forma determinada, útil para diversos usuarios y diferentes aplicaciones, que permiten recuperar esa documentación proporcionando la información deseada como respuesta a una consulta".

- Bases de datos jerárquicas: en éstas la nota esencial es la organización jerárquica o arbórea:" Aquellas que tienen los datos organizados en forma arbórea según una estructura jerárquica. Partiendo de un tronco principal, en el que está definido un elemento o concepto y que se conoce con el nombre de nodo, nacen diferentes ramas de las que "cuelgan" a su vez distintos elementos o conceptos, que forman otros nodos, que a su vez pueden poseer otras ramas, y así sucesivamente".

- Bases de datos de red: son aquellas que parten de una base jerárquica o una estructura similar y permiten "una relación asociativa mayor entre sus miembros, de forma que un nivel inferior puede tener asociado más de un nivel superior con lo que, mediante una organización en malla o red, se permite multiplicar las relaciones entre los elementos de la base".

- Bases de datos relacionales: son aquellas que "tienen un número de campos y subcampos igual por cada fichero, de forma que permite relacionarlos entre sí, posibilitando un diálogo amplio con el usuario".[27]

Si se atiende al medio de acceso a la información contenida en la base de datos, cabe distinguir dos tipos:

■[27] Vid. Actualidad Informática Aranzadi, número 4 de Julio de 1992.

- Bases en línea ("on line"): se accede a la consulta de la base mediante una conexión desde el ordenador del usuario que consulta al ordenador del distribuidor. A través de la línea telefónica se establece la conexión entre ambos.

- Base autónoma: en ella el soporte físico en el que se contiene la información es independiente y puede ser manejado autónomamente por el usuario en su ordenador. Normalmente, el usuario recibe el programa que permite la consulta y la información contenida en un disco compacto.(CD-ROM)

Los problemas básicos que plantean las bases de datos están referidos a la confluencia de distintas relaciones jurídicas que se dan en su seno. Así lo pone de manifiesto Terrado cuando dice: "Quizá la característica más sobresaliente de las bases de datos reside, a nuestro entender, en el hecho de que se trata de una prestación informática en la que subyace la conexión de diferentes figuras contractuales que actúan en unos casos a modo de contratos preparatorios y que van dirigidos a la obtención de la cosa o bien informático - contrato de adquisición de hardware, de suministro logicial o software y de mantenimiento - y en otros caso institutos contractuales que acentúan más el resultado, la prestación del servicio informático y que quedan englobados en contratos de explotación, comercialización y distribución". [28]

Se deben proteger y armonizar los derechos de los autores del material informativo contenido en la base y los de los productores sobre la base que han producido y cuya explotación realizan. Al margen de ello, se deben tutelar los derechos de los usuarios de la base por vía contractual y mediante las normas ajenas a la propiedad intelectual, como por ejemplo, el Derecho de los Consumidores.[29]

Según la doctrina ya citada, la base de datos es una creación intelectual que contiene aspectos de dos tipos de obras legalmente definidos. Efectivamente, posee matices de la obra colectiva y la obra en colaboración, porque la contribución de cada una de las personas que intervienen en su creación es

■[28] Vid. "Protección jurídica de las bases de datos". Actualidad Informática Aranzadi, número 18 de Julio de 1995.

■[29] Vid. Davara Rodríguez: "Derecho Informático".cit. pág.142

perfectamente identificable y explotable por separado (art.7 LPI); sin embargo se explota como una obra colectiva en la que se funden las distintas aportaciones y bajo el nombre de la persona física o jurídica que aparece como titular. (art.8 LPI) Parece lógico concluir que cualquier explotación parcial de una de estas aportaciones deviene en perjuicio de la obra completa, por lo que no cabría admitir esta posibilidad. En este complicado panorama debemos de atender a las reglas para aplicar el derecho de autor a sus distintos aspectos que nos dan Linant y Hollande:[30]

- La base debe estar protegida en cuanto conjunto organizado de información, pues la estructura organizativa que se ha dado a ese fondo documental es de por sí una creación original, por lo que no cabe admitir una reproducción total o parcial de la misma.

- Son también objeto de derecho de autor las representaciones en las cuales se plasma esa información que se facilita al usuario, pues suponen un reflejo documental del trabajo de la base.

- Otros productos derivados de la base tales como listados, fichas o sumarios, son protegibles en la medida en que suponen un reflejo de la organización de la misma.

- También se protege el "thesaurus" interno de la base y los documentos de utilización específica que se facilitan al usuario, tales como listas de conceptos, etcétera.

- Los criterios establecidos para clasificar la información, así como para realizar las búsquedas y consultas, alfabéticos, por listas, por palabras, por fechas, etcétera no son susceptibles de dominio exclusivo, pues pertenecen al acerbo común.

- Son exigibles a este objeto de propiedad intelectual los requisitos de creatividad y originalidad predicados del resto de las obras protegidas por la legislación sobre la materia.

■[30] Vid. "Droit de l'informatique". Delmas, París, 1984.

- Están protegidas en nuestra Ley por medio del Libro I al igual que el resto de las obras literarias. En consecuencia, el productor de la base de datos posee los derechos sobre la misma que la ley atribuye a los autores y puede explotarla y oponerse a cualquier conducta que suponga una lesión a su derecho sobre esta creación intelectual. Ello comporta, además, la posibilidad de acogerse igualmente a los instrumentos de protección que la Ley prevé para la defensa de estos derechos, pues estamos ante una obra literaria original merecedora de un tratamiento específico, pero protegida por los mismos cauces.

Cuestión diferente es la de la titularidad del derecho sobre la información contenida en la base, pues a tal efecto conviene distinguir varios supuestos:

- Si la información es original y pertenece al productor, éste será el titular exclusivo del derecho de autor sobre la misma.

- Si es información de dominio público, entonces no es apropiable por ningún sujeto, por lo que la base puede incluir esa información, pero no puede impedir que otros hagan lo propio de acuerdo a otros criterios.[31]

- Si pertenece a terceros se produce la concurrencia del derecho de estos con el productor. Es indudable que el derecho del autor de la información es prioritario y preferente, pues será precisa su autorización para incluirla en la base. A título de ejemplo, podemos referirnos a una base de datos sobre obras y autores literarios: si se introduce el texto completo de la obra, es precisa autorización; si sólo se trata de un listado de obras y autores, no será necesario porque no hay reproducción. No obstante, si se reproduce parcialmente la obra, selección de una parte o resumen, será necesario citar la fuente y siempre que no se exceda del derecho de cita.[32]

Este panorama, un tanto "confuso", se va a aclarar merced a la aprobación de la Directiva 9/96 CE de 11 de Marzo de 1996 sobre "protección

■[31] A tal efecto, es interesante el paralelismo que se presenta con respecto a las enciclopedias que, de algún modo, son tambien colecciones de datos. Véase nuestro comentario a la sentencia del Tribunal Supremo de 20 de febrero de 1992 en "Acerca de la protección de las ideas.." cit. loc. cit.

■[32] Vid. Bertrand:" Le droit...".cit. páginas 452 y siguientes.

jurídica de bases de datos ". [33] Esta norma es consciente de la insuficiencia y falta de uniformidad de la protección que se dispensa a las bases de datos por parte de los Estados miembros, lo cual produce diversos efectos nocivos sobre el funcionamiento del mercado interior, problema que se pretende solucionar mediante la técnica uniformadora que persiguen las directivas y acortando el plazo de adaptación que expira el 1 de enero de 1998. Mientras tanto, la Directiva sirve como criterio interpretativo para suplir la laguna legal por Jueces y Tribunales y, una vez expirado, actuará como norma directamente aplicable. Además, hemos de tener en cuenta que los ciudadanos pueden accionar contra los Estados miembros por los daños que sufran en sus derechos, como consecuencia de la negligencia de éstos en la aplicación de las normas comunitarias.

Una vez definido su amplio concepto de bases de datos, la Directiva deslinda la protección de éstas de la que se dispensa al programa de ordenador utilizado para crearla o gestionarla. En este sentido, el artículo 1.3 afirma que la protección prevista en ella no se aplica a los programas de ordenador utilizados en la fabricación o en el funcionamiento de bases de datos accesibles por medios electrónicos. En esta misma línea de delimitación normativa, el artículo 2 asienta su compatibilidad con las normas comunitarias referidas a la protección de los programas, a los derechos de arrendamiento, préstamos y otros derechos afines y a la duración de los derechos de autor y derechos afines. Así mismo, el artículo 13 establece que esta Directiva no afectará a la normativa sobre otras materias que fuere aplicable al caso, tales como las de Propiedad industrial, Derecho de la competencia, protección de datos, contratos, acceso a los archivos públicos, etcétera.

Siguiendo la línea antes expuesta, el artículo 3.1 establece que "las bases de datos que por la selección o la disposición de su contenido constituyan una creación intelectual de su autor estarán protegidas, como tal creación, por los derechos de autor. No serán de aplicación otros criterios para determinar si tales bases de datos son susceptibles de dicha protección". Llama la atención la poca claridad del precepto pues parece excluir la exigencia de originalidad y licitud para desplegar la protección legal, criterios estos que sí se aplican a los programas. Realmente, el requisito de originalidad está implícito en la norma toda vez que

■[33] Esta norma trae causa de la propuesta 93/C 19/02 (DOCE de 23/6/92) y la propuesta modificada 93/C 308/01 (DOCE de 15/11/93)

utiliza la expresión"... que por la selección o la disposición de su contenido constituyan una creación intelectual de su autor...", esto quiere decir que esa selección o disposición debe emanar de la creatividad del autor, no proceder de la actividad creadora de otro al cual se copia.

En este sentido, nuestro Tribunal Supremo ha negado que exista creatividad susceptible de protección conforme a la Ley de Propiedad Intelectual en aquellas bases de datos en las que se ha empleado una sistemática concreta y determinada, pero que no incluyen datos originales. Tal es el caso de la reproducción parcial de las bases de datos publicadas por las Cámaras de Comercio, referidas a las empresas en ellas registradas. La demanda por plagio fue desestimada dado que se entiende que se trataba de una compilación de datos obrantes en registros públicos, guías telefónicas, directorios, etcétera, pero no había una originalidad en el contenido, ni en los criterios y técnicas de sistematización y acceso.(Cfr. STS 12/12/1988 y 2/3/1992)

Del mismo modo, el artículo 3.2 excluye que la protección que se dispensa a la base se aplique al contenido, aunque se hace compatible con los derechos sobre dicho contenido. Hemos de insistir en que el objeto del derecho del autor de la base no es el programa ni el contenido, es la obra inmaterial concretada en el resultado de analizar, seleccionar, recoger, ordenar, coordinar, interconectar y hacer accesible por medios informáticos unas unidades de información llamadas datos.

En el artículo 4 se hace referencia a la titularidad de los derechos, atendiendo a los distintos supuestos de autoría:

- Se considera autor, o autores, a la persona física, o conjunto de ellas, que haya creado la base. Se prevé la posibilidad de que la titularidad corresponda a una persona jurídica, tal y como se recoge en el artículo 5.2 de nuestra LPI.

- Se admite la atribución de los derechos patrimoniales a la persona que figure como titular de la obra colectiva, tal y como se establece en el artículo 8 LPI.

- Se prevé la posibilidad de que la base de datos sea una obra en colaboración, aplicándose entonces el artículo 7 LPI.

En el artículo 5 se recoge el catálogo de derechos de explotación que corresponden al autor respecto "de la forma de expresión de dicha base susceptible de protección de los derechos de autor". A tal efecto, tiene el derecho exclusivo de realizar o autorizar:

A - La reproducción temporal o permanente, total o parcial, por cualquier medio y de cualquier forma.

B - La traducción, adaptación, reordenación y cualquier otra modificación.

C - Cualquier forma de distribución al público de la base de datos o de copias de la misma.

D - Cualquier forma de comunicación, exhibición o representación.

E - Cualquier reproducción, distribución, comunicación, exhibición o representación al público de los resultado de los actos a que aludíamos en el apartado B.

En definitiva, el autor de la base de datos lo es de una obra literaria, que puede ser accesible "on line" o mediante la adquisición del soporte físico individualizado, (v.gr. CD) en consecuencia , debe ostentar los mismos derechos que el resto de los autores de esta naturaleza. No obstante, el usuario legítimo de la base de datos o de su copia, ya sea de toda o una parte de ella, tiene derecho a realizar tales actos cuando sean necesarios para el acceso al contenido de la base de datos y a su normal utilización por el propio usuario.[34]

Por otra parte, el artículo 6.2 de la Directiva admite la posibilidad de establecer unas limitaciones a estos derechos que se mantienen en la línea de las establecidas en nuestra LPI, en sus artículos 31 y siguientes:

■[34] Téngase en cuenta que lo normal es que al adquirir la copia legítima de la base de datos en el mismo CD se incluya un programa de gestión y consulta que se instala en el disco duro y mediante el cual se accede a los datos recogidos en el disco que, a su vez, se va renovando periódicamente por el proveedor. Se puede adquirir la bese completo o una parte de ella, por ejemplo legislación y jurisprudencia penal.

A- Cuando se trate de una reproducción con fines privados de una base de datos no electrónica. En este caso, consideramos que su "cobertura" en nuestra Ley procede del artículo 31.2 y, por tanto, se debe aplicar a su vez el artículo 25.1 en cuanto al derecho de remuneración por copia privada, por cuanto se alude a "... obras divulgadas en forma de libros o publicaciones que a estos efectos se asimilen...".

B- Cuando su utilización se haga únicamente con fines ilustrativos de enseñanza o de investigación científica, siempre que indique la fuente, en la medida justificada por el objetivo no comercial que se persiga. (cfr.20.2 y 32 LPI)

C- Cuando se trate de una utilización para fines de seguridad pública o a efectos de un procedimiento administrativo o judicial. (cfr. art.31.1 LPI)

D- Cuando se trate de otras excepciones a los derechos de autor "tradicionalmente contempladas por su derecho interno", sin perjuicio de lo dispuesto en las letras A), B) y C). El término "tradicionalmente" implica, a nuestro juicio, una excepción ya recogida en las normas legales del Estado, no una autorización a crear otras nuevas no previstas, tarea a la que los Estados suelen ser, por cierto, muy aficionados. En nuestro caso, básicamente, serían las contempladas en el capítulo 2º, del Título III, del Libro primero, bajo el epígrafe de límites, en la medida en que le fueran aplicables.

En tal sentido hemos de interpretar, como "límite a las limitaciones", lo establecido en el artículo 6.3: "Conforme a lo dispuesto en el Convenio de Berna para la protección de las obras literarias y artísticas, el presente artículo no podrá interpretarse de manera tal que permita su aplicación de forma que cause un perjuicio injustificado a los intereses legítimos del titular del derecho o que vaya en detrimento de la explotación normal de la base de datos". Ello supone que estas limitaciones a los derechos de explotación de las bases de datos no pueden ir más allá de lo establecido para el resto de las obras literarias y artísticas, para no romper con la igualdad del estatuto jurídico de sus titulares con respecto a los demás autores.

En su capitulo 3º la Directiva consagra el llamado "derecho sui géneris" en favor del fabricante de la base de datos, merced al cual éste puede prohibir la "extracción" ("transferencia permanente o temporal de la totalidad o de una parte sustancial del contenido de una base de datos a otro soporte, cualquiera que sea el medio utilizado o la forma en que se realice") y/o "reutilización"("toda forma de

puesta a disposición del público de la totalidad o de una parte sustancial del contenido de la base mediante la distribución de copias, alquiler, transmisión en línea o en otras formas") de la totalidad o una parte sustancial del contenido de ésta, evaluada cualitativa o cuantitativamente, cuando la obtención, la verificación o la presentación de dicho contenido representen una inversión sustancial desde el punto de vista cuantitativo o cualitativo. A tal efecto, el préstamo no se considera un acto de extracción o reutilización.

Se trata de un derecho a fin de carácter patrimonial que debe conciliarse con los derechos de los autores, reconocido al fabricante en aras de la protección de las inversiones que éste ha realizado.(cfr. art.7.4) Se trata de un derecho autónomo y conexo que limita al derecho del autor y cesionarios, así como a los reconocidos a los usuarios. En esta línea, el artículo 7.5 tampoco permite la norma que se autoricen extracciones y/o reutilizaciones repetidas o sistemáticas de partes no sustanciales del contenido de la base de datos que supongan actos contrarios a una explotación normal de dicha base o que causen un perjuicio injustificado a los intereses legítimos del fabricante de la base.

Es un derecho patrimonial, conexo con los del autor, pero que puede transmitirse, cederse o darse en licencia contractual, que también está sometido a unas limitaciones que se consagran en los artículos 8, 9, 10 y 15 de la Directiva. En ellos se impone un equilibrio entre los derechos y obligaciones del usuario para evitar que su utilización conlleve la posibilidad de realizar actos que sean contrarios a una explotación normal de la base o lesionen injustificadamente los intereses legítimos del fabricante de la base.

El artículo 10 establece como plazo general de duración de este derecho el de 15 años a contar desde el 1 de enero del año siguiente al de terminación del proceso de fabricación de la base de datos, si bien se prevén ciertos supuestos especiales, entre los cuales destaca el caso en que se produzca una modificación sustancial, cualitativa o cuantitativa, en el contenido de la base: adiciones, supresiones o cambios sucesivos que permitan considerar que se trata de una nueva inversión sustancial, lo cual permitirá atribuir a la base resultante un plazo de protección propio.

Finalmente, la norma insta a los Estados miembros a establecer las sanciones adecuadas para asegurar el cumplimiento de lo dispuesto en ella, que en nuestro caso se concretan, actualmente, en la LPI y en el Código Penal, artículos 270 y siguientes. Tal y como dijimos antes, esta Directiva obligará a introducir ciertas modificaciones en nuestra Ley de Propiedad Intelectual para acoger en su seno las cuestiones que no se encuentran ya en su texto, si bien no creemos que nuestro Legislador cumpla con esta tarea antes del plazo previsto, por lo que, de

nuevo, entraremos en una situación "movediza" poco adecuada en una época en la que la difusión y el respeto a los derechos de la autores y afines es, todavía, una tarea ardua y complicada.

6.- A modo de conclusión.

Hemos expuesto aquí las dos cuestiones más importantes que, a nuestro juicio, se deducen de la relación entre informática y Propiedad intelectual, pero somos conscientes de que la tarea es mucho más amplia y complicada, lo cual excede de las intenciones y fines de esta obra. No queremos dejar de mencionar que un nuevo problema empieza a reclamar la atención del Derecho: las llamadas "autopistas de la información", redes o INTERNET, que están planteando diversos desafíos a los juristas y, en lo que a nosotros interesa, se vertebran en los nuevos fenómenos de utilización de obras protegidas por la propiedad intelectual e, incluso, fenómenos de coautoría merced al juego de la interoperatividad y el llamado "hipertexto" que permite, no sólo hacer un uso indiscriminado de las obras, sino introducir aportaciones o modificaciones no consentidas en una obra ajena. El problema no es ahora la censura de contenidos o el control de accesos, sino la "redefinación" de muchos conceptos y técnicas [35] de la propiedad intelectual, que suponen un serio desafío a unos juristas no muy avezados en un campo donde la técnica "aventaja" al Derecho que tendrá que cambiar muchos esquemas si quiere responder adecuadamente a ese desafío.

■[35] Tal es el caso de las llamadas "matrículas digitales" para controlar la utilización de las obras, los derechos sobre las "copias efímeras" que se pretenden imponer a los proveedores de INTERNET o los problemas de difusión de obras "ilícitas" como la biografía de Mitterrand en el "cibercafé" de Besançon".

Algunos problemas puntuales. Experiencias Legislativas y Jurisprudenciales en Latinoamérica

YARINA AMOROSO FERNÁNDEZ

Especialista del Ministerio de Justicia de Cuba.
Presidenta de la Sociedad Cubana de Derecho e Informática.

INTRODUCCIÓN:

Estamos frente a un tema original: el binomio "Nuevas Tecnologías y Derecho", los que en interacción generan nuevos fenómenos y su vez demandan respuestas a corto, mediano y largo plazo. También para encauzar la acción ante este binomio se requiere un esfuerzo sostenido, capacidad informática y jurídica específicas, así como determinante voluntad política de romper los moldes tradicionales y caducos. De esta forma podremos enfrentar, por un lado un lado las nuevas tecnologías que son un medio y no un fin; y por otro, el desafío que las mismas han provocado en nuestro entorno social y cultural.

La expresión más comunmente utilizada en nuestro medio para expresar estas nuevas tecnologías: La Informática, incide en todas las ramas del Derecho.

La Informática como objeto de Derecho, demanda de éste respuestas tendentes a establecer nuevas reglas jurídicas en materias tales como: la promoción y protección del software y la industria Informática; el valor probatorio del documento electrónico; las materias contractuales en la adquisición de bienes y servicios informáticos.

La égida Derecho al reclamo de la Informática alcanza además a todo lo relativo al flujo de datos Trasfronteras y la defensa de los derechos individuales, frente a los riesgos que la información acarrea para las libertades públicas y privadas.

También el Derecho se ha tenido que pronunciar en cuanto a las particularidades de los contratos laborales en el contexto de servicios y producciones informáticas y las enfermedades profesionales derivadas del uso de las nuevas tecnologías y más recientemente las regulaciones que rigen el régimen jurídico del Teletrabajo.

Otro tema emergente de las nuevas tecnologías y que ha reclamado protección del Derecho es el referido a los bancos de datos así como los contratos de transferencia de tecnologías informáticas, entre otros múltiples aspectos.

Pero como es de presumir, el desarrollo de la rama jurídica asociada a la informática está en relación estrecha con el grado de difusión de esta última y más aún con el tipo de política informática aplicada, por eso a continuación intentaré aproximarme a experiencias latinoamericanas[1] y especialmente la experiencia cubana, para ello haré referencia algunas soluciones legislativas, jurisprudenciales y la doctrina de los temas que abordaré en este curso de Maestría, aunque el tema central de estas experiencias están referidas fundamentalmente al Derecho Penal de la Informática, y más aún si se puede hablar una "filosofía del Derecho Penal de la Informática"

A continuación les voy a exponer en tópicos independientes y muy sucintamente tratado a mi juicio las principales realizaciones en materia de Derecho de la Informática en Latinoamérica. Así como aquellas que se refieren al otro segmento de interés de estudio en el devenir de la incidencia Derecho e Informática, este caso en el que el Derecho es el objeto de estudio y la informática la herramienta, lo que metodológicamente se ha identificado como Informática Jurídica.

I. MUY BREVE REFERENCIA DEL DERECHO DE LA INFORMÁTICA EN LATINOAMÉRICA. EXPERIENCIAS EN CUBA.

a)- ¿Qué entiendo por Derecho de la Informática?:

[1] Carlos Ferreyros, "Aspectos metodológicos del delito informático", Notas del curso Nuevas Tecnologías y Derecho, UNED, mayo de 1995. Mérida, España.

Como parte también consustancial al proceso de "Informatización de la Sociedad", es necesario contar con el orden legal que nos permita proteger a la sociedad ante las arbitrariedades y abusos que puedan cometerse en el uso indebido de las nuevas tecnologías de la información y la comunicación: así como ordenar los procesos de desarrollo de aplicaciones de estas tecnologías, para que cuenten con las garantías técnicas y jurídicas que permitan su generalización y comercialización como bienes y servicios de valor patrimonial, tutelares por el Derecho a pesar de tener en muchas ocasiones una naturaleza inmaterial.

El impacto social de las nuevas tecnologías incide en casi todas las ramas tradicionales del Derecho tales como: Constitucional, Civil, Laboral, Administrativo, Mercantil, Penal y en las normas procesales, reclamando de todas ellas la reconceptualización de sus postulados doctrinales, y la adaptación de sus normativas ante las nuevas relaciones sociales y jurídicas, que se generan por la incidencia y generalización de las aplicaciones de dichas tecnologías en la sociedad, e incluso la regulación de nuevas realidades no previstas por el Derecho.

Pero, en mi criterio, el Derecho de la Informática no es sólo orden normativo, sino práctica jurídica y es también, por qué no, una comunidad doctrinal en búsqueda de nuevas soluciones. Estimo que está muy vinculado a una modernización del Derecho y por tanto es la gestación de un Derecho del porvenir que estamos necesitando en el hoy. Es transitivo con respecto a que muchas de sus instituciones ya paulatinamente se incorporan al acervo doctrinal y el devenir de las ramas tradicionales y en sí mismo por su objeto de estudio siempre está evolucionando y estudiando nuevos problemas, pienso que asistimos a un momento excepcional del desarrollo del Derecho y que podemos ser activos contribuyentes en su consolidación.

b)- ¿Dónde se encuentran las principales realizaciones?:

La protección de los Datos y la Información en general: Experiencias en Cuba y otros países latinoamericanos.

Como se sabe la información procesada por medios electrónicos o que circula por las redes no tiene iguales características, por lo que no se puede adoptar para ésta las mismas normas de protección. Generalmente existen dos grandes áreas de atención por parte del Derecho, las que alcanzan a un tratamiento muy especializado; por una parte, nos encontramos con los Datos Personales, y por otra, la información de carácter patrimonial, que es la que abarca

a los datos estratégicos de entidades, y la que está sujeta a las normas de propiedad intelectual siempre que sean creaciones reconocidas por sus dos regímenes jurídicos Derecho de Autor y Propiedad Industrial.

Alrededor de estas dos grandes áreas muy diferentes se han generado desde la década de los años 60, tanto pronunciamientos de la ONU, específicamente la Comisión de Tratamiento de las Minorías, y la adopción del Convenio de Estrasburgo, sobre "Protección de Datos Personales", así como la promulgación de legislaciones nacionales que ya alcanzan la tercera generación y cuya expresión más reciente es la Ley Orgánica de Protección de Datos Personales más conocida como LORTAD, de España.

En el caso de la Protección de los Datos Personales, considero que el origen lo podemos encontrar vinculado a la diversificación de las aplicaciones informáticas al tratamiento de la información personal, entiéndase cuentas bancarias, Registros Civiles, de Personal, de Actos de Ultima Voluntad, de Sancionados, entre otros; se inició en la década de los años 60 un movimiento de la doctrina jurídica y de la jurisprudencia de los países con mayor grado de desarrollo tecnológico tendente al reconocimiento del derecho a la libertad informática y a la autodeterminación en la esfera informativa, que tiene su principal instrumento de garantía en el Habeas Data, es decir en la facultad de las personas de conocer y controlar las informaciones que les conciernen y que están procesados en bancos de datos informatizados.

Las disposiciones legales surgidas como consecuencia del tratamiento automatizado de los datos personales, están destinados a proteger a los titulares de los datos: el individuo, ante los usos abusivos de información que pueden atentar contra los derechos fundamentales, es por ello que las leyes de Protección de Datos Personales, tienen un fuerte vínculo con el Derecho Constitucional, como por ejemplo, tanto en la Constitución española como en otras latinoamericanas se reconoce el deber de uso correcto de la informática y se instituye el Habeas Data, que no es más que un recurso procesal que se erige en garantía en el ejercicio de los derechos sobre la información.

Lo que se ha dado en llamar el Habeas Data, tal como lo ha definido el Dr. Antonio E. Pérez Luño, "constituye, en suma, un cauce procesal para salvar las libertad de la persona en la esfera informática" y cumple una función paralela en el seno de los derechos humanos de la "tercera generación", en

correspondencia con los que en los de la "primera generación" correspondió el Habeas Corpus respecto a al libertad física o de movimientos de las personas.

En latinoamérica, Brasil es el primer país que recogió este postulado en su constitución, más recientemente se han incorporados postulados en la de Perú y Argentina.

La destrucción, manipulación, adulteración o divulgación no autorizada de datos puede ser causada. básicamente, por problemas técnicos, desastres naturales y por seres humanos; son estos últimos los más comunes y que mayores preocupaciones tienen para aquel que tienen información o que tienen el deber de protegerlos de los peligros que semejantes eventualidades pueden producir.

Considero que el empleo razonable de los sistemas de información en interés de la sociedad, así como la protección segura de toda la información, son factores predeterminantes de una actitud de respeto por esta ciencia. En consecuencia, a la par de las aplicaciones informáticas haya que desarrollar valores éticos entre los sujetos vinculados a los sistemas. En tal sentido las normas jurídicas deben establecer claramente el régimen de disciplina informática.

En el caso de Cuba, desde el punto de vista institucional, se constituyó, desde 1988, un Grupo de Expertos de Protección de Datos, que más tarde se denominó Comisión Nacional de Protección de Datos, adscripta al Frente Nacional de la Electrónica.

Esta comisión estaba integrada por especialistas en Informática y en Derecho, los cuales tuvieron a su cargo estudiar y proponer las soluciones técnicas respectivas que se deban adoptar con el fin de garantizar la seguridad de los datos almacenados en los sistemas de información.

Así la comisión asesoró la promulgación por parte del Instituto Nacional de Sistemas Automatizados y Técnicas de Computación (INSAC), del Reglamento de Protección de Datos y Programas Informáticos; en el que quedaron establecidas las funciones de los responsables de la protección de datos y las medidas que se deben hacer cumplir en las entidades que procesen datos por medios informáticos.

A este esfuerzo de la Comisión se incorporó el apoyo decisivo de la UNESCO, para el coauspicio del Laboratorio Latinoamericano de Protección

contra Virus Informático, inaugurado el 11 de mayo de 1993; destinado al intercambio activo de información y productos detectores y descontaminadores de virus; además de ofrecer un marco propicio para el fomento de una cultura de protección y el trabajo técnico de desactivación y aislamiento de virus en el ámbito de toda la región iberoamericana.

Es menester señalar que este laboratorio tuvo como antecedentes inmediatos trabajos realizados en Nicaragua y México, en los que especialistas cubanos han ofrecido su experiencia y productos antivirus y en las jornadas desarrolladas en mayo de este año que dieron cabida a la materialización del Seminario Internacional de Protección contra Virus Informáticos, el Taller Práctico, y el Curso de Problemas Eticos y Jurídicos de la Información Automatizada, que sesionaron en el marco de la inauguración de esta importante institución.

Particular interés debe despertar al que lee estas notas el conocer que este Laboratorio de Protección contra Virus Informáticos tiene entre sus objetivos primordiales servir de centro de formación de profesionales vinculados a la Informática Jurídica en los temas de protección de la información, permitir el intercambio de experiencias legales en los diferentes aspectos que las nuevas tecnologías de la información le plantean al Derecho, así como propiciar la realización de proyectos de investigación relacionados con esta materia e incluso facilitar, en tanto centro coordinador, el intercambio de expertos entre los diferentes países.

Desde el punto de vista de las aplicaciones informáticas al Derecho, para el desarrollo de las políticas y estrategias que rigen la realización de proyectos vinculados a la actividad registral y documentaria que se llevan a cabo por los especialistas del Ministerio de Justicia de Cuba, se han tenido como bases las funciones y atribuciones de esta institución dentro de Sistemas de Organización de la Administración Central del Estado, establecidas por el Decreto Ley N° 67 de 19 de Abril de 1983.

La solución legislativa de protección de datos, abarcó además los regímenes de importación y exportación de productos informáticos, específicamente soportes magnéticos, por lo que las normas jurídicas de protección se hicieron extensivas a las normas de control aduanero.

Otro hecho relevante para Cuba y Latinoamérica en este área cada vez más urgente, dada la cantidad y peligrosidad creciente de los agentes contaminadores de los sistemas informáticos, fue la inauguración el 11 de mayo de 1993 del Laboratorio Latinoamericano de Protección contra Virus Informáticos, el que tiene entre sus objetivos fundamentales contribuir al noble empeño de fomentar en los sujetos vinculados a los sistemas informáticos una cultura y ética de utilización de las innumerables ventajas que la Informática como ciencia aporta a la humanidad.

- Protección legal del Software.

Al igual que en otros países, estuvimos al tanto y practicamos las diferentes vías de protección del software: Protección Industria, Derecho de Autor y una protección especial.

Hoy con la pertenencia de nuestros países a la Organización Mundial del Comercio, todos estamos inmersos en una actualización de nuestras leyes de Derecho de Autor, existen algunos pioneros dentro del área, pero también no se puede perder de vista las experiencias y prácticas desarrolladas en los entornos de esquemas de integración tales como MERCOSUR, NAFTA, Tratado de Libre Comercio y Pacto Andino.

- Contratación Electrónica y Contratos Informáticos.

Por este tema también se ha transitado, se ha legislado particularmentç en Argentina y en Venezuela, y también hay que estudiar el tema en el entorno de los esquemas regionales de integración.

Existen trabajos muy interesantes sobre el EDI.

Para la solución de conflictos se ha reconocido al Tribunal de Conciliación y Arbitraje de Mercosur. (TRICAMER)

En resumen se puede asegurar que existe un Derecho de la Informática en el área, algunos países como Brasil y México, han emprendido proyectos sistematizadores sobre el tema.

En Brasil desde el Ministerio de Ciencia y Tecnología, así como el Programa SOFTEL 2000.

En México desde la Cámara del Senado y el INEGI, a partir del Programa de Informática para el 2000.

c)- ¿Existe una comunidad intelectual en el área preocupada y ocupada en estos temas?:

Sí, existe y debe consolidarse aún más sobre la base de integrarnos en proyectos de investigación y en la búsqueda de soluciones prácticas en correspondencia con las características, tradiciones y realidades jurídicas, sociales y económicas de nuestra región.

Entre los principales centros de investigación, desarrollo y capacitación se encuentra el ILATID, en Argentina, fundado por el Dr. Antonio Millé, que desde hace muchos ha identificado a los problemas generados por la incidencia social de los avances tecnológicos como Derecho de Alta Tecnología.

Con otras realizaciones y orientados a otras áreas de conocimientos: aplicaciones informáticas al Derecho, hay que tener en cuenta: al CINADE, de Uruguay; el Instituto de Investigaciones Jurídicas de la UNAM; el Instituto de Informática Jurídica, de la Universidad Mayor de San Marcos, en Perú, a las experiencias de la Universidad del El Salvador, en Argentina y a la Facultad de Derecho de la Universidad de La Habana, entre otras muchas instituciones académicas, algunas de las cuales, como es el caso de ésta última que alcanza también al estudio del Derecho de la Informática.

d)- ¿Cuáles son las principales realizaciones en materia de Informática Jurídica?.

Atendiendo a la clasificación de las áreas de aplicación de la Informática Jurídica podemos hablar por ejemplo:

Informática Jurídica Documental:

El Sistema Argentino de Informática Jurídica, SAIJ;
El Sistema del Senado en Brasil, PRODASEN;
El Sistema del Congreso del Perú;
El Proyecto MENJUR, Cuba.

Informática Jurídica de Gestión y de auxilio a la toma de decisiones:

El sistema de Controlaría de Uruguay.

e)- ¿Cuál es la realidad y perspectiva de Cuba en las áreas de la Informática Jurídica y el Derecho de la Informática?.

En la actualidad nuestro país asiste a este extraordinario momento en que vive el planeta y se ha planteado un proceso de consolidación de la infraestructura nacional de la información: La Industria Nacional del Software y la Industria de los Contenidos de Información.

Como resultado de este proceso se ha comenzado a gestar un proceso de integración del Derecho en Cuba que exige la evaluación constante de la eficacia social de las normas preexistentes al fenómeno info-telemático y la generación además de nuevas disposiciones, lo cual ya va conformando un segmento del orden legal que reúne en su seno más de 30 disposiciones de diferentes rangos y materias (leyes, decretos leyes, decretos y resoluciones) e incluso la exigencia de adopción de Códigos Eticos por parte de los profesionales vinculados a estas actividades.[2]

También se ha transitado hacia una organización institucional que responda a la infraestructura de la información y que establece la constitución del "Registro de Redes", el "Registro de Distribuidores de Información Electrónica" y el "Registro de Dominios IP", por solo citar algunos ejemplos.

Lo anterior está íntimamente relacionado con la decisión de nuestro país de emprender "Proceso de Informatización de la Sociedad Cubana" en víspera del próximo milenio.

En correspondencia con ello, ya nuestro Estado viene trabajando en el proyecto de documento programático que debe implementar la política trazada, todo lo cual ha sido expresado en el Documento "Lineamientos estratégicos de informatización para el año 2000".

■[2] Correa y otros, "Derecho Informático", pág. 230. Ediciones Depalma, Buenos Aires, 1987.

El ámbito de la Informática Jurídica se viene trabajando en la consolidación de varios proyectos de informatización de los principales Registros: Civil, Actos de Ultima Voluntad, Central de Sancionados. También en un Banco de Datos sobre resoluciones judiciales e instrucciones del Tribunal Supremo Popular. Algunos resultado se han alcanzado en la Fiscalía General de la República. También trabaja en sistemas de información jurídica automatizada (doctrinal y legislativa).

f)¿Cómo acercarse a la realidad de nuestro área para conocerla, intercambiar e integrarnos en la investigación?.

Existe desde el año 1984 un foro sistemático para conocer la realidad de Iberoamérica en estos temas: los Congresos Iberoamericanos de Derecho e Informáticos que tiene como antecedente el I realizado en Santo Domingo, a los que les han sucedido los de Guatemala (1989), Mérida (1992), Bariloche (1994) y La Habana (1996), de los que en sus Actas se recoge un devenir práctico y conceptual sobre todos temas de la mutua incidencia del Derecho y las Nuevas Tecnologías de la Información y la Comunicación.

II. RESPONSABILIDAD PENAL DERIVADA DEL USO INDEBIDO DE LAS NUEVAS TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN: ¿DELITOS INFORMÁTICOS?.

La destrucción, manipulación, adulteración o divulgación no autorizada de datos puede ser causada, básicamente, por problemas técnicos, desastres naturales y por seres humanos; son estos últimos los más comunes y que mayores preocupaciones tienen para aquel que tiene información o que tiene el deber de protegerlos de los peligros que semejantes eventualidades pueden producir.

Como se ha dejado sentado, la Informática no es un fenómeno exclusivamente tecnológico con implicaciones estrictamente positivas. Sus efectos dependen del uso que se les dé. Las computadoras, al permitir un manejo rápido de grandes volúmenes de información, facilitan la concentración y disponibilidad automática de datos de diversa índole, lo que condiciona la necesidad de regular su protección desde el punto de vista de su uso y conservación.

Lo que se ha dado en llamar el dato electrónico, hoy más ya es más adecuado hablar de información digitalizada, debe ser protegido contra factores de riesgo tanto objetivos y subjetivos. Estos últimos generados por conductas

negligentes, culposas o inexpertas, las que condicionan la posibilidad de pérdida, alteración, sustracción o uso inadecuado de la información almacenada en soportes magnéticos o producir alteraciones en el funcionamiento de los sistemas informáticos, llegando a producir incluso un colapso en una actividad bien sea de servicios o productiva.

A menudo se escucha hablar de los perjuicios causados por los virus informáticos, de la práctica ilícita en torno a los sistemas automatizados que tipifican conductas de "fraude", "sabotaje" o "robo" de la información, o de programas "piratas" que penetran en las redes computarizadas y logran destruir o alterar los datos o programas incluso los medios técnicos.

En este segmento del problema me detendré a exponer más detenidamente, por lo que necesariamente me referiré a aspectos "históricos" del tema hasta nuestros días, específicamente con motivo de las II Jornadas del Delito Cibernético, realizadas en Mérida, entre los días 20 a 22 de noviembre.

II.(a) - Algo que ya es historia.

Desde sus orígenes, en 1890, cuando Herman Holleriht inventó un sistema capaz de realizar tabulaciones y, decisivamente, cuando en 1954, se comercializó por primera vez un microprocesador, el hombre se ha empeñado en ofrecer soluciones a los problemas de velocidad, volumen, capacidad y coste de la información.

Así, gracias a los estudios y aplicaciones de los circuitos integrados de silicio, ha logrado una velocidad de procesamiento más de 2000 veces superior a los primeros ordenadores, y reducir su costo en más de 25 veces.

No obstante, la propia complejidad de la técnica impone nuevos límites físicos, tecnológicos y económicos, y el hombre se ha dedicado a buscar soluciones basado en estudios de nuevas aleaciones mecánicas, memorias ópticas, células de memoria tridimensional, que marcan el presente y futuro de la Informática, y que se refleja en todo cuanto está, asociado a las partes físicas de la computadora (hardware), lo que alcanzó también al software, mientras éste era parte indisoluble de las unidades centrales de procesamiento.

Con el desarrollo independiente de la parte lógica (software), se varió este estado de correspondencia y entraron a jugar determinantemente otros factores.

En estos momentos el software es un elemento tan importante o más que las propias computadoras y en el que se han destinado fuertes inversiones al desarrollo de implicaciones y programas al servicio del hombre.

Producto de este vertiginoso desarrollo, hoy se cuenta con programas accesibles y de fácil utilización, pantallas de contacto, teclados y lenguajes sencillos, que han hecho posible la diversidad de aplicaciones informáticas así como el manejo y acceso cada vez más masivo y menos especializado a las técnicas de información.

Unido a este devenir de desarrollo tecnológico, la humanidad ha ido identificando un cambio en los paradigmas en cuanto al soporte de informaciones, pero ninguno ha sido tan trascendental como los que son fruto de la Revolución Informática, hito en el desarrollo social a partir de la cual se comienza a gestar lo que hoy se conoce indistintamente como "Sociedad de la Información" o "Sociedad del Conocimiento" e incluso algunos la identifican como la "Era digital", en cualquiera de ellas encontramos que en el vértice de todas estas realizaciones y como piedra angular sobre la cual se erige la información.

Por eso una de las características de este fin de siglo, denominado "La era de la Información" son, por una parte, la explosión de la información y, por otra, el desarrollo de nuevas tecnologías de información y comunicación. Estas últimas, permiten con facilidad desconcertante y apenas inimaginable, almacenar, recuperar y diseminar la información.

Por tal motivo se le reconoce a la Informática cuatro características las cuales están en directa relación con el efecto multiplicador que ha producido en las actividades económicas y sociales; particularmente en el aumento de la productividad técnica. La primera y principal característica son de permitir mayor velocidad de cálculo que aquella realizada por el hombre. La segunda característica, relacionada con la primera, es la de asociación y relación lógica. Una tercera es la relativa a la memorización, es decir, al almacenamiento de datos,

informaciones, imágenes y sonidos; y una cuarta, es la relativa a la posibilidad de ampliar la comunicación de estos datos, informaciones, imágenes y sonidos.[3]

Pudiéramos decir, además, que estas cuatro características sirven de pauta, además, para dividir metodológicamente esta era de la información, desde la informática en búsqueda de más posibilidades de almacenamiento de información, hasta la informática interactiva en la que estamos inmersos.

Pero la Informática no es un fenómeno exclusivamente tecnológico, con implicaciones estrictamente positivas. Junto a las ventajas que reportan los avances tecnológicos en la información, se manifiestan puntos débiles, problemáticos y riesgos que no eramos capaces de imaginar.

Con estos avances tecnológicos, se han introducido nuevos soportes de datos de dimensiones reducidas, que no sólo son fáciles de ocultar, sino que resulta común su trasiego, con el fin de intercambiar datos y programas.

Esta tecnología ha obligado a reestudiar y crear nuevos mecanismos para proteger la información, los cuales se complican cada vez más, si analizamos que en un inicio se limitaban quizás a un centro de cálculo cerrado, pero ahora se ha extendido al uso de las máquinas interconectadas tanto nacional como internacionalmente, a través de líneas telefónicas.

Por lo que podemos afirmar que el impacto social de las nuevas tecnologías y sus efectos dependen del uso que se les dé.

De ahí que a finales del siglo XX, el balance del desarrollo de la Informática exhiba enormes posibilidades y aciertos, como efectos indeseables. Uno de ellos lo constituyen las manifestaciones de uso indebido de las nuevas tecnologías de la información y la comunicación[4].

■[3] Carlos Ferreyros, "Aspectos metodológicos del delito informático", Notas del curso Nuevas Tecnologías y Derecho, UNED, mayo de 1995. Mérida, España.

■[4] Antonio Enrique Pérez-Luño, "Impacto social de la nuevas tecnologías" pág. 15 Editorial Fundesco, 1987.

La magnitud de los daños[5], es un fenómeno que ha quedado, podemos decir en sentido general, fuera de las legislaciones, pues hasta estos momentos no existe de modo integral un sistema de normas que proteja específicamente a los datos computarizados contra robo, desvío, daño, alteración, destrucción, acceso indebido u otras acciones que afectan de alguna forma la información que se procesa por medio de esta tecnología.

Dichas conductas, tienen su origen desde el propio surgimiento de las aplicaciones informáticas y a pesar del nivel de desarrollo de la sociedad e incidencia de afectaciones en múltiples bienes tutelados o tolerables jurídicamente, aún existe una pobre presencia de respuestas legales a tales actos indebidos.

Muchos autores al tratar el tema, hablan de "Delitos Informáticos", refiriéndose en forma genérica a todas aquellas acciones en que los sujetos se valen de la Informática para realizar sus actos.

En la actualidad, existen dos realidades latentes, algunos códigos penales y leyes especiales –pocos- que recogen en forma de tipos penales, dichas conductas y en cuyo caso puede hablarse propiamente de "delito". Y otra realidad - la más generalizada -, la constituyen las manifestaciones de conductas que valiéndose de las computadoras como medio o fin, transgreden un orden legal establecido o causan un daño, pero no constituyen delitos por no estar tipificadas como conductas antijurídicas en un cuerpo legal, rigiendo en estos casos el principio de nullum pena sine previe llegue penal.

De modo que ante el tema, expresión del impacto negativo de las nuevas tecnologías de la información y la comunicación en la sociedad, por el momento y al parecer aún por un rato, siempre nos estaremos refiriendo, a conductas típicas y a conductas atípicas.[6]

■[5] Se estima que las pérdidas de información, oscila anualmente entre los US$ 3 y 5 millones. Esto en una empresa grande; en una empresa pequeña, la pérdida de información puede significar el fin de su existencia.

■[6] Julio Téllez Valdés, "Derecho Informático", pág. 81. Editorial Instituto de Investigaciones Jurídicas, Serie A: Fuentes, b) texto y estudios legislativos, No. 75. No. 75.

En lo particular, preferimos no hablar de delito para aludir a un comportamiento no tipificado como tal en un cuerpo normativo, por tal motivo hemos preferido al titular este trabajo, en tales supuestos, referirnos a actos indebidos.

Aunque de inicio también hago explícita mi posición en cuanto a compartir el criterio que en la inmensa mayoría de los casos se está en presencia de viejos delitos cometidos por medio de nuevas tecnología. Afortunadamente estas posiciones van ganado espacio en la realidad jurídica en el ámbito mundial y presiento una especie de madurez intelectual y práctica al abordar el tema, dejando de un lado las primeros tendencia de "adjetivación de informático a las nuevas manifestaciones de actos indebidos", no obstante pienso que estamos en el deber de agradecer a los pioneros de estas posiciones y prácticas el haber contribuido al desarrollo, aún no consolidado, de las tendencias más modernas de legislar y enfrentar el tema, tanto desde la instrucción como desde el Derecho.

III.(b) - Dimensión del Problema.

Como se conoce los sistemas informáticos a menudo se utilizan para almacenar datos políticos, económicos, médicos, sociales y personales muy delicados y ofrecen posibilidades ilimitadas de concentración y manejo de información.

La información que se elabora automáticamente y se archiva en las computadoras, es algo vivo, cambiante, dinámica y directamente relacionado con la vida humana en todas las esferas de la sociedad y constituye hoy en día, uno de los patrimonios más valiosos.

En la actualidad la información ha adquirido características de bien social, económico y jurídico autónomo. En cuanto a su forma, se ha separado de su continente tradicional: el paradigma papel, que hoy convive con el soporte digital; sin embargo la información se ha independizado de los mismos sin perder su identidad y su función.

Por otra parte, a la información se le reconoce valor como materia prima fundamental en el cuarto sector industrial. Se identifica además, como un recurso estratégico para el desarrollo; de manera tal, que los cambios estructurales son

palpables en términos de indicadores de crecimiento económico, ya se comienza a distinguir entre países inforricos e infopobres.

También se reconoce, que la aplicación de las nuevas tecnologías de la información y la comunicación al entorno social en general es fuente de un sector productivo en tanto genera bienes y servicios y modos diferentes de realización del comercio internacional.

El uso de estas nuevas tecnologías ha generado importantes beneficios en el tratamiento de los datos; sin embargo, tales beneficios constituyen a la vez un motivo de preocupación, pues la informatización ha resultado otra posibilidad de realizar actos indebidos.

Las acciones generadas en el manejo de las técnicas de computación han sido consideradas como conductas delictivas en el contexto del desarrollo; lo que evidencia la interdependencia entre el nivel de evolución tecnológico, el grado de desarrollo económico y social y la manifestación de tales conductas.

El empleo indebido de dichas técnicas o los atentados contra su integridad y funcionamiento de los sistemas automatizados de información, constituyen o puede constituir una agresión a múltiples intereses, tales como la vida de las personas, los derechos humanos, las libertades fundamentales y la soberanía e independencia de los Estados.

El peligro de que tales hechos se produzcan, se acrecienta cada vez más con la multiplicación de todas las aplicaciones en forma de redes informáticas, lo cual es posible gracias al desarrollo e integración de las técnicas informáticas y de telecomunicaciones, conocido como Telemática.

Con el desarrollo de los sistemas telemáticos, tales como transmisión de datos en paquetes y el correo electrónico, se amplía el horizonte de la acción transgresora, al facilitarse que el hecho que se produzca sea contrario al orden social o jurídico de más de un país; de manera que estos actos indebidos constituyen, además, un reto para el Derecho Internacional, cuando la acción transgresora afecta a más de una jurisdicción nacional.

Sin duda alguna, las manifestaciones de actos indebidos generados por el mal uso de las técnicas informáticas constituye uno de los más complejos y preocupantes fenómenos surgidos de la interacción hombre-máquina.

La complejidad del tema está dada por la propia naturaleza de la Informática, la amplitud y profundidad del avance tecnológico de las técnicas de comunicación y su incidencia en todas las esferas de la vida humana, lo que la ha hecho portadora de profundos cambios en nuestras formas de conductas y modos de pensamientos.

Es una preocupación, porque, ante su manifestación la sociedad en general se encuentra doblemente desarmada; bien sea por la ausencia de una legislación especifica en materia de Informática, o la insuficiencia de las fórmulas legales tradicionales para subsumir en ellos las nuevas formas de instrumentación de la acción, o porque, aún en los casos de tipificación especifica, no están preparados sus órganos de represión y justicia en el manejo técnico necesario para comprender y enfrentar a los sujetos de estas acciones.

A la vez, la falta de una legislación especifica y la escasa preparación del personal de los cuerpos de seguridad del Estado, son factores que en cierta medida han condicionado el grado de proliferación de éstas conductas.

Pero, al parecer, aún no existe una conciencia general de esta relación causa-efecto, pues a la par del desarrollo tecnológico continúan presentes el silencio jurídico y grandes áreas de desrregularización.

Si la informática supone una actividad y ésta se manifiesta en muchos de los ámbitos del quehacer humano es necesario regularla por el Derecho.

Regular todas las actividades relacionadas con la informática en general y con las tecnologías relacionadas con ésta, supone establecer normas jurídicas que fijen un marco regulatorio tanto con relación a las actividades y creaciones informáticas; como la regulación de conductas jurídicas; derechos y obligaciones relacionadas con la Informática.

Pero el horizonte ya empezó a cambiar y se comienza a hablar en el seno de Naciones Unidas de comenzar a trabajar a favor de un marco regulatorio fruto de la colaboración y armonización de nuestras legislaciones nacionales y especialmente de la voluntad de enfrentar coordinadamente esta realidad. Cierto es que es un camino difícil pero transitable.

Por otra parta también ya desde hace algún tiempo la comunidad intelectual viene trabajando en el tema. Sobre el decursar de ambas rutas y con la esperanza de que algún día converjan me referiré a continuación a algunas cuestiones más bien de derecho positivo, otras de hechos; otras de líneas de pensamientos que comparto.

IV. DELITO INFORMÁTICO: ESPECIFICIDAD Y COMPLEJIDAD.

Asistimos a la conceptualización del fenómeno por lo que las referencias que a continuación se relacionan no se deben entender como definitivas, sino más bien son intentos de explicación de tales acciones.

Algunos ejemplos de conceptos constituyen una tipificación legal propia y están contemplados en leyes y códigos penales; otros son citas puramente doctrinales.

Según la Organización para la Cooperación Económica y el Desarrollo (OCDE) delito informático es "Abuso informático, y es cualquier acto ilegal o contrario a la ética o no autorizado que concierne a un tratamiento automático de datos y/o transmisión de datos".[7]

El Departamento Norteamericano de Justicia ha definido delito informático como cualquier acto ilegal para el que es esencial el conocimiento de la tecnología informática para su comisión, investigación y persecución.

Según Correa "delito informático es toda acción dolosa, que provoca un perjuicio a personas o entidades, en cuya comisión intervienen dispositivos utilizados en las actividades informáticas".[8]

■[7] OCDE: Manual de las Naciones Unidas sobre el Desarrollo y Control de Delitos Informáticos, 1994.

■[8] Correa y otros, "Derecho Informático", pág. 230. Ediciones Depalma, Buenos Aires, 1987.

Para el destacado penalista italiano Carlos Sarzana, delito informático es "cualquier comportamiento criminógeno en que la computadora está involucrada como material, objeto o mero símbolo".

Para la Dra. María de la Luz Lima, es el "Conjunto de comportamientos dignos de reproche penal que tienen por instrumento o por objeto a los sistemas o elementos de técnica informática, o que están en relación significativa con ésta, pudiéndose presentar múltiples formas de lesión de variados bienes jurídicos".

Por su parte Luis M. del Pont y Abraham Nadelsticher, lo consideran como "toda acción típica, antijurídica y culpable, pero cuya conservación se usa la tecnología computacional o se afecta a la información contenida en un sistema del tratamiento automatizado de la misma".[9]

El destacado jurista costarricense Juan Diego Castro, reconoce que delito informático es "aquel hecho en el que el que independientemente del perjuicio que pueda causarse a otros bienes jurídicamente tutelados y que eventualmente pueden causar en forma real o ideal y se atacan elementos puramente informáticos."[10]

Sin embargo algunos tratadistas como Parker 1985; han intentado definirlo como "Todo acto intencional asociado de una manera u otra a los ordenadores; en los cuales la víctima habría podido sufrir una pérdida; y cuyo autor ha o habría podido obtener un beneficio".[11]

Otros se circunscriben al aspecto patrimonial del problema y lo definen como el "Conjunto de acciones dolosas que provocan un perjuicio a personas físicas o entidades, sin que sea necesario que ello conlleve un beneficio material para su autor, o viceversa, produce un beneficio ilícito para su autor aun cuando no perjudique de forma ostensible a la víctima".

■[9] Luis M. del Pont y Abraham Nadelsticher, "Delitos de Cuello Blanco". Cuaderno No. 8 del Instituto Nacional de Ciencias Penales (INACIPE), México, 1981.

■[10] D. B. Parker, "Combatte la criminalité informatique". París, Editorial Oros, 1985.

■[11] Notas del Curso "Derecho e Informática", Universidad de Zaragoza, 1991.

Dirk Hanson, en su articulo "Los nuevos alquimistas" dice que delito informático es "una forma de irrumpir y penetrar en los que herramientas del ladrón son, en esencia, un conocimiento de la estructura lógica o los puntos lógicos débiles inherentes a un sistema particular de programación y proceso. Más allá de un conocimiento profundo de la programación, las únicas herramientas que el forajido necesita son un terminal de ordenador y teléfono. No tiene que acercarse en absoluto al escenario del crimen".

Por su parte, Klaus Tiedmann, en Criminalit da Computer, dice: "cometer delito informático la persona que maliciosamente use o entre a una base de datos, sistema de computadoras o red de computadoras o al cualquier parte de la misma con el propósito de diseñar, ejecutar o alterar un esquema o artificio, con el fin de defraudar, obtener dinero, bienes o información".

Para el autor, también comete este delito "el que maliciosamente y a sabiendas y sin autorización intercepta, interfiera, recibe, usa, altera, daña o destruye una computadora, un sistema o red de computadoras o los datos contenidos en la memoria, base, sistema o red".

De manera tal que "no existe una definición que esté reconocida en el plano internacional, lo corriente ha sido ahora que se utilicen definiciones funcionales", tal como apunta un informe de la OCDE " Manual de las Naciones Unidas sobre prevención y control de Delitos Informáticos" (1994).

A1 profundizar en las definiciones expuestas, éstas resultan igualmente vagas, ya que necesariamente tiene que entrar en la descripción de hechos o acciones diversas en móviles, sujetos y bienes jurídicos atacados, todo lo cual apunta tal como lo han considerado muchos estudiosos del tema, a las hipertrofias de los ordenamientos penales que así lo han considerado.

Sin embargo la expresión "Delito Informático" nos motiva además otros comentarios, ya que tal denominación a nuestro juicio resulta literalmente confusa, al parecer Informático califica al género y no a la especie, por eso consideramos que en todo caso serían Delitos contra la Informática, además se trata de una multiplicidad de conductas que se pueden generar que tienen en común utilizar las nuevas tecnologías de la información y la comunicación como medio para cometer el hecho.

No obstante, se habla y se seguirá hablando de los delitos informáticos como término que engloba a dichas acciones, e incluso propio de un tipo de delincuencia.

En términos de tipificación de conductas los especialistas generalmente coinciden en reconocer como delito acciones de fraude informático, falsedad informática, sabotaje informático, acceso no autorizado, interceptación no autorizada, reproducción no autorizada de un programa protegido, reproducción no autorizada de una topografía, los delitos de alteración de datos o programas, espionaje informático, y utilización no autorizada de un equipo informático o de un programa.

La primera tipificación de delitos perpetrados por computadoras o sobre soportes informáticos fue realizada por Lampe en 1975, quien al decir de Sieber, responde, no sólo a un criterio de sistematización vinculado a la característica del procesamiento de datos, sino al mismo tiempo a una separación de diversos tipos criminológicos de conductas.

Primero Lame y más tarde Sieber proponen los siguientes tipos delictivos: fraude por manipulaciones de un computador contra un sistema de procesamiento de datos.

Fraude informático, constituye la forma más frecuente de aparición de conductas desválidas en las sociedades de alto desarrollo tecnológico y constituyen el núcleo criminológico de los llamados "delitos informáticos".

Consiste en el cambio de datos o informaciones ya contenidas en la computadora en cualquier fase de su procesamiento o tratamiento informático, en el que media ánimo de lucro y genera perjuicio a terceros

b) espionaje informático y robo de software.

Es la obtención ilegal de información mediante medios informáticos para su utilización en actos posteriores en el que se busca satisfacer un interés, el cual tiene efectos económicos de gran magnitud.

c) sabotaje informático.

Destrucción o inutilización de datos o programas informáticos dirigidos a causar un perjuicio sobre bienes patrimoniales, tanto para el titular como al usuario del sistema.

O los que se realizan con finalidad política actuando contra la seguridad y defensa de los Estado al dirigir sus actos nocivos a la destrucción o inutilización de sistemas de información sobre armamentos, organización operativa de las fuerzas armadas o ficheros de la policía.

d) robo de servicio.

Robo de tiempo de máquina. Utilización indebida del equipo informático o de los servicios de procesamiento de datos; bien sea en sito o a través de acceso remoto del que puede resultar la obtención ilegal de información.

e) acceso no autorizado a sistemas de procesamiento de datos.

f) ofensas tradicionales en los negocios asistidos por computador.

g) uso de un equipo propio para defraudar o enmascarar acciones punibles.

Otros autores, como el Dr. Julio Téllez, profesor del Instituto de Investigaciones Jurídicas de la UNAM, de México, lo clasifican atendiendo a dos criterios: como instrumento o medio y como fin u objeto, al proponer los supuestos siguientes: Supuestos en que se utilizan las nuevas técnicas como medio u objeto. Falsificación de documentos vía computarizada (tarjetas de crédito, cheques). Variación de los activos y pasivos en la situación contable de las empresas. Planeación o simulación de delitos convencionales (robo, homicidio, fraude). "Robo" de tiempo de computadora. Lectura, sustracción o copiado de información confidencial. Modificación de datos, tanto en la entrada como en la salida. Simulación de servicios no rendidos.

Aprovechamiento indebido o violación de un código para penetrar a un sistema, introduciendo instrucciones inapropiadas.

Variación en cuanto al destino de pequeñas cantidades de dinero hacia una cuenta bancaria específica, método conocido como técnica de salami.

Uso no autorizado de programas de cómputo.

Introducción de instrucciones que provocan interrupciones en la lógica interna de los programas, a fin de obtener beneficios.

Alteración en el funcionamiento de los sistemas.

Obtención de información residual impresa en papel o cinta magnética luego de la ejecución del trabajo.

Acceso áreas informatizadas en forma no autorizada.

h) Intervención en las líneas de comunicación de datos o teleproceso.

Supuestos en que las nuevas técnicas constituyen el fin u objeto del acto indebido.

Programación de instrucciones que producen un bloqueo total al sistema.

Destrucción de programas por cualquier método.

Daño a la memoria.

Atentado físico contra la máquina o sus accesorios (discos, cintas, terminales).

Sabotaje político o terrorismo en que se destruye o surja un apoderamiento de los centros neurálgicos computarizados .

Secuestros de soportes magnéticos en los que figure información valiosa con fines de chantaje o el pago de rescate, entre otros.

Entre los años 1985 y 1989, un Comité Especial de Expertos sobre delitos relacionado con el empleo de computadoras, del Consejo de Europa, se dieron a la tarea de examinar los problemas jurídicos que planteaban los delitos informáticos.

El resultado de este trabajo se conoció en forma de Recomendación que suscribieron el Comité especial y el Comité Europeo para los Problemas de

Delincuencia, que el Consejo de Europa aprobó el 13 de septiembre de 1989, Recomendación N° R (89)9.

Las directrices del Consejo de Europa recogen:

" 1. Lista mínima de los delitos reconocidos normativamente y entre los cuales enuncia a los siguientes:

a) Fraude informático.

b) Falsificación informática.

Daños ocasionados a datos de computadoras.

- Sabotaje informático.

- Acceso no autorizado.

- Intersección no autorizada.

- Reproducción no autorizada de un programa de computadora protegido.

- Reproducción no autorizada de una topografía".

"Lista facultativa que contiene las formas de conductas siguientes:

- Alteración de datos de computadoras o de programas de computadoras.

- Espionaje informático.

- Utilización no autorizada de una computadora.

- Utilización no autorizada de un programa de computadora protegido".

En el informe de la OCDE que ya aludimos con anterioridad se presenta también una lista de propuestas de sistematización de conductas generadas del uso indebido de tecnologías de información y comunicación sean éstas como objeto de delitos o como instrumento para cometerlo.

Al relacionarlas el Informe reconoce que los supuestos que a continuación relacionaremos resultan ser los que más comúnmente se han presentado:

"Manual de las Naciones Unidas sobre prevención y tratamiento de los Delitos Informáticos":

Tipos comunes de delitos informáticos.

- Fraudes cometidos mediante manipulación de computadoras.

- Falsificaciones informáticas.

- Daños o modificaciones de programas o datos computarizados.

- Acceso no autorizado a servicios y sistemas informáticos.

- Reproducción no autorizada de programas informáticos de protección legal".

Las relaciones taxativas de supuestos de actos indebidos siempre quedan incompletas, y además se identifican con figuras delictivas convencionales vigentes en nuestros Código, lo cual no siempre es conveniente para comenzar a estudiar el problema, pero sin lugar a dudas dan medida de la diversidad de sus manifestaciones, las que están íntimamente relacionadas como ya dijimos con anterioridad con la multiplicidad de aplicaciones informáticas.

No obstante consideramos que la propuesta de la OCDE en sí mismo constituye un primer intento de sistematización del fenómeno de la tipología y una importante contribución a la estandarización en el tratamiento del mismo fenómeno, especialmente si consideramos que estamos ante conductas típicas de una delincuencia sin fronteras.

El debate doctrinal se desarrolla en varias direcciones. Algunos especialistas consideran que algunos supuestos no son otra cosa que modalidades de un mismo tipo delictivo, otros estiman que no todas las conductas pueden ser enmarcadas como delitos informáticos en el sentido de una nueva forma de un nuevo tipo de tipología, tal es el caso de la reproducción o utilización no

autorizada de un programa o de una topografía de semiconductores, éstos considerados, como delitos contra la propiedad intelectual o industrial.

Por su parte, otros creen que supuestos tales como los de fraude informático, falsedad informática o espionaje, son modalidades de delitos reconocidos por la doctrina penal, en los que el uso del sistema informático no es otra cosa que el medio de comisión.

Y no faltan los que plantean que la novedad de la acción está en que el bien afectado son los recursos informáticos.

Tal es el caso que la acción recae sobre los elementos físicos donde se pueden dar manifestaciones típicas de hurto, robo o apropiación indebida del equipamiento o parte de éste, incluso la inutilización o destrucción de los mismos, por lo que no estaríamos en presencia de nuevas conductas sino de acciones delictivas a las que le son aplicables las reglas propias de la legislación ordinaria.

Otro supuesto puede ser la destrucción, menoscabo o inutilización de los elementos fiisicos los que podrían subsumirse en las figuras de estragos y daños.

Particular análisis merece el hurto de tiempo de máquina el que se considera un caso atípico como tal hurto de uso.

Ahora bien, cuando se atenta contra el software y la acción recae sobre la información o conjunto de datos almacenados en soportes magnéticos, sin que resulte alterado alguno de los elementos del Hardware, o por lo menos sin que sea necesaria dicha alteración física, aunque pueda ocurrir; entonces el tema merece otro comentario.

Pienso que las acciones sobre el software, por la propia naturaleza de éste -intangible- son las que más interrogantes por no decir las únicas, ofrecen al Derecho.

Un caso, el apoderamiento de ficheros informáticos, en la que la acción puede ser la copia sin destrucción del original.

Tal conducta genera un sinnúmero de situaciones para subsumir el acto en un tipo legal convencional, ya que la sustracción del fichero no conlleva la

acción "tomar o apoderarse" en el sentido literal y jurídico de la definición, tal supuesto es sólo válido en caso de sustracción de soportes magnéticos.[12]

En sentido general tanto de las definiciones como de las tipificaciones de tales actos indebidos podemos extraer varios elementos comunes, las que a su vez están relacionadas con los factores de vulnerabilidad consustanciales a los sistemas informáticos.

A nuestro juicio entre los factores que propician tales conductas y los rasgos comunes que están presentes en la generalidad de ellas se encuentran las siguientes:

- Son conductas diversas que se manifiestan a través de una gama de actos específicos con características muy peculiares, lo cual está dado por la diversidad de aplicaciones informáticas las que abarcan casi todas las esferas sociales por lo tanto íntimamente relacionado con dos factores: densidad de la información y procesos, así como la vulnerabilidad electrónica.

- Ilegales; los sistemas aplicaciones y servicio informático legítimo deben estar realizados en correspondencia con los principios legalmente reconocidos y ajustados a las normas técnicas internacionalmente reconocidos (ISO/9000).

- No éticas; entre las implicaciones sociales de la incidencia de las nuevas tecnologías de la información y la comunicación se encuentra la generación y el fomento de nuevos valores éticos y la adopción de códigos deontológicos. La infracción de las reglas del deber ser siempre está presente en estas conductas.

- Agreden tanto al elemento físico como al lógico de los sistemas de información, lo cual está sustentado en la condición de vulnerabilidad de los medios electrónicos de procesamiento de datos.

- Se utilizan los sistemas informáticos como medios o fin del acto; lo que se corresponde con las reglas de accesibilidad indispensable para el uso de sistemas.

■ [12] Notas del Curso "Derecho e Informática", Universidad de Zaragoza, 1991.

- Atacan varios bienes jurídicos, a veces los propios medios informáticos, ello está derivado tanto de la densidad de la información y procesos, como del factor de vulnerabilidad electrónica presente en toda aplicación informática o telemática.

- Su descubrimiento bastante dificultoso, de altísimo costo económico; lo que está fundamentado en la complejidad de los propios medios o sistemas atacados o utilizados para cometer la acción y el factor humano imprescindible para la materialización de los hechos.

- Los autores operan en condiciones de máxima seguridad, en virtud de estar amparados por conocimientos técnicos fuera del alcance de cualquier individuo no especializado, este supuesto se fundamenta también en la conjugación de dos factores: de complejidad y elemento humano.

Por otra parte, estas conductas suscitan problemas respecto a la determinación de la autoría, la delimitación del inter-crimen y la valoración del perjuicio.

En sentido general, la tipificación de estas acciones requiere la determinación de un sujeto específico.

En muchas ocasiones estas acciones se cometen en el desempeño de las funciones laborales[13], lo que evidentemente es otra característica que pone de manifiesto además los móviles que impulsan al comisor a incurrir en estas acciones.

También es propio, en la manifestación de estas conductas, el hecho de que el sujeto se aprovecha de una ocasión creada o altamente intensificada en el mundo de funciones y organizaciones del sistema tecnológico y económico en que se manifiesta la acción[14]. Al sujeto en muchos casos le motiva demostrar cuan vulnerable es el sistema.

■ [13] Notas del Curso "Derecho e Informática", Universidad de Zaragoza, 1991.

■ [14] Notas del Curso "Derecho e Informática", Universidad de Zaragoza, 1991.

Las acciones de vulnerabilidad de sistemas de información no son nada vulgares, por el contrario se caracterizan por ser sumamente sofisticadas, y donde su mismo carácter técnico, dificulta mucho los actos de comprobación.

En un alto número, no se manifiesta la intencionalidad del autor, y muchas acciones se llegan a realizar por imprudencia.

Debido al uso frecuente y casi natural de las modernas técnicas de computación por parte del público infantil y juvenil, muchas de estas acciones pueden ser cometidas por menores, para los que el acto en sí constituye un juego o una reafirmación.

En otras ocasiones, personas mayores, conscientes del daño que ocasionan o del beneficio que pueden obtener, realizan sus fechorías en auxilio de menores.

Otro de los elementos que se manifiesta en estos casos, es que el comisor del delito no requiere estar presente en el lugar de los hechos ya que la manipulación de los medios necesarios para realizar su acción le permite hacerla a distancia.

Por tal razón el "Manual de las Naciones Unidas sobre la Prevención y Control de los Delitos Informáticos" en su párrafo acerca de las compilaciones debidas al carácter internacional del problema apuntó:

"Las fronteras nacionales, que en el pasado quizás obstaculizasen las actividades de los criminales, han desaparecido prácticamente con la llegada de las telecomunicaciones modernas. Para reunir las pruebas, los investigadores tienen que ser capaces de percatarse y ocuparse de cuestiones internacionales como la extradición y la asistencia recíproca. Al efectuar investigaciones internacionales hay que tener en cuenta los requisitos en materia de pruebas, procedimiento penal y protección de datos que se hallen vigentes en otras jurisdicciones".

De manera que, tal como alude el Manual de referencia: "El elemento internacional en la perpetración de delitos informáticos plantea nuevos problemas y nuevos retos para la ley. Es posible que se tenga acceso a un sistema en un país, que se manipulen los datos en otro, y que las consecuencias se dejen sentir en un tercero. Los datos informáticos pueden operar materialmente en un país, desplazarse electrónicamente a través del mundo, yendo de una red a otra, y

obtener fácilmente acceso a bases de datos situadas en un continente diferente. El resultado de todo esto es que hay que tratar con soberanías, jurisdicciones, leyes y normas diferentes. Más que en el caso de cualquier otro delito internacional, (la velocidad, movilidad, flexibilidad, importancia y valor de los delitos informáticos, la determinación del locus delicti (lugar del delito) influirá en la capacidad de un país determinado para castigar el delito. ¿Se basará la sanción en la jurisdicción territorial y en el derecho nacional, o habrá que aplicar principios extraterritoriales?".

Pueden ser víctima de estos actos cualquier persona individual o colectiva: bancos, compañías de seguros, servicios postales, organizaciones de seguridad social, bancos de datos de asistencia médica.

En los supuestos de entidades bien sean publicas o privadas, serán particularmente propicias aquellas instituciones con escaso o nulo nivel de seguridad informática.

También pueden ser víctimas titulares y demás beneficiarios legítimos de los sistemas informáticos ya sean usuarios directos o terceros.

Conjuntamente con su manifestación en la sociedad se genera un lenguaje en términos y modalidades propias que hacen más difícil su detección y comprensión para quienes no son especialistas en el área de informática.

Entre otros elementos que gravitan sobre el llamado delito informático haciendo más difícil su detección y sanción, es el hecho de que un elevado número de casos es descubierto al azar, ya sea por tratarse de situaciones no previstas por los mismos técnicos de seguridad, o por la inobservancia de las normas de seguridad por parte de los usuarios del sistema.

En las condiciones en que se operan estas acciones se dificulta la identificación de los autores, permitiéndoles a éstos gozar de los beneficios en absoluto grado de impunidad.

Al supuesto anterior se suma en que un alto porcentaje de casos descubiertos no son denunciados por distintas razones, entre otras, dificultad de detectar estas conductas debido a las condiciones y rapidez en que pueden ser manifestadas, las dificultades técnicas para probar el cuerpo del delito y el temor de evidenciar fallos de seguridad en los sistemas de información.

Esta situación ha generado que se considere que las acciones perpetradas en conexión con los medios informáticos son los casos de más índice de cifras negras en las estadísticas de eficacia policial y judicial.

Según J. Carroll "los delitos informáticos constituyen probablemente el ejemplo más importante de encubrimiento de la realidad desde Watergate" y al referirse al respecto apunta "es difícil determinar de forma exacta y fiable la magnitud de las pérdidas y el número real de delitos penales.

En un Coloquio sobre delitos informáticos y otros delitos contra tecnología informática, convocado y realizado en Wuzburgo, Alemania, en octubre de 1992, la Asociación de Internacional de Derecho Penal presentó un informe sobre los delitos informáticos basado en informes de sus países miembros, según el cual solamente el 5% de los delitos informáticos eran denunciados a las autoridades encargadas de hacer cumplir la ley, por eso sobre este particular me referiré a continuación.

IV. CAUSAS QUE GENERAN LAS CIFRAS NEGRAS.

Varias son las causas por la cual se generan estas cifras negras. Una de ellas es la ausencia de medios adecuados para la detección y control de los hechos; pues como se conoce no siempre se cuenta con un sistema de seguridad en las entidades afectadas.

Por otra parte, la víctima desconoce el hecho la mayoría de las veces o, aún conociéndolo y sospechando fundamentalmente quién lo cometió, tiene dificultades para probar ambas cosas, tanto la perpetración del hecho como la figura del autor.

Descubrir el hecho no resulta fácil, las propias características del mismo lo impiden: por los medios que emplean las que son sólo conocidos por especialistas; por la facilidad del autor de borrar las huellas; por el tiempo que puede mediar entre las manifestaciones de la acción y la manifestación de los efectos, condiciones que afectan además a la realización de las pruebas para la substanciación del proceso.

En otras muchas ocasiones, la víctima no denuncia los hechos, pues teme reconocer que ha sido sujeto de uno o varios de estos comportamientos; o lo que es peor, evidenciar la ausencia o ineficacia de sus medidas de seguridad; también en muchos casos la víctima desconfía la efectividad del proceso jurisdiccional para enfrentar el caso; bien sea por la falta de mecanismos adecuados o por la ausencia de una legislación que contemple las acciones y determine las medidas a imponer.

De manera que las acciones generadas por el uso indebido de la Informática y la Comunicación pueden estar relacionada a figuras convencionales tales como el hurto, robo, fraude, estafa, espionaje, pero que al realizarse con auxilio de medios informáticos exigen de un reanálisis de los elementos típicos a través de los cuales se pueden subsumir estas acciones con las figuras delictivas vigentes.

Por otra parte, es importante resaltar también que estas acciones generadas por el uso indebido de las modernas tecnologías pueden tener rasgos totalmente nuevos y que no encuentran cabida en figuras convencionales cual puede ser por sólo citar dos ejemplos:

El productor y distribuidor de programas de efectos nocivos (virus informáticos, bombas lógicas, gusanos, entras manifestaciones);

el intruso en las redes; pero, sólo apuntamos la idea ya que sobre el tema volveremos en lo adelante.

Recurrimos nuevamente al Manual de la OCDE para resumir todo que hemos querido resaltar hasta este momento y que constituye el planteamiento problemático del tema para adentrarnos en consideraciones más particulares.

E1 Manual expresa lo siguiente: "(...) esta proliferación y ampliación de las tecnologías informáticas ofrece un aspecto negativo: ha abierto la puerta a conductas antisociales que se manifiestan de formas que hasta ahora no era posible imaginar. Los sistemas de computadoras ofrecen oportunidades nuevas y sumamente complicadas de infringir la ley, y han creado la posibilidad de cometer delitos de tipo tradicional en formas no tradicionales. La sociedad sufre las consecuencias económicas de los delitos relacionados con el uso de computadoras, pero la verdad es que recurren a sistemas computarizados para prácticamente todas las actividades de la vida: desde el control de la circulación de autobuses, trenes y aviones, hasta la coordinación de los servicios médicos o la seguridad nacional. El más pequeño desliz en el funcionamiento de esos sistemas puede representar un peligro para la vida humana. La rápida expansión transnacional de las redes de computadoras en gran escala y la utilización de líneas telefónicas corrientes aumentan la vulnerabilidad de esos sistemas y las posibilidades de uso indebido o de actos delictivos. Las consecuencias del delito informático pueden suponer importantes costos económicos y un elevado precio en términos de seguridad humana."

V. CONSIDERACIONES SOBRE LAS EXPERIENCIAS LEGISLATIVAS EN EL ÁMBITO INTERNACIONAL.

Ante la aparición de estas acciones en los países que se ha legislado sobre la materia, se han puesto en práctica dos vías de solución legislativa:

a) dedican un título a los llamados delitos informáticos.-

Agregar las figuras que se puedan generar por estas acciones a continuación de los delitos convencionales que puedan tener relación, o la inclusión de dichas acciones como figuras agravadas, según sea el caso.

Estas técnicas tienen partidarios y detractores, en lo particular estimo que es saludable hacer la revisión de los delitos convencionales y en lo posible atemperar su formulación a las nuevas condiciones de posibilidad de materialización de la acción por medios informáticos, pero en ningún caso debe apuntar a la adjetivación de "informáticos" de tales acciones porque en realidad lo que puede cambiar es el medio de comisión en algunos casos, en otros de lo que se trata es de delimitar el alcance y naturaleza del bien protegido.

Por otra parte, la consideración como delito informático es portadora de una lista prácticamente infinita -en virtud de las posibilidades que brinda la técnica- de acciones que pueden constituir delitos, cuya práctica ha demostrado en la casi generalidad de los casos, la insuficiencia de su aplicación a hechos concretos, por razones múltiples que van desde la pronta obsolescencia de la descripción de la acción hasta la falta de medios de prueba para demostrar el hecho.

En otra dirección, pienso que en realidad ante la existencia y dependencia de los sistemas informáticos, tal como apuntamos anteriormente, el bien jurídico a tutelar es la "Seguridad Informática", toda vez que es el sistema de normas de todo tipo adoptadas en los diferentes entornos informáticos para garantizar la integridad, disponibilidad y confidencialidad de los datos contenidos en dichos sistemas, por lo tanto las acciones atentan indiscutiblemente contra estos tres elementos consustanciales al tratamiento de la información y al desarrollo de los sistemas de tratamiento y comunicación de ésta.

Dichos elementos son tangibles y se pueden establecer con normas sustantivas que al ser violados -por culpa o negligencia- constituirían delitos.

En otro orden de cosas, es sabido también que existe una tendencia a regular los llamados "delitos informáticos" y los llamados derechos inmateriales en general, por legislaciones especiales, que en un mismo cuerpo legal especial se establezcan las normas sustantivas y las normas sancionadoras -medidas administrativas o penales- aplicables ante incumplimiento.

Generalmente, éstas modalidades han sido el fruto de primeras intentos legislativos en materia de Informática, que abarcan, además, áreas muy particulares de aplicación -uso de ficheros automatizados, protección de datos

personales, medios audiovisuales- que son legislaciones nacidas ya a finales de la década de los 60 en los principales países desarrollados, obviamente.

Toda esta experiencia legislativa ha ido llegando como práctica al resto de los países, y nos permite evaluar los resultados en la aplicación y eficacia de las mismas.

Entre las figuras más nítidas y realmente nuevas nacidas en la interacción hombre-máquina se encuentran las siguientes:

- El creador de virus informáticos o programas informáticos destinados a realizar acciones con fines de lucro;

- El distribuidor de virus informáticos o de informaciones sobre la elaboración de programas con fines "malignos".

- El "intruso" -acceso no autorizado- en las redes de información electrónica y en los sistemas informáticos.

Hay otras figuras que se generan en cierta forma de éstas, como la distribución y venta no autorizada de información electrónica.

Además, la consideración de este tipo de delito exige la delimitación de qué información es susceptible de estas normas, pues hay que recordar que la información es un recurso estratégico.

Este tipo de acciones tiene un punto de contacto con la protección de los datos personales, cuyos principios han sido reconocidos por Naciones Unidas.

En el "Manual de las Naciones Unidas sobre Prevención y Control de Delitos Informáticos" se dedica el Título II a la exposición de las leyes penales sustantivas que protegen a los poseedores de datos y de información.

Haciendo un muy breve recorrido por los antecedentes del tema de la Protección de Datos y las experiencias nacionales en la elaboración de los estatutos jurídicos que conforman el régimen legal vigente en esos países.

Para concluir con el tema de las conductas típicas en esta mirada internacional, podemos decir además, que un estudio comparativo de la

experiencia legislativa evidencia que las sanciones ante tales conductas abarcan tanto la multa administrativa, para casos no previstos en la legislación penal pero sí en legislaciones especiales, y el binomio alternativo o no de multa y privación de libertad, en caso de legislaciones penales.

En cuanto a la sanción también hay criterios divergentes, pues algunos estudiosos insisten en que debe ser una sanción penal, por el principio de proporcionalidad de las penas, pues son cuantiosos los daños que pueden ocasionar, lo que supera el marco impositivo por la vía administrativa. Además del valor ejemplarizante de la sanción penal.

En cuanto al tema apelo más al desarrollo de las tendencias de política penal al amparo del desarrollo del Derecho Penal y de las propias condiciones y tradiciones jurídicas de cada país.

VI. LA SEGURIDAD INFORMÁTICA COMO OBJETO DE TUTELA JURÍDICA. UNA PROPUESTA PARA LA MODIFICACIÓN DEL ACTUAL CÓDIGO PENAL CUBANO.

El desarrollo creciente de las aplicaciones de la Informática en Cuba ha incrementado su dependencia a los sistemas automatizados.

Estos sistemas se pueden ver amenazados por diferentes acciones que pueden poner en peligro actividades tan importantes como la salud (fundamentalmente en relación con el diagnóstico clínico), las investigaciones científicas, los controles económicos y financieros, la automatización industrial, los servicios de reserva de pasajes, hoteles y otras capacidades, el pago de la seguridad social, el cobro de servicios como el telefónico, la electricidad, el gas, entre otros, todos los cuales al ser afectados causarían cuantiosos daños económicos y sociales.

Los actos nocivos generados por medios informáticos o contra estos en Cuba, al parecer no encuentran por parte del Derecho una respuesta enérgica pues obviamente se trata de nuevas conductas que se han generado o incrementado con posterioridad a las principales modificaciones de la legislación penal vigente. Pero la realidad es que existe un conjunto de tipos delictivos vigentes que resultan suficientes para enfrentar una diversidad de conductas indebidas, no obstante pensamos que como toda obra humana, nuestro Código es perfectible y que ante los desafíos tecnológicos generados por un sostenido desarrollo informático en un

país es necesario emprender estudios multidisciplinarios para su estudio y cuando proceda introducir las modificaciones que resulten necesarias.

Por ello, en la actualidad constituye un imperativo buscar una respuesta a tales acciones pues esa impunidad puede constituir un elemento que propicie la manifestación continua de tales aciones, de hecho en los últimos tiempos se nota un incremento en la incidencia de hechos.

Estas afirmaciones se basan en la experiencia de la Comisión Nacional de Protección de Datos, creada desde 1988, la cual desde entonces comenzó a estudiar el problema y a sugerir la implementación de un sistema integral de Protección de la Información.

Dicho sistema de protección está sustentado en el establecimiento de un régimen de Disciplina Informática que comprende todas las normas de uso y conservación de los sistemas automatizados y los datos en ellos contenidos, esto se realiza sobre la base del establecimiento del registro nacional de cada virus que existe o entra en el país, un sistema de alerta a todas las entidades y la realización de una versión en software de protección contra cada agente infeccioso, así como el establecimiento de medidas de protección entre las cuales se encuentra las modificaciones realizadas al Reglamento de Ferias y Exposiciones, en el sentido de disponer el control de protección de la información a todo expositor tanto nacional como extranjero, en evitación de la propagación de virus informáticos por el intercambio de información en soportes infectados y la propagación de nuevos de nuevos virus ya que éstos son detectados a su entrada al país.

Las cifras demuestran la efectividad de estas medidas. No hay que olvidar que según datos oficiales del Virus Test Center (VTC) de la Universidad de Hamburgo, aparecen diez nuevos virus informáticos como promedio diario en el mundo.

En Cuba donde hay alrededor de 80.000 computadoras que se utilizan en todos los sectores de la economía, han sido, detectados y aislados 141 virus, de un total de más de 10.000 virus existentes en el ámbito mundial. De esos 141 virus se han podido determinar que 14 de ellos son autóctonos o hechos para surtir efectos en Cuba.

De esos 141 detectados, no todos han llegado a propagarse por la eficacia en las medidas de protección.

También se ha trabajado en la formación de una cultura de utilización de las técnicas informáticas y en la formación de nuevos valores éticos.

Otras normas han sido recogidas en textos de limitado rango jurídico, como fue en su momento la Resolución N° 3 "Reglamento de Protección de Datos y Programas de Computación" promulgada por el INSAC, que ya no es un organismo de la Administración Central del Estado y cuyas funciones han pasado al Ministerio de la Industria Sideromecánica y la Electrónica. En tanto otras normas han sido establecidas por el Ministerio del Interior a través de Instrucciones.

En cuanto a este último Ministerio cabe señalar que en un esfuerzo sostenido por actualizar y atemperar la legislación vigente en materia de protección de la información, no sólo ha elaborado algunas normas de inferior rango jurídico, como resoluciones, sino recientemente aprobó un Reglamento que regula lo concerniente a la Seguridad Informática, lo que permite el análisis planteado, como objeto de tutela jurídica.

De igual forma en 1995 a través de un Decreto de Contravenciones se establecieron las primeras medidas administrativas, que sancionan conductas contrarias a la protección de la información que se procesa por medios informáticos.

Pero todo el esfuerzo que hasta hoy se ha realizado, no sería todo lo eficaz que queremos y necesitamos si no se complementa con otras acciones de orden práctico, como es la preparación del personal de instrucción policial y judicial.

No puede entenderse que contamos con un universo jurídico general, coherente, sistémico y sistematizador de las reglas de conductas en materia de Informática y comunicaciones electrónicas, pero estamos trabajando por ello.

Algunas disposiciones abarcan sólo una parte del problema, el virus informático, preferiría que fuera a los programas dañinos en general.

VII. PRESENTACION DEL SOFTWARE ROGER.

Existen varios tipos de software diseñados especialmente para modificar o destruir sistemas de computación o datos informatizados.

A estos tipos de programas se les conoce dentro del medio como Software Roger[15], y dentro de ésta denominación genérica se agrupan cuatro tipos de programas: el Caballo de Troya, el Gusano, la Bomba de Tiempo, el Virus Informático.

A estos tipos de programas se le llaman genéricamente y erróneamente: "Virus Informáticos".

Sin embargo, es preciso destacar que existen substanciales diferencias entre cada uno de ellos en virtud de las técnicas de elaboración, los objetivos que persiguen y la forma de manifestarse, por eso no es correcto la consideración de que todos son Virus Informáticos.

VII. (a) - El Caballo de Troya

Un Caballo de Troya es un programa legítimo que contiene una sección de "código oculto", y a primera vista, parece un programa inofensivo, identificado generalmente con un nombre provocativo, que en pleno siglo XX "reproduce" el pasaje mítico del Caballo de la Iliada.

Este programa puede permanecer inactivo por un largo período de tiempo antes de activarse. Otro rasgo importante es que al carecer del efecto de autorréplica; su código pernicioso se activa una sola vez.

Este tipo de programa se utiliza para extorsionar funciones rutinarias provocando que el programa realice tareas no autorizadas, tales como la habilitación de cuentas bancarias a nombre de alguien violando todo el trámite de banco, incluso el depósito, o el otorgamiento indebido de un salario o beneficio de seguridad social.

■ [15] Notas del Curso "Derecho e Informática", Universidad de Zaragoza, 1991.

En los sistemas bancarios también se han introducido programas que contienen instrucciones que obligan al sistema a realizar operaciones de redondeo de cifras en los procesos de actualización de cuentas bancarias y depositar dichos resultados en una cuenta habilitada, proceso que se repite automáticamente infinidad de veces, sin ulterior intervención del autor; este método automático de fraude es comúnmente conocido como "técnica de salami".

Otro empleo malicioso que se le ha dado a este tipo de programas es para atacar los sistemas de empresas, introduciendo por vía legítima los programas en determinado entorno informático.

El "software lock" es un tipo de Caballo de Troya, que funciona como un dispositivo capaz de trabar un programa una vez que sea activado. También se manifiestan como un "crash programs".

VII. (b) - La Bomba de tiempo o lógica

La Bomba de Tiempo, conocida también como Bomba Lógica, es un conjunto de instrucciones que se autoejecutan en un momento determinado, dada determinadas condiciones, como puede ser la coincidencia de determinada fecha o la secuencia de algunas teclas.

Se reconoce como el método más común empleado para perpetrar sabotaje por medios informáticos, y se clasifica como un programa de actuación retardada, ya que su efecto puede ser el de destruir un programa o sistema computacional, o la introducción de una "rutina-cáncer" que distorsiona el funcionamiento del sistema del propio equipo.

VII. (c)- El Gusano

El Gusano, es un programa con identidad propia, que una vez que ha sido abierto, busca espacio libre en la memoria interna de la computadora y se autograba en dicha memoria hasta el desbordamiento físico de la misma.

Este tipo de algoritmo está orientado a que los segmentos de programas que se van generando mantengan comunicación con el segmento de programa por el que fueron creados, lo que indudablemente da el efecto de anillado de los

gusanos naturales. Su acción se manifiesta generalmente en la lentitud de ejecución del sistema.

El gusano está diseñado para atacar fundamentalmente sistemas de comunicación. Los programas que se autotransmiten o exigen de la acción del usuario para transmitirse a diferentes direcciones electrónicas.

Por ello su presencia es típica en los sistemas de redes, particularmente proclive en entornos de redes públicas de comunicaciones y en redes locales, donde se reproduce en cada una de las terminales, hasta que la cantidad de memoria que ocupa es tal, que ocasiona la caída o fallo del mismo.

El medio de propagación de estos programas lo constituye el correo electrónico, especialmente para atacar sistemas unidos en una misma red.

Por su capacidad de autotransmisión entendida en ocasiones como autorreproducción puede considerarse un antecedente técnico de los virus informáticos, más su diferencia fundamental es el carácter de identidad propia con respecto al virus informático.

VII. (d) - El Virus Informático

La utilización de las técnicas de elaboración típica del Caballo de Troya -código oculto-, de la Bomba de tiempo -activación bajo determinadas condiciones- o del Gusano -autotransmisión-, en la elaboración del Virus, es lo que ha originado en cierta forma el criterio de identificación de que todos estos programas son Virus Informáticos, pero tal como hemos expuesto no lo son, entonces ¿qué es un Virus Informático?.

El Virus Informático es un segmento de programa de computación con capacidad para autorreproducirse y que al ser ejecutado cambia la estructura del software del sistema y destruye o altera programas o datos, o provoca otras acciones nocivas, sin autorización ni conocimiento del operador[16].

■ [16] Notas del Curso "Derecho e Informática", Universidad de Zaragoza, 1991.

Su capacidad de autorreprodución, como técnica de programación, es lo que nos permite reconocer su analogía con los virus biológicos.

La elaboración y distribución de virus informáticos, es una de las diversas conductas disválidas que se manifiestan en la actualidad en grados realmente alarmantes. A sus antecedentes, características y tratamiento como acciones constitutivas de Responsabilidad me referiré en los tópicos siguientes.

VIII. OTRA CONSECUENCIA DEL SOFTWARE ROGER

La analogía entre virus informáticos y virus biológico ha traído como consecuencia la asimilación por la Informática de otros términos tales como "profilaxis, vacuna, epidemia, infección, contagio, tiempo de incubación, antídoto, cuarentena", los que si bien no tienen en el medio una interpretación literal, sí su dominio y alcance en el lenguaje natural favorecen la interpretación y explicación de los nuevos fenómenos y la asimilación análoga también de determinadas prácticas las que por supuesto son ajustadas al entorno informático.

El chequeo de todo software nuevo y su registro en el control de la entidad es un ejemplo de medidas profilácticas y una acción muy importante en caso de que el virus necesite un tiempo de incubación para provocar su efecto.

Para comprender mejor todas estas manifestaciones es preciso conocer todo en cuanto al surgimiento y devenir en el tiempo de los virus; pero, la historia y evolución de los Virus Informáticos ha sido muy bien desarrollada por algunos autores cubanos, entre ellos el Ing. Edgar Guadis autor de una enciclopedia electrónica sobre el tema, por lo que sólo motivo a los interesados a que vayan a las fuentes originales[17] para que puedan conocer más sobre el tema, sólo me concentraré en los elementos que tipifican a los virus y a algunos argumentos jurídicos esgrimidos en su defensa desde su surgimiento.

La historia de los virus informáticos se remonta a los años cincuenta. Los primeros programas con fines de destrucción o alteración de información, fueron diseñados como medios de protección de Software con el ánimo de impedir su reproducción o ejecución no autorizada.

■[17]

Así quien intentase reproducir esos programas, se llevaría también, sin saberlo, unas instrucciones dentro del programa que copie, que no sólo impediría la ejecución del software pirateado, sino que destruiría toda la información de la computadora utilizada para el efecto.

De modo que podemos decir que los primeros virus, tuvieron origen protector, pero constituían una práctica de justicia por mano propia, donde se manifestaba una sed de venganza, más que lograr la equidad y resarcirse de los perjuicios ocasionados por el acto de piratería informática.

No es posible reconocer al virus como medio de protección, aunque sí reconozco el fin legítimo de protegerse, pero la propia informática brinda otros medios, uno de ellos puede ser la criptología -reconocido procedimiento que garantiza la confidencialidad y la autenticidad de la información-, a los que no se les puede imputar ineficacia porque los virus no han impedido tampoco los actos de piratería.

No es válido argumentar legítima defensa en un acto de premeditación como es la creación de un virus. Otro principio es válido, no puede causarse un mal mayor para defenderse de un daño, pues queda patente que el autor de un virus no se detiene a evaluar el perjuicio que su programa puede acarrear.

También fueron diseñados programas similares a los que hoy tipificamos como virus, para sabotear la ejecución de un programa, muchas de estas acciones de sabotaje perseguían un fin lucrativo o eran acciones en el que el autor pretendía reparar un daño, a veces en el plano laboral, que la entidad le había ocasionado.

En la actualidad ya no se puede decir que los móviles son puramente de protección, aunque reitero, protegerse empleando como medio un virus es totalmente ilegítimo.

Para la mejor comprensión de las implicaciones generada por la acción de los virus informáticos, es preciso descomponer la misma a partir de relacionar las características esenciales de estos programas.

VIII. (a) - Características de los virus informáticos

Del concepto de virus informático podemos extraer los elementos típicos que permiten determinar que estamos en presencia de un Virus. Estos son:

1. Es un segmento de código ejecutable: Esta característica implica que el conjunto de instrucciones que contiene el "programa" está orientada a que sólo bajo determinadas condiciones -la coincidencia de frases, nombres, fechas, lugares- se activen sus efectos.

Por ejemplo, el virus "Martes 13", se ejecuta al encenderse una máquina en la que la fecha calendario del equipo coincida con esa fecha. Por su parte la acción del virus 1530, se materializa al teclearse la 1530 a vez, otros como el virus Stoned anuncian su presencia al momento de la infección, pero ocasionan el daño al azar.

2. Producen un daño: Estos programas han sido diseñados para ocasionar un daño, cuyos efectos pueden determinarse inmediatamente, a corto plazo o largo plazo.

Los daños pueden ocasionarse tanto al hardware como al software. En cuanto a la información, la misma puede ser destruida total o parcialmente y también puede ser alterada, lo cual puede ser aún más peligroso, especialmente en sistemas de información diseñados para el auxilio en la toma de decisiones, como por ejemplo los diagnósticos médicos.

Con el correr del tiempo estos programas han aumentado sorpresivamente su capacidad destructiva.

Desde el punto de vista económico el daño que se produce con este tipo de acciones cuando se dirigen a bienes patrimoniales resulta de alto valor económico. Este daño puede derivarse de una o varias acciones, también pueden tener carácter continuado, o se manifiestan en infinidad de operaciones por un importe mínimo, modus operandi típico cuando se emplean técnicas de salami.

La lesividad de estas acciones se acentúa en la actualidad debido a la interconexión entre las actividades económicas, viéndose afectados varios receptores informáticos, por lo que el perjuicio aumenta considerablemente, esto es lo que se conoce como efecto de cascada, lo que además dificulta mucho la cuantificación del perjuicio.

La concurrencia en el delito de daños se determina por la producción efectiva de la destrucción o inutilización, admitiéndose las formas imperfectas de ejecución. Quizás el ejemplo más común sea determinar si la introducción de una rutina destructiva en el programa constituye un acto ejecutivo punible -tentativa- o uno preparatorio impune.

3.- Tienen la capacidad de autorreproducción: La reproducción parte de la existencia de un código "padre" encargado de iniciar la epidemia vírica.

Los segmentos de virus son capaces de reproducirse infinidad de veces en soportes magnéticos, al generar copias de sí mismos de forma homogénea o en parte discreta, en un fichero, disco o unidad física distinta a la que ocupa.

Esta condición conlleva a la multiplicación del virus con pocos o ningún esfuerzo y sin disponer el autor apenas de recursos, basta que el virus sea creado e introducido en determinado entorno para que pueda ser propagado, sin limitaciones de tiempo y espacio, incluso trasladarse de un país a otro, pudiendo establecerse cadenas mundiales de propagación de los virus informáticos.

Ello se debe a que el virus informático una vez que está en una computadora puede tomar el control temporal del sistema operativo o en ocasiones en los programas ejecutables, a los que infectan y convierte en un canal transmisor, por ende al ser ejecutado, trasmite el virus.

En estos casos cada vez que entra en contacto con un software no infectado, se autorreproduce en el mismo, de ahí que todo ambiente promiscuo de intercambio de disquetes y programas sea un entorno favorable para la fácil diseminación del software infeccioso.

Es importante resaltar además que por las mismas características de autorreproducción y objetivos para los que fueron creados, siempre que se den las condiciones mínimas necesarias, el daño que pueden ocasionar irremediablemente lo causará y de eso están conscientes sus autores.

Al igual que el efecto de daño se ha ido sofisticando, la capacidad reproductiva adquiere nuevas modalidades de presentación.

4.- No tiene identidad propia: Los virus informáticos al carecer de identidad propia, es decir, al no ser programas sino segmentos de código, tienen

una ejecución parasitaria para lo cual requieren endosarse en los programas ejecutables, a los que añade la tarea adicional la ejecución del propio virus.

Por tal condición el propio usuario -víctima de la acción- involuntariamente provoca la activación del virus al ejecutar el programa que lo contiene; que son generalmente los de uso más frecuente: procesadores de texto u hojas de cálculo y especialmente los propios programas ejecutables del sistema operativo, que son los que más se utilizan por los creadores de virus dada su estandarización en el mundo informático.

Así atendiendo a las partes que modifican los virus en su ataque éstos se clasifican en: Virus del sector de arranque y Virus de Programas.[18]

Hoy en día tienen gran presencia los Virus Macro que han introducido modificaciones en las concepciones de clasificación, por lo que resulta más conveniente hablar de virus que atacan al sector de arranque y virus de ficheros, entendiendo así que un fichero puede ser un programa ejecutable o un documento.

5.- Se manifiestan a través de diferentes acciones: Por la diversidad de manifestaciones, sólo limitada por la creatividad de sus autores, no se puede hablar de un "síntoma o patología" de los virus.

El abanico de manifestaciones abarca tanto desde el simple mensaje en pantalla para saludar o dar a conocer la presencia del virus en su máquina, así como la disminución de la velocidad de ejecución de las operaciones en su computadora.

Esta característica ha servido de base para la clasificación de los virus en benignos: el simple mensaje o en malignos: cuando hay afectación al sistema o los datos.

Tal clasificación es inaceptable, ya que toda acción de los virus afecta el proceso de tratamiento de información, lo menos que hace es interrumpirlo y ese tiempo es irrecuperable y tiene un costo.

■ [18] Notas del Curso "Derecho e Informática", Universidad de Zaragoza, 1991.

En síntesis el efecto maligno de los virus está dado en:

- comparte tiempo de ejecución;

- comparte memoria; y,

- comparte espacio en el disco.

6.- Son códigos residentes: Al carecer de identidad propia, es decir no ser un programa sino un segmento de código, los virus necesitan alojarse en la memoria de la máquina, para poder obtener el control permanente de funciones del sistema operativo.

7.- Su funcionamiento comprende dos fases definidas: Una primera fase es de infección o réplica. En analogía con los virus biológicos esta seria la etapa de incubación, pero esta etapa de "ocultamiento" es válida a su vez para la propagación, pues el código oculto se reproducirá todas las veces que sea posible.

La segunda fase es de ejecución, en virtud de la cual el código se activa al responder a la acción para la cual ha sido programado: la introducción de una cadena especial de caracteres, una fecha determinada o un tope de autocopias del virus alojado, la fase de ejecución se materializa en la consecución de efecto nocivo del virus.

Es importante resaltar que la acción de infección es inmediata.

8.- No muestran el rostro: Los virus son diseñados para ser introducidos en los sistemas sin que se note su presencia, por eso sus creadores los enmascaran, algunos utilizan en este enmascaramiento técnicas propias de los otros programas Roger que enunciamos con anterioridad.

De las características de los virus se puede concluir, además, que en todo acto de creación de un virus existe premeditación; ningún código o segmento de programa con estas características puede ser creado al azar.

VIII. (b).- La distribución de los virus informáticos y programas dañinos en general.

Comentario aparte merece la distribución del virus, los programas dañinos en general. Esta puede realizarse de manera consciente o inconscientemente, y puede darse por medios tradicionales, o en soportes magnéticos, así como a través de las redes.

De manera consciente el autor del virus, o un tercero, puede dar inicio a una cadena de contagio, basada en las características de reproducción de los virus. Es obvio que para cumplir sus objetivos estos sujetos se valen de fisuras en los sistemas de seguridad o violan la disciplina informática.

En el supuesto anterior el medio informático es el canal de distribución.

Pero en otros supuestos la distribución se da mediante la difusión de la información sobre virus y resulta posible mediante la publicación del listado completo de virus.

En estos casos, amparado en una trasparencia informativa, y en el entendido de que a mayor información y más conocimiento sobre el hecho, el impacto social es menor; el efecto es de "rebote", pues lo cierto es que a partir de la publicación de las cadenas de virus han aparecido más versiones.

Al parecer muchos programadores que hasta el momento no habían prestado atención a estos programas y que por sí mismos serían incapaces de crear un código nocivo, por no conocer los mecanismos de manejo de hardware a bajo nivel, los han empezado a experimentar con las instrucciones destructivas que han sido divulgadas.

Los efectos son conocidos por todos, con la variación se puede introducir modificaciones en el modo de activación, dando por origen a nuevas versiones de la cepa vírica.

IX - LA RESPONSABILIDAD LEGAL ANTE EL SOFTWARE ROGER.

En este particular hay más preguntas que respuestas. Me permito citar algunos interrogantes y formular otros propios, para que la comunidad intelectual me ayude a despejarlas, pues insisto: el tema merece de respuestas.

Para muchos autores el virus constituye una modalidad de sabotaje y estimo que puede ser entendido como tal, aunque por los efectos puede ser subsumido en el delito de Daño.

Si analizamos a la luz de todo lo que hemos apuntado sobre este asunto vemos que existe una desproporción entre el gran perjuicio que se puede causar y la "gravedad" o modalidad del ataque.

No obstante quedan espacios oscuros y mucho que definir y desentrañar de estas manifestaciones; por ejemplo: la extrema sencillez de los métodos, a la que se añade la posibilidad de que los resultados se adviertan tras un lapso más o menos largo, facilita la impunidad de los autores; a ello se une además, la dificultad de valorar el perjuicio, a lo que se suma, también, la enorme diferencia entre éste y el valor material de los objetos destruidos.

Por eso es tan importante instrumentar los registros de activos: medios e información para poder valorar el monto del daño y en consecuencia exigir responsabilidad.

Supongamos que una entidad ha sufrido pérdida por un virus. ¿Se puede recuperar de ésta pérdida? Probablemente no y más si no tenía previsto un buen plan de seguridad informática.

Es evidente que existe una responsabilidad legal, y por tal motivo es necesario definir, entre otras, las siguientes cuestiones:

a)¿A quién se debe demandar? Los autores de virus no publican su existencia.

b) ¿Es responsable quién opera el equipo informático?

c) ¿Dónde se originó el virus?

d) ¿Se trata de un proyecto de alguna clase que alguien usurpó o fue claramente diseñado para dañar información? ¿O se trata de una técnica de programación empleada y que por descuido se ha propagado y por ende tener consecuencias nocivas para otro entorno informático ajeno al que fue diseñado?.

e) ¿Cómo fue liberado el virus? Fue sólo liberado de un software pirata. Para ser infectado, el usuario tenía que tener el software pirata instalado en su computadora.

f) ¿Le otorgaría un tribunal un recurso a un sujeto agraviado a causa de que utilizó un software "pirata"?

g) ¿Cómo se introdujo el software en el sistema?

h) Suponiendo que el autor del virus pueda ser identificado y la premeditación probada. ¿Es posible cobrar indemnización por daños?

i) ¿Qué ley deberá ser aplicada al autor de virus introducido, cuyos efectos se producen en un país diferente al de su residencia?. ¿La de su país o la ley donde se produjo el daño?

j) ¿Es el autor del virus el único responsable del daño?

k)¿En qué sentido puede la ley condenar a un autor de un virus que nunca tomó ninguna participación activa en su distribución del programa?

l) En el caso de la Bomba Lógica, algunos estudiosos se han preguntado: ¿Cómo se determina el grado de ejecución de un acto ilícito consumado por la introducción de un programa del tipo "Bomba de Tiempo", cuando el sujeto introduce la orden o cuando ésta se ejecuta?

m)¿Cabe en este caso la posibilidad de comisión imprudente, o estamos siempre en caso de dolo?

X. LOS SUJETOS ACTIVOS O DELINCUENCIA INFORMATICA.

Si bien coincido con otros autores que no se puede hablar de un tipo de delincuente único con características propias y definidas, pues al decir de Lafuente, "el panorama es amplio y variado, desde el ratero aficionado, al administrativo furtivo, pasando por el timador casual y el niñato adolescente y desocupado, hasta llegar al profesional astuto, que emplea medios sofisticados para alcanzar un lucrativo fin". Si hay algo común: el sujeto es un conocedor de la técnica, y sólo personas con conocimientos técnicos pueden ser autores del delito.

El término "delincuencia informática" ha sido acuñado como categoría exclusivamente criminológica y se ha empleado para aludir a las conductas disválidas o indebidas que tienen vinculación con las nuevas tecnologías de la información y la comunicación.

También se emplea la expresión para referirse a todos los actos, antijurídicos según la ley penal vigente, socialmente perjudiciales y penalizables en el futuro, realizados con empleo de un equipo automático de procesamiento de datos.

Unido al tema surgen las discusiones al intentar esclarecer a qué forma de criminalidad se hace referencia cuando se habla de "delincuencia informática".

Algunos estudiosos como Luis M. del Pont y Abraham Nadelsticher lo consideran como un delito de cuello blanco. Calificación que tiene partidarios y detractores; mientras otros la inscriben en la delincuencia económica o como un subgrupo de la de guante blanco.[19]

La delincuencia Informática no es subsumible en ninguno de los dos tipos de delincuencia aludida: de cuello blanco o delincuencia económica, sino que debe constituir una categoría criminológica aparte; y sirven de fundamento a esta afirmación investigaciones empíricas llevadas a cabo en Estados Unidos, en las que se constata que el autor sólo en ocasiones pertenece a altas capas de la sociedad. Otras investigaciones realizadas en España ponen en evidencia que los autores pueden ser primarios u ocasionales y que generalmente se trata de empleados de las empresas afectados.

Por su parte, los criminólogos han empezado a expresar las características y particularidades en las cualidades internas de los individuos actores de estas actitudes, a partir del estudio de los que han sido identificados como autores de delitos.

Al caracterizarlos señalan los rasgos de personas solitarias y poco comunicativas, lo que hace poco frecuente la coautoría con estos actos.

Otros rasgos que reconocen estar presentes en los autores es el resentimiento e insatisfacción familiar, personal o profesional y muchas veces hasta desadaptados sociales.

También se destaca el rasgo de que no hay disposición delictiva inicial, esta nace más bien de su contacto con el sistema informático.

Y aunque sin ser un criterio unánime muchos estiman que los autores de delitos informáticos son altamente calificados desde el punto de vista técnico, incluso por encima del promedio, lo que explica la perfección técnica y operacional de los delitos.

■ [19] Dr. Antonio Millé, "El Derecho de Autor y la Infraestructura Global de la Información en las Américas", Seminario sobre Derecho de Autor y Derechos Conexos para países de América Latina.

De modo que no se trata de un autor común, por lo que además de las circunstancias psicológicas y socioeconómicas que deben tomarse en cuenta en su estudio criminológico, deben sumarse una serie de variables particulares.

XI . ENTONCES, ¿CÓMO SE PUEDE ENFRENTAR EL PROBLEMA?.

Está claro que la solución no es una sola, sino varias, incluso algunas no excluyentes entre sí, y son de muy diferentes características y alcance.

Están dados en el ámbito de la administración de las organizaciones, en el plano técnico informático, en el legislativo y muy especialmente en el ámbito de la Deontología.

Tal como adelanté existe una clasificación más o menos coincidente entre los especialistas sobre acciones generadas por el uso de medios informáticos, algunas ya tipificadas como delitos.

Como apunté en otra parte de este trabajo, el aspecto penal es sólo una parte del problema, se trata de dotar a la sociedad de las medidas efectivas para evitar y protegerse del efecto nocivo de tales conductas, incluso a convivir con ellas; y no de adjetivar de "informáticos" acciones delictivas constituidas en nuestros códigos, sino de evaluar las características fundamentales que revisten estas actitudes y de qué modo pueden tener una respuesta real.

Por eso es necesario además conocer similitudes y definiciones, para poder conseguir una protección jurídica eficaz sin caer en el casuísmo, ya que casuísmo provoca lagunas legales e inaplicabilidad.

Dicho de otro modo: desde el punto de vista legislativo somos partidarios de la fórmula de número apertus; aunque como hemos dicho, también hay que crear tipos especiales: producir programas dañinos; distribuir programas dañinos; el intruso. Por otra parte, estimamos conveniente considerar a la Seguridad Informática como un bien atacable y por ende tutelable jurídicamente, en el entendido de que por acción o por omisión se puede atentar contra la disponibilidad, integridad y accesibilidad de la información digitalizada o de los sistemas y redes.

Tal consideración está fundada en el propio carácter multisectorial del impacto social de las nuevas tecnologías, que obliga a la reconceptualización de muchos conceptos tradicionales: "cosa juzgada, correspondencia, documento jurídico, bienes"; y además, en la necesidad de búsqueda de respuestas integrales, en evitación de la hipertrofia en las ramas del Derecho. La acción penal debe concebirse bajo el principio de intervención mínima, pero intervención suficiente.

Para tratar con realismo jurídico y práctico el fenómeno, se requiere un análisis especial, en cuanto a sus formas de manifestación y medios de comisión de la acción; delimitar qué bienes atacan y qué valores ponen en peligro; y determinar en qué medida se pueden prevenir y reprochar suficientemente estas conductas.

Lo que presupone que hay que determinar el valor del bien jurídico tutelado, la intensidad del ataque y el contexto social en que se manifiestan.

Además, debe atenderse al beneficio que reporta el hecho para el comisor, el daño que provoca, tanto al entorno físico del sistema, o al hombre en sentido amplio -individuo o grupo- en su integridad física, honor o patrimonio; y se precisa delimitar en qué supuestos las nuevas técnicas de información son empleadas como instrumento o medio para realizar la acción, o como fin para alcanzar determinado objetivo.

Es imprescindible que previa a la conceptualización penal, exista una regulación administrativa en materia de Informática que sirva de marco jurídico y defina el ámbito de actividad Informática los supuestos y conductas válidas y las acciones reprochables, además de establecer un sistema legal de medidas de seguridad que funcione como eficaz control con finalidad preventiva.

Luego, se debe evaluar concienzudamente hasta qué punto los tipos penales tradicionales pueden ser reformulados y adecuados, en tanto figuras específicas o agravadas, de manera que sean suficientes para subsumir en ellos una conducta determinada.

Si del análisis anterior se llega a la conclusión que lo más conveniente es introducir en la legislación modificaciones que conlleven la adición de nuevas figuras, bien sea en legislaciones especiales o en el propio Código Penal, los legisladores deben tener presente que la Sociedad de la Información está en fase de transición progresiva, por lo que al legislar se debe evitar el casuísmo excesivo

-no se puede pretender recoger todos los supuestos- porque además, dichas tipificaciones pueden quedar en breve en desuso, debido al acelerado ritmo del desarrollo tecnológico y las posibilidades de constante surgimiento de nuevas formas de manifestación, condición que es válida también para la reformulación de tipos tradicionales.

Coincido con el Dr. Emilio del Peso, en el sentido de que si a la par de la formalización jurídica no se presentan estudios doctrinales profundos, no sólo no se resolverán las cuestiones para los que fueron creados tales postulados, sino que se contribuye al surgimiento de nuevos problemas, cuestiones éstas que están además muy vinculadas a la formación del personal que enfrentará este tipo de delitos.

Por otra parte, tal como expusimos con anterioridad estos fenómenos se manifiestan en muy diferente grado en el concierto de las naciones, por lo que asumir modelos normativos puede dar lugar a serios problemas de ineficacia legislativa.

XII. UNA INTERROGANTE DEL "MAÑANA" QUE ES "HOY": ¿ES NECESRIO UNA LEGISLACION PARA EL CIBERESPACIO?.

Al decir del Dr. Vittorio Frosini "(...) Esta es la nueva forma de la información, asimila en nuestro tiempo de civilización tecnológica, después de las formas anteriores de información verbal o gestual, simbólica con dibujos y con escritura, y más tarde con la imprenta y con los medios de transmisión eléctrica, hasta llegar al actual tratamiento (...)"[20], en nuestro caso la información digital.

Unido a este devenir de desarrollo tecnológico, la humanidad ha ido identificando un cambio en los paradigmas en cuanto al soporte de las informaciones, pero ninguno ha sido tan trascendental como los que son fruto de la Revolución Informática, hito en el desarrollo social a partir de la cual se comienza a gestar lo que hoy se conoce indistintamente como "Sociedad de la Información" o "Sociedad del Conocimiento" e incluso algunos la identifican

■[20] Antonio Enrique Pérez-Luño, "Impacto social de la nuevas tecnologías" pág. 15 Editorial Fundesco, 1987.

como la "Era digital", en cualquiera de ellas encontramos que en el vértice de todas estas realizaciones y como piedra angular sobre la cual erigen a la información.

Al aproximarnos al fenómeno nos encontramos que una de las características de la Sociedad de la Información es la convergencia en los medios de transmisión de información: Sistemas Informáticos y Sistemas Telemáticos de múltiples tecnologías y soportes a través de los cuales se almacena, procesa y trasmiten diferentes tipos de información (texto, imagen y sonido) a partir de las cuáles se genera el mensaje.

Por lo tanto, se ha definido al mensaje hoy en día "como una información trasmitida en la cuarta dimensión, aquella de la cognocibilidad pura, similar a la de la memoria y el pensamiento humano, ya que la elaboración de los datos por obra del computador se produce a una velocidad que se mide en millonésimas de segundos, y su transmisión en tiempo real anula las distancias, el espacio y el tiempo (...)".[21]

Así el desarrollo de la infraestructura mundial de información está transformando ya nuestro entorno común, especialmente en lo que se refiere a la generación y transmisión de conocimiento, convirtiéndose a su vez en generador de nuevas fuentes y formas de realización de empleo, por ende trasciende a nuestra vida cotidiana.

En la actualidad la información ha adquirido características de bien social, económico y jurídico autónomo. En cuanto a su forma, se ha separado de su continente tradicional: el paradigma papel, que hoy convive con el soporte digital; sin embargo la información se ha independizado de los mismos sin perder su identidad y su función.

Por otra parte, a la información se le reconoce valor como materia prima fundamental en el cuarto sector industrial. Se identifica además, como un recurso estratégico para el desarrollo; de manera tal, que los cambios estructurales son

■[21] Se estima que las pérdidas de información, oscila anualmente entre los US$ 3 y 5 millones. Esto en una empresa grande; en una empresa pequeña, la pérdida de información puede significar el fin de su existencia.

palpables en términos de indicadores de crecimiento económico, ya se comienza a distinguir entre países inforricos e infopobres.

También se reconoce, que la aplicación de las nuevas tecnologías de la información y la comunicación al entorno social en general es fuente de un sector productivo en tanto genera bienes y servicios y modos diferentes de realización del comercio internacional.

En el ámbito social, surgen oportunidades sin precedentes para la comunicación lo cual favorece extraordinariamente procesos de generación e intercambio de información.

Entre los componentes que integran esta estructura global de la información identificamos al factor humano; a la información que como se dijo es el elemento estratégico y la infraestructura material: el equipamiento (incluidas las telecomunicaciones) y el software, que son los que constituyen los elementos indispensables a través de los cuales se materializa esta realidad.

Todo ello deriva en consideraciones ético-jurídicas sobre el tratamiento digitalizado, el uso y la conservación de la información; tanto a través de los sistemas ya tradicionales de información, como en las más modernas formas de acceso, distribución y comercialización de la información que existen actualmente: las redes digitales de servicios integrados (ISDN) y las redes de comunicación de datos de alta velocidad.

Ante estas realidades entonces nos hemos empezado a preguntar: ¿Es necesario una regulación jurídica para INTERNET?; por el momento, es igual que preguntarnos: ¿es necesario ordenar jurídicamente el ciberespacio?.

Desde hace algún tiempo algunos juristas y otros profesionales, así como usuarios en general, han hablado del tema, algunos niegan toda posibilidad, otros a los cuales me afilio pensamos que se puede y se debe emprender desde el Derecho, pero la viabilidad para el establecimiento de un marco regulatorio del Ciberespacio exige una mixtura entre el Derecho que conocemos y el del porvenir, que es el que ya estamos necesitando hoy.

En otras palabras; y qué mejor que las expresadas por el profesor Michel Vivant, en La Habana, en marzo de 1996.

(. . .) "si las redes no son espacios de no-derecho, hay respuestas en el "arsenal" jurídico (...). Seguro no son perfectas y es la razón por la cual debemos revisar las soluciones conocidas para explorar pautas nuevas (...)"[22].

Entre las cuestiones que quiero resaltar para contribuir a la respuesta es la necesidad de abordar el problema desde la coordinación entre los países que conformamos el concierto de naciones, pues tal como se ha apuntado ya aquí en este foro, uno de los problemas fundamentales es la jurisdicción y la competencia.

No creo que sea difícil lograr la coordinación, máxime cuando este propio espacio de realización del Derecho es paradigmático en cuanto acelera los procesos de comunicación e intercambio de información de modo impresionante: entonces de lo que se trata es de asumir una voluntad de contribuir a la solución de problemas.

Por otra parte, si bien es cierto que se plantean cuestiones cada vez más complicadas para el Derecho Internacional pero a la vez se nos brinda la posibilidad de lograr una mejor realización de su papel en el sentido de desempeñar una función más activa, tanto como orden normativo así como a través de instituciones internacionales, lo cual pone en evidencia que se trata de cuestiones de hecho además del Derecho[23]. Por lo tanto, si bien pienso que las soluciones pueden ser logradas desde el Derecho no creo que exclusivamente desde éste.

En tal sentido, pienso que es necesario fomentar valores éticos, por eso atribuyo mucha importancia a los códigos deontológicos, lo que condiciona que para su efectiva autorregulación es necesario crear o reconocer espacios competentes, no obstante se sabe que no siempre las normas del deber ser son cumplidas, entonces interviene el Derecho para exigir responsabilidad.

■[22] Carlos Ferreyros, "Aspectos metodológicos del delito informático", Notas del curso Nuevas Tecnologías y Derecho, UNED, mayo de 1995. Mérida, España.

■[23] Antonio Enrique Pérez-Luño, "Impacto social de la nuevas tecnologías" pág. 15 Editorial Fundesco, 1987.

También considero que el fomento a asumir conductas éticas, resulta además una garantía de un cumplimiento consciente de las normas jurídicas, que es en definitiva a lo que se aspira en tanto eficacia social del orden legal.

En este sentido, entonces podemos hablar de un espacio habitable civilizadamente en el que se integre armónicamente: el factor humano, la información y la infraestructura material, que curiosamente como fruto de la creación intelectual como lo es el software también tiene que ser protegido.

El proyecto de las autopistas de la información quedaría en una aspiración sin ricos y abundantes contenidos, pero la existencia de los mismos dependen de la seguridad de sus propietarios de ser respetados en sus derechos.

Como se conoce, la vida en el espacio informático ya está generando prácticas, roles y valores diferentes. La relación jerárquica de los bienes también está cambiando. Por lo tanto el mundo jurídico debe reflejar esa realidad produciendo las normas que sean necesarias para impulsar el progreso y mantener un justo equilibrio de intereses en las partes que participan en este proceso. Aunque se debe propiciar la participación de todos en las oportunidades que brindan las nuevas tecnologías de la información y la comunicación.

En el ámbito del Derecho que protege las creaciones de formas, debe tomarse en cuenta el aumento de la importancia de los derechos de acceso, transmisión y usos de la información digitalizada, para reformar consiguientemente su protección legal. El alcance del derecho a la integridad deberá revisarse, para adaptarlo al actual estado del arte.

Debe atribuírsele importancia de primer rango a lo referente a la difusión de normas para la información sobre Propiedad Intelectual, así como de otros segmentos especializados del Derecho que confluyen en estas realidades, lo cual tiene implicaciones en cuanto a las reglas de publicación y divulgación del orden legal.

La información y la protección técnica a los archivos y medios digitales debiera recibir fuerte tutela jurídica, incluso por vía de la sanción penal, según corresponda, aunque en todo caso se debe propender al uso racional y permitir un tratamiento como recurso estratégico.

Coincido con el Dr. Antonio Millé, que en este proceso evolutivo del orden legal, "los cambios jurídicos deben preparase al detalle, la intensidad y la calma que los generosos plazos disponibles autorizan, no emprender tal proceso con urgencia implicaría la seguridad de frustrar parcialmente uno de los mejores esfuerzos de la humanidad tiene en el horizonte cercano."[24]

Es imprescindible atacar el problema desde el frente internacional. La ausencia de un mínimo uniforme de protección a lo largo del mundo crearía "desiertos de información" eludidos por el tráfico de contenidos, se arriesgaría la aparición de "paraísos de piraterías" desde donde se atribuyen contenidos usurpados o adulterados, al tiempo que se facilitaría aun más la circulación de programas dañinos, expresión de justicia por mano propia, en mi criterio un retroceso en el desarrollo de la humanidad; así como la proliferación de una nueva forma de cometer actos de agresión, los cuáles ponen en peligro infinidad de intereses: sociales, políticos, económicos e incluso la propia seguridad nacional y la soberanía.

Por otra parte, en cuanto a los aspectos técnicos (materiales técnicos) hay que continuar incorporándolos al servicio de la humanidad, en el sentido de utilizarlos como recursos materiales para garantizar la tranquilidad y el cumplimiento de ciertos presupuestos de Derecho.

El propio desarrollo tecnológico puede y de hecho lo hace, brindarnos muchas posibilidades de protección real y eficaz, asumiéndose por nuestra parte el rango de previsión posible del riesgo y de vulnerabilidad que ellas mismas son portadoras, por lo que es necesario diseñar e implementar políticas y estrategias de Seguridad Informática, reconocer el justo e imprescindible valor de los procesos de Auditoría Informática, al tiempo de dedicarnos a fomentar una cultura de protección de la información.

Para ello se exige invertir en recursos y esfuerzos en la formación del profesional del Derecho, en el sentido de contar con operadores jurídicos capaces de enfrentar este reto tanto culturalmente como en un ejercicio eficiente de sus

■[24] Se estima que las pérdidas de información, oscila anualmente entre los US$ 3 y 5 millones. Esto en una empresa grande; en una empresa pequeña, la pérdida de información puede significar el fin de su existencia.

funciones y desempeños profesionales. Lo mismo sucede con el profesional de instrucción policial para poder contar con cuerpos especializados en prevenir y perseguir los actos indebidos que pueden ser cometidos.

Sin embargo, pienso también que este esfuerzo sería menguado si se alcanza al ciudadano común, usuario potencial de toda esta la tecnología.

Comencé citando al profesor Vivant, inspirador de estas meditaciones y termino también con una reflexión que me sugiriera: pensemos en un Derecho no para el mundo virtual sino para los hombres que asistimos a él.

Al decir de José Martí. "Para qué sino para poner paz entre los hombres han de ser los adelantos de las ciencias".

XI - BIBLIOGRAFIA

- Amoroso Fernández, Yarina - "La Informática como objeto de Derecho", Revista Cubana de Derecho No. 1, 1990.

- Correa y otros,- "Derecho Informático", Ediciones Despalma, Buenos Aires, 1987.

- B. Parker - "Combatte la criminalité informatique". París, Editorial Oros, 1985.

- del Pont, Luis y Nadelsticher - "Delitos de Cuello Blanco." Cuaderno No.8 del Instituto Nacional de Ciencias Penales (INACIPE), México, 1981.

- Facultad de Derecho - Actas del Congreso sobre Derecho Universidad de Zaragoza Informático, 1990.

- Ferreyra Cortes Conzalo - "Virus en las computadoras", 2a Edición. Macrobit.tm, México 1991.

- Ferreyros, Carlos - "Aspectos metodológicos del delito informático", Ponencia II Congreso Internacional de Derecho e Informática.

- Lima, María de la Luz -"Delitos Electrónicos" Trabajo presentado para ingresar a la Academia Mexicana de Ciencias Penales.

- Pérez-Luño, Antonio E. - "Impacto social de la nuevas tecnologías", Editorial Fundesco, 1987.

- Téllez Valdés, Julio - "Derecho Informático",. Editorial Instituto de Investigaciones Jurídicas, Serie A: Fuentes, b) texto y estudios legislativos, No. 75.

Citas:

- Vittorio Frosini, "Humanismo y Tecnología en la jurisprudencia". Revista internagionalle di filosofía del diritto, 1965.

- Vittorio Frosini, "Hacia un Derecho de la Información", Ponencia presentada en el II Congreso Internacional de Derecho e Informática, Mérida, España, 1996.

- Vittorio Frosini, Obis, Cit.

- Chaumoux, "L' appropation de l' information", Libraries Tecniques, París, 1986.

- Chaumoux, Obis. Cit.

- Yarina Amoroso Fernández, "Informática en Clave Jurídica. Apuntes para un estudio del orden legal cubano. Premio Ensayo en el Concurso de la Sociedad Cubana de Derecho e Informática, UNJC 1997.

- Carlos Lage, Informe económico al V Congreso del Partido Comunista de Cuba, 1997.

- Documento "Programa de Informatización hasta el año 200", elaborado por un grupo de especialistas de los OACE: SIME, CITMA, MICOM y MINJUS, 1997.

Bibliografía:

- Tecnología de la información, su impacto social y su consecuencia legislativa. Algunas consideraciones. UNESCO.

- Conferencia General. 29° reunión, 29 c, Punto ó.4.

- Vittorio Frosini: "Hacia un derecho de la información", Revista Informática y Derecho, No. 12, 13. 14 y 15 - Actas del III Congreso Internacional de Informática y Derecho, Mérida, UNED, España, 1996.

- Pierre Catalá: "Ebanche dúne theorie juridique de l'information, Reeveil Dalloz, 16° cahier, Cronique, 1984.

- Antonio-Enrique Pérez Luño: "Nuevas Tecnologías, Sociedad y Derecho. El impacto sociojurídico de la N. T. de la información. Libro Fundesco, 1987.

- Horacio H. Godoy: El reencuentro de la ética con la ciencia y la tecnología en las puertas del siglo XXI". Ponencia IV Congreso Iberoamericano de Derecho e Informática, Bariloche, Argentina 1994.

- Horacio H. Godoy: "El Espacio Informático". Ponencia IV Congreso Iberoamericano de Derecho e Informática, Bariloche, Argentina 1994.

- Antonio-Enrique Pérez Luño: "Los derechos de la era tecnológica en la obra de Vittorio Frosini". Revista THEORIA - segunda época No. 16-17-18 tomo B. 1992.

- Michel Vivant, "Lamy Droit de 1' Informatique",Ed. Lamy, S.A, 1997.

Las Nuevas Tecnologías en la Seguridad Social

FERNANDO MARTIN COBISA

Licenciado en Derecho

Esta ponencia versa sobre el impacto de las nuevas tecnologías de la información en el campo de la Seguridad Social, dentro del movimiento general dirigido a la incorporación de estos medios técnicos en el seno de la actividad de la Administración e inspirado principalmente por la Ley 30/1992 de 26 de noviembre cuyos dictados se han adaptado en el terreno de la Seguridad Social, gracias a normas como el RD 84/1996 de 26 de enero, la OM de 3 de abril de 1995, la Resolución de 23 de mayo de 1995 desarrolladora de la anterior norma o la Orden de 17 de enero de 1996.

El trabajo analiza la normativa encargada de regular la utilización de estos instrumentos, la validez de los documentos generados por estos, las relaciones entabladas a través de ellos entre las Administraciones y estas con los ciudadanos, y finalmente, las consecuencias derivadas de su uso en cuanto a los derechos de los ciudadanos y de los trabajadores en especial.

INTRODUCCIÓN.

La informática hoy por hoy, se está implantando con gran celeridad en la vida cotidiana de las personas. El gran desarrollo que las nuevas tecnologías están sufriendo en los últimos años es fácilmente constatable en el caso de los ordenadores personales. Estos surgieron a principios de la década de los 80, y su desarrollo e implantación ha ido creciendo paulatinamente hasta su gran eclosión, producida al inicio de la década de los 90.

A consecuencia de este imparable empuje de las nuevas tecnologías en general, en la sociedad se está experimentando una serie de transformaciones a todos los niveles, tanto en el terreno económico (cuyos efectos empiezan a ser patentes a consecuencia de actividades como la informatización de los procesos, el teletrabajo...) como en el social y cultural. Este fenómeno de nuestros días,

afecta también al campo del Derecho por el contacto que éste tiene con la comunidad y por ser sensible en mayor o menor medida a los cambios que se producen en el interior de ésta, debiendo dar respuesta a los problemas derivados de esos cambios sociales.

EVOLUCIÓN HISTÓRICA DE LA INFORMÁTICA EN EL ÁMBITO ADMINISTRATIVO.

El primer hito en la aplicación de la informática en la Administración española data de 1958. El legislador de ese momento ve en las nuevas tecnologías un importante avance. Por ello en la Ley de Procedimiento Administrativo aprobada en ese mismo año se recoge una primera disposición (art.30) encaminada a introducir la mecanización en los trabajos burocráticos, mecanización que en este momento no incluye a los sistemas informáticos y telemáticos, de aparición posterior en el tiempo.

Hay que esperar a finales de los años 60, para observar un nuevo impulso mediante reglamentos como el 2704/67 cuyo objetivo es la creación de un inventario de recursos con el fin de reducir el coste de la mecanización. Un año después (17 de noviembre) se crea el Servicio Interministerial de Mecanización que tiene como fin principal llevar a cabo una actividad de promoción de la mecanización así como coordinar la política de compras.

Durante la década de los 70 se producen un cúmulo de modificaciones de carácter organizacional, hasta llegar a 1983, año en el que aparece el RD 2291/83 (modificado posteriormente en 1987) que supone un nuevo impulso con la creación del Consejo Superior de Informática, como medida para fomentar una política propia en la materia, y que tiene como resultado dos planes nacionales, los cuales no dejan de ser meras declaraciones de intenciones, que no normas. Fruto de toda esta actividad, son los denominados "Informes Reina" reveladores de las necesidades, tanto técnicas como económicas, exigidas para la implantación de estos sistemas en la Administración.

Al hilo de esta situación planteada, surgen comisiones especiales como la CIABSI (Comisión Interministerial de Adquisición de Bienes y Servicios Informáticos) y la Comisión Nacional para la Cooperación entre las Administraciones Públicas.

Todo este esfuerzo innovador desemboca finalmente en la Ley 30/1992[25], en donde el legislador lleva a cabo una serie de medidas dirigidas a una urgente adaptación de los medios electrónicos informáticos y telemáticos (en adelante MEIT) en los procedimientos y actividad administrativa.

Esta ley tiene como objetivo central la regulación de la informática encargada de la tramitación, archivo y desarrollo de los expedientes, a lo que se suma la relación existente a través de estos medios, entre los administrados y la Administración.

LA LEY 30/1992

El ideario de esta ley se encuentra perfectamente recogido de forma general en la exposición de motivos, quien recoge como causa de este avance legislativo, el carácter anquilosado del procedimiento administrativo al convertirse en un obstáculo para dar una respuesta satisfactoria a las necesidades reales de una Administración moderna, que pretende ser eficaz y más cercana a los ciudadanos. Aspecto este confirmado a su vez por el apartado cuarto de la exposición de motivos, de donde se deduce que como resultado de los presupuestos y principios seguidos por la Administración con anterioridad, se ha impedido "*el que la informatización, soporte, tejido nervioso de las relaciones sociales y económicas de nuestra época, haya tenido hasta ahora incidencia substantiva en el procedimiento administrativo, por falta de reconocimiento formal de la validez de los documentos y comunicaciones emitidos por dicha vía. El extraordinario avance experimentado en nuestras Administraciones Públicas en la tecnificación de sus medios operativos, a través de su cada vez mayor parque informático y telemático, se ha limitado al funcionamiento interno, sin correspondencia relevante con la producción jurídica de su actividad relacionada con los ciudadanos. Las técnicas burocráticas formalistas, supuestamente garantistas, han caducado, por más que a algunos les parezcan inamovibles, y la Ley se abre decididamente a la tecnificación y modernización de la actuación administrativa en su vertiente de producción jurídica y a la adaptación permanente al ritmo de las innovaciones tecnológicas*".

No obstante, y a pesar de la actitud y del talante antes descrito, esta materia se encuentra con importantes escollos, pues en palabras del profesor

[25] Ley 30/1992, de 26 de noviembre (BOE de 27 de noviembre), del Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.

Miguel Ángel Davara[26]: *"...los medios de que disponen las administraciones en la actualidad, pueden no ser los adecuados o los requeridos para esta nueva forma de tratamiento de la información y es necesario tener un tiempo de asimilación y preparación para poder adoptar estos nuevos métodos de trabajo".*

Por todo ello, se están dando importantes pasos encaminados a la incorporación de los nuevos medios, si bien es verdad que la transformación hacia la informatización de la Administración depende en gran medida de la voluntad política así como de la dotación presupuestaria que se destine en el seno de la Administración Pública. Esta posición queda corroborada por la propia Ley en su Disp. Adic. 2ª, que dice lo siguiente: "*La incorporación a soporte informático de los registros a que se refiere el art.38 (registro general) de esta ley, será efectiva en la forma y plazos que determinen el Gobierno, los órganos de Gobierno de las Comunidades Autónomas y las entidades que integran la Administración Local, en función del grado de desarrollo de los medios técnicos de que dispongan".*

En lo sucesivo se tendrá oportunidad de valorar cómo se ha aplicado este ideario, y más concretamente, su desarrollo positivo (arts.38, 45 y 46) en el campo de la Seguridad Social.

LOS PROCEDIMIENTOS INFORMÁTICOS Y TELEMÁTICOS EN LA SEGURIDAD SOCIAL.

La primera norma que debe tenerse en cuenta a la hora de establecer el régimen jurídico para la aplicación de medios telemáticos e informáticos en el entorno de la Seguridad Social es el art. 73 de la orden de 8 de abril de 1992, que desarrolla el RD 1517/1991, cuyo articulado ya recoge la posibilidad de transferir los datos de la relación nominal en soporte magnético.

Más explícitos en sus contenidos son el RD 2317/1993 de 29 de diciembre y principalmente, la OM de 17 de enero de 1994, al permitir la transmisión de datos de afiliación, altas y bajas, y variaciones de datos de trabajadores en la Seguridad Social por "medios electrónicos, informáticos y telemáticos" (MEIT).

■[26] "Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común". Actualidad Informática Aranzadi, 1993, n°6.

En concreto, la exposición de motivos de la OM de 17 de enero de 1994[27] determina cual es el espíritu de la norma (completado por su art. 1.1 y 2), al defender que "... *el uso actual de los medios informáticos y telemáticos[....] posibilitan una gestión más ágil y eficiente, tanto por parte de las empresas como por las Administraciones Públicas, facilitando de esta forma al ciudadano el cumplimiento de sus obligaciones, tal como se preveía en el Plan Integral de Modernización de la Gestión de la Seguridad Social*".

Esta misma filosofía también aparece en el propio RDL 1/1994[28] refundidor de la LGSS (arts.101 y 102) al facultar a los empresarios, para utilizar otros medios de documentación establecidos por normas reglamentarias, que no sean el Libro Matrícula.

LA TRANSMISIÓN DE DATOS POR MEDIOS ELECTRÓNICOS, INFORMÁTICOS Y TELEMÁTICOS

El génesis de la utilización de estos sistemas pertenecientes a las nuevas tecnologías de la información en este sector, lo encontramos en el acerbo normativo contemplado en el apartado anterior.

Dentro de la ley 30/1992, el primer artículo referido a la aplicación de estos sistemas es el art. 38.3 al perfilar como necesario que "*los registros generales, así como todos los registros que las Administraciones Públicas establezcan para la recepción de escritos y comunicaciones de los particulares o de órganos administrativos, deberán instalarse en soporte informático*". Este punto a nuestro juicio, incide sobre la premisa, consistente en la agilización y actualización del procedimiento administrativo. Según el profesor Davara, este es "*el instrumento adecuado de control y seguimiento de los expedientes, así como el más eficaz medio de información del estado de los mismos y su cumplimiento o no de la normativa y reglas que regulan su funcionamiento*"[29].

■[27] Orden de 17 de enero de 1994 (BOE de 24 de enero) sobre presentación de las solicitudes de afiliación y altas de los trabajadores en la Seguridad Social y de afiliación, altas y bajas relativas a determinados trabajadores contratados a tiempo parcial.

■[28] Real Decreto Legislativo 1/1994, de 20 de junio (BOE de 29 de junio), por el que se aprueba el Texto Refundido de la Ley General de la Seguridad Social.

■[29] Miguel Ángel Davara. Derecho Informático, Editorial Aranzadi, 1993.

La innovación en la actividad administrativa, se manifiesta de una manera más concreta ya dentro del ámbito de la Seguridad Social, en el art.38.1 RD 84/1996 de 26 de enero[30] con las siguientes palabras: "*La inscripción del empresario, la afiliación, alta y baja del trabajador y la variación de datos de uno y otro podrán formalizarse también suministrando los documentos y datos correspondientes por medios o procedimientos electrónicos, informáticos o telemáticos*",

A continuación el propio art. 38 de la Ley 30/1992 - junto a lo contenido en el art. 7.2 y 3 del RD 263/1996 de 16 de febrero[31]- establece los elementos que deben conformar los sucesivos asientos que se realicen en el registro. Los que conforman el número, epígrafe expresivo de su naturaleza, fecha de entrada, fecha y hora de su presentación, identificación del interesado, órgano administrativo remitente, si procede y persona u órgano administrativo al que se envía, y, en su caso, referencia al contenido del escrito o comunicación que se registra.

El propio apartado 3º del art. 38 (Ley 30/1992) hace aunque sea de una manera indirecta, una primera referencia a la compatibilidad del sistema informático que se emplee, para permitir y en consecuencia, facilitar la transferencia de los datos ("*... el sistema garantizará la integración informática en el registro general de las anotaciones efectuadas en los restantes registros del órgano administrativo*"), esta idea se encuentra mucho más detallada en el apartado siguiente de este artículo, que predica la necesidad de una compatibilidad entre los registros de las diferentes Administraciones Públicas, por medio de sistemas de coordinación e intercomunicación ("*Mediante convenios de colaboración suscritos entre las Administraciones Públicas, se establecerán sistemas de intercomunicación y coordinación de los registros que garanticen su compatibilidad informática y la transmisión telemática de los asientos*"). El RD 84/1996, nuevamente se hace eco de estas normas y en su art. 52.2 regula la constitución de sus registros automatizados y la integración de las anotaciones de estos, en un fichero general establecido por la TGSS.

■[30] Real Decreto 84/1996 de 26 de enero (BOE de 27 de febrero), por el que se aprueba el Reglamento General sobre inscripción de empresas y afiliación, altas, bajas y variaciones de datos de trabajadores en la Seguridad Social.

■[31] RD 263/1996 de 16 de febrero (BOE de 29 de febrero), que regula la utilización de técnicas electrónicas, informáticas y telemáticas por la Administración General del Estado.

El art. 45.4 de la misma ley hace hincapié en la coordinación para permitir una mejor agilidad y seguridad, al señalar que los medios telemáticos necesarios para el ejercicio de las potestades propias de la Administración, deberán ser aprobados previamente por el órgano competente quien será a su vez el indicado para establecer sus características, ya que no sería acertado pedir a la Administración la aceptación de todo tipo de soporte, bien sea de naturaleza informática o telemática para relacionarse los ciudadanos con ella, pues de lo contrario se derivaría un alto coste para esta última.

Sobre este aspecto debemos hacer referencia necesaria al RD 263/1996 de 16 de febrero, desarrollador del art.. 45 de la ley 30/1992. Sus arts. 5 y 9 dedicados a la regulación y aprobación de las aplicaciones, hacen en el primero de los artículos, una diferenciación entre las aplicaciones y programas que efectúen tratamientos de la información en ejercicio de las potestades (inciden en el contenido de las mismas) que la Administración General del Estado tiene atribuidas (Apartado1º), y las aplicaciones y programas cuya utilización tenga un carácter meramente instrumental (Apartado 2º), o lo que es lo mismo, instrumentos que no determinan de forma directa las decisiones administrativas.

De la distinción se deriva el requerimiento o no de autorización para el uso de estos medios. Será necesaria para la primera clasificación y no para la segunda, si bien es cierto que ambas están sometidas a las garantías y mecanismos de seguridad recogidos en los arts. 2 y 4 del citado Real Decreto.

Como contrapartida a lo arriba comentado, la Administración Pública deberá otorgar facilidades y flexibilidad en los MEIT a emplear, para así poder acceder por estas tecnologías el mayor número de sujetos. Un elemento importante de su actividad relativo a este aspecto, será la "publicidad" de los instrumentos informáticos y telemáticos. La constatación de esta política tendrá como resultado una comunicación más fluida y dotada de un mayor nivel de seguridad.

Los arts. 7 y 9, y principalmente el art. 10 del ya citado RD 263/1996 hacen más notoria si cabe, la obligación de la Administración General del Estado de hacer pública la relación de aplicaciones, medios y soportes. La publicidad se va a materializar en la actualización permanente que los Departamentos y entidades deben hacer de la relación de MEIT con los que cuentan, a lo que se suma la elaboración de un directorio por parte del Consejo Superior de Informática con una periodicidad mínima de un año. Incluso el propio art.9 en

sus apartados 4 y 5, manifiesta la exigencia de que los elementos técnicos que configuren las características de aplicaciones... sean hechos públicos por la Administración. El órgano encargado de la aprobación y difusión de los criterios generales de seguridad, normalización y conservación de las aplicaciones a las que refiere el anterior art. 5, es el Consejo Superior de Informática (Disp Adic.1ª RD 293/1996).

Al hilo de lo hasta aquí expuesto, hay que referirnos necesariamente a la O.M. de 3 de abril de 1995 que lleva por título *"sobre el uso de los medios electrónicos, informáticos y telemáticos en relación con la inscripción de empresas, afiliación, altas y bajas de trabajadores, cotización y recaudación en el ámbito de la Seguridad Social" (BOE de 7 de abril).* Se trata de la primera regulación que se encarga en profundidad del tema central de esta exposición, tras los primeros pasos dados por la O.M. de 17 de enero de 1994 en su art. 1 apart. 1 y 2.

La O.M. de 3 de abril de 1995 es el reflejo del trabajo impulsado por la ley 30/1992, participando de sus mismos principios y fines (mejora de la gestión y eficacia, y facilitar la tramitación) aplicados en este caso al ámbito de la Seguridad Social. Sus arts. 1 y 2 recogen de forma genérica, la posibilidad de realizar las tareas de inscripción de empresas, afiliación, altas y bajas, variaciones de datos así como de cotización y recaudación por estos sistemas en los términos establecidos por la TGSS, quien se encargará de establecer los programas, estructuras de datos requeridos para una correcta conexión.

La Resolución de 23 de mayo de 1995 [32]dictada en desarrollo de la anterior Orden Ministerial, otorga en conceptos similares dicha opción, siendo el órgano competente para la adaptación y aplicación en el tiempo de los MEIT, la Dirección General de la Tesorería General de la Seguridad Social (en adelante, DGTGSS), a lo que se suma el hecho de que las empresas recibirán de la TGSS los actos administrativos que ésta realice referentes a estos datos y las notificaciones de los trámites seguidos (Resuelve 1º).

■[32] Resolución de 23 de mayo de 1995 (BOE de 7 de junio), de la Dirección General de la Tesorería General de la Seguridad Social, por la que se desarrolla la Orden de 3 de abril de 1995, sobre uso de medios electrónicos, informáticos y telemáticos en relación con la inscripción de empresas, afiliación, altas y bajas y trabajadores, cotización y recaudación en el ámbito de la Seguridad Social.

A esto cabe añadir una sensible modificación, recogida en la O.M. de 3 de abril de 1995 respecto al procedimiento general, consistente en la no obligación de las empresas a adjuntar para el sellado y validación del boletín de cotización o TC-1, el de la relación nominal o TC-2 cada vez que se tenga que efectuar del ingreso de las cuotas; para lo cual se establece en el boletín de cotización la expresión "*no acompaña TC-2*" (Disp. Adic. 2ª, O.M. 3 de abril de 1995), reseña que por otro lado aparece de manera repetitiva en otras reglamentaciones.

Precisamente en lo tocante a los TC-2, la Resolución de 23 de mayo de 1995, faculta a los considerados autorizados, para la presentación en soporte informático de dicho formulario, en conexión con otras peculiaridades en torno a la utilización de los documentos TC-1 y TC-2. El punto 1° tanto del Anexo II como III del mismo texto regulan la presentación de la relación nominal de los trabajadores, [modelos TC2, TC2/1, TC2/2, TC-2/3, TC2/4, TC2/5, TC2/13 Y TC2/19] el tratamiento y control de recaudación, e incluso la incorporación al Fichero General de Bases de Datos de Cotización.

Los requisitos que deben contener las relaciones nominales para su transmisión quedan encuadrado en el punto 4° del Anexo III, aspecto tratado con detalle más adelante.

La sustitución del Libro de Matrícula por otro instrumento, es otra importante modificación al régimen general. Consiste en la autorización otorgada por la Dirección General de la Inspección de Trabajo, gracias a la cual este documento se sustituye por un sistema de documentación que ofrece las mismas garantías a las empresas solicitantes siempre que se justifique la procedencia de la sustitución.

Todas estas novedosas facilidades deben contemplarse desde la óptica del art. 2 RD 263/1996, manifestación del carácter no discriminatorio a la hora de utilizarse estas técnicas, de manera que su no uso impliquen dificultades o restricciones en el acceso a prestaciones de servicios públicos o procedimientos administrativos. Se deberán facilitar medios substitutivos para las personas que no accedan por estos sistemas, o lo que es lo mismo, seguirán existiendo los formularios TC-1 y TC-2 en soporte papel. El art. 38.1 RD 84/1996 de 26 de enero es claro al respecto.

LAS AUTORIZACIONES: solicitud y sujetos

La utilización de los MEIT en el ámbito de la Seguridad Social, y muy concretamente, en cuanto a las altas, bajas.. no es libre. El uso de estos queda sujeto a la concesión de la correspondiente autorización por parte de la TGSS, facultad que le es reconocida de forma general en el art. 3 del RD 84/1996 y de forma expresa en el Apartado 2 de los Anexos II y III de la Resolución de 23 de mayo de 1995. La autorización será concedida, en los términos del art. 3 de la O.M. de 3 de abril de 1995, a las empresas, agrupaciones de empresas, y demás sujetos obligados en relación con estas actuaciones.

Los sujetos quedan delimitados en primer lugar, por la Resolución de 23 de mayo de 1995 (Resuelve 1º), siendo aplicable a las empresas pertenecientes al Régimen General y a los Regímenes Especiales de los Trabajadores del Mar y de la Minería del Carbón, al igual que a las entidades u organismos con concierto de asistencia sanitaria que deban de efectuar liquidaciones de cuotas. El art. 3 de la OM de 3 de abril de 1995 y la Resolución de 23 de mayo 1995, precisan que en caso de ser solicitada la autorización por parte de profesionales colegiados (cuya actividad gira en torno a esta documentación de altas, bajas..), o por agrupaciones de empresas, éstos deberán de ostentar la representación de los sujetos en cuyo nombre actúen. Respecto a este requisito, también se debe de tener en consideración el Resuelve 5º de la Resolución de 23 de mayo de 1995 en la materia que hace referencia a los códigos de cuenta de cotización (CCC).

La autorización previa (y la aceptación de las condiciones que con ella supone), se formalizará por escrito y podrá solicitarse a la DGTGSS con motivo de la presentación de los datos correspondientes a las relaciones nominales de los trabajadores, exigencia que se hace también extensible a la hora de efectuarse las comunicaciones que tengan por contenido la afiliación, altas, bajas y variaciones de datos.

La solicitud queda sin efecto en el momento en que se produzca el incumplimiento de cualquiera de las condiciones de la autorización. Las condiciones vienen enumeradas en los Anexos IV A y B de la Resolución de 23 de mayo de 1995, correspondientes respectivamente, al documento de autorización del soporte magnético y del intercambio electrónico.

Estos formularios recogen como rasgos comunes en ambos anexos, la aceptación por el solicitante de las condiciones generales de los dos medios, el

sistema de variaciones de datos como sistema de seguridad junto a la protección de los datos de los trabajadores por parte del solicitante, la adjudicación de un número de autorización, la anulación de la autorización si en el plazo de dos meses consecutivos se produce el desuso del soporte magnético(anexo IV-A) o la no presentación en ese plazo de las relaciones nominales (anexo IV-B), el carácter de exento de la presentación del documento TC2 y por último, los efectos frente a terceros.

Por otro lado, se hace oportuna la enunciación de una serie de especialidades contenidas en el formulario destinado al intercambio electrónico de datos debido a su mayor complejidad intrínseca. En esta concreta modalidad, la autorización requiere con carácter preceptivo el envío de los datos de la relación nominal de los trabajadores y se habilita un sistema de resolución de conflictos y discrepancias en materia de CCC entre las partes, con intervención discrecional de la TGSS. Además, y debido a las características técnicas que le son propias, se ha de conceder una clave personal publica (SILCON) y otra privada (Pass-word) al titular de la autorización, obligándose este sujeto a mantener la confidencialidad de las mismas y a llevar a cabo un correcto proceder en los movimientos de los datos (la inactividad en el uso de los procedimientos telemáticos por un período de 6 meses podrá ser causa de anulación de la autorización). El solicitante va a estar obligado a la notificación de los cambios de operador del sistema que se produzcan, así como al mantenimiento de una relación actualizada de las personas autorizadas a comportarse como operadores. Por último, en el Anexo IV-B se hace una precisión dirigida a concretar la condición de representante y otra en lo tocante a los efectos de las notificaciones de la TGSS a agrupaciones de empresas o profesionales colegiados.

LA APLICACIÓN INSTRUMENTAL DE LAS NUEVAS TECNOLOGÍAS.

LLegado este momento, nos situamos ante el factor desencadenante de esta nueva regulación. Se trata de la introducción de las nuevas tecnologías de la información.

El art. 45 Ley 30/1992, tiene como tema central, la incorporación de medios técnicos en la administración, implantación que encontrará sus límites en la Constitución y las Leyes. Las bases asentadas por él (comentado ya con

detenimiento en el apartado correspondiente a la "Transmisión por Medios Electrónicos Informáticos y Telemáticos"), tendentes a la gradual implantación de las nuevas tecnologías en la Administración[33], van a tener gran influencia en la reglamentación llevada a cabo dentro de la Seguridad Social.

La O.M. 3 de abril de 1995, es la encargada de plasmar las líneas directrices. Según los arts.1 y 2 de la citada norma, se atribuye a la TGSS la labor de acometer la incorporación progresiva de estos sistemas en el entorno de la Seguridad Social. Esta manifestación de competencia encuentra su confirmación en su Disp. final 1ª, que reconoce concretamente a la DGTGSS, la capacidad para la aprobación e implantación continuada de estos sistemas mediante resoluciones en función de las posibilidades y los medios técnicos (competencia confirmada nuevamente por el art. 38.2 del RD 84/1996).

Precisamente en atención a una exhaustiva regulación de los sistemas a emplear y en desarrollo de la Disp. final, la DGTGSS dicta la Resolución de 23 de mayo de 1995. Su Resuelve 4º (y en menor medida el Resuelve 6º) introduce la obligación de cumplir las instrucciones técnicas que la Dirección General designe tanto en lo tocante a los soportes magnéticos como al procedimiento de intercambio de datos. Estos "fundamentos técnicos", los encontramos recogidos en los anexos I, II y III .

- ANEXO I

Este anexo consiste en un conglomerado de términos, con el que el legislador pretende facilitar la comprensión de una serie de conceptos caracterizados por su tecnicidad, tales como, análisis morfológico o sintáctico, EDI, impresión de contraste, RVA, segmentos o teleproceso...

- ANEXO II

[33] "Las Administraciones Públicas impulsarán el empleo y aplicación de las técnicas y medios electrónicos, informáticos y telemáticos para el desarrollo de su actividad y el ejercicio de sus competencias..."

El objetivo del presente anexo está dirigido a establecer los requisitos técnicos que debe de reunir el soporte magnético utilizado para las relaciones con la Administración.

Su apartado 3° está destinado a las condiciones generales del soporte magnético. En él se mencionan las instrucciones técnicas facilitadas con la intención de conseguir una correcta configuración del soporte, y caracterizadas por ser de una mayor sencillez en comparación con las requeridas para la transmisión electrónica de datos. La entrega del soporte con los datos se efectuará en el Centro de Control de Recaudación (CENDAR) o bien el la DGTGSS o Administración de la misma, adjuntando una nota de entrega conformada de la siguiente manera:

* Código de Cuenta de Cotización principal
* Nombre o razón social
* El número de autorización
* Período de liquidación
* Fecha y firma de la empresa.
* Fecha y firma de la Administración de la Seguridad Social como constatación del recibimiento.

El soporte será único por clave de autorización y mes de presentación, incluyéndose tantos documentos como sean necesarios, según las cuentas de cotización, los tipos de liquidación y los períodos. Los soportes deberán llevar adheridos una etiqueta que contenga:

* La razón social
* Clave de cotización
* Código de Cuenta de Cotización Principal
* Período de liquidación
* Fecha y hora de presentación
* Persona de contacto
* Teléfono y fax
* Referencia

Cuando la etiqueta adolezca de alguna irregularidad, se procederá a su devolución a la empresa para su subsanación sin que por ello se modifiquen los plazos de presentación. A continuación la TGSS llevará a cabo un segundo control en el que analizará el soporte y en el supuesto de que se encuentre algún

tipo de deficiencia para su tratamiento, se enviará a la empresa correspondiente para que en el plazo de 5 días hábiles lo corrija. Tendrá la consideración de no presentado, si no se realiza su presentación en dicho plazo

- ANEXO III

Este anexo especifica las condiciones generales requeridas para el intercambio electrónico de datos (EDI). La Instrucción Técnica de la TGSS va a desarrollar los siguientes aspectos:

* Las características y formato del mensaje, a fin de ser interpretado por ambos agentes.
* Dotación informática del agente emisor, incluyendo material y programas.
* Características de la RVA, encargada del transporte y el almacenamiento preventivo de los mensajes.
* Características del centro de control de recepción (agente receptor).

La TGSS deberá de mantener enlaces con los centros de mensajería, que operando en todo el Estado, den cobertura a nivel nacional. Mandato recogido en la Ley 31/1987, modificada en su art. 22 por Ley 32/1992 y por RD 804/1993 que lo desarrolla[34].

Para la transmisión se hará uso de las redes de valor añadido o RVA[35], pudiéndose optar entre:

* Las diseñadas para el tráfico de mensajería internacional X-400 [36]

■[34] Ley 31/1987 de 8 de diciembre, de ordenación de las telecomunicaciones (BOE del 19). Ley 32/1992 de 3 de diciembre. Real Decreto 804/1993 de 28 de mayo (BOE de 11 de junio).

■[35] Quedan encuadradas bajo este concepto, tanto las nuevas ofertas de telecomunicación como las aplicaciones que, soportadas por servicios básicos como el telefónico, conforman un sistema más complejo con un valor añadido específico. Son ejemplos, el EDI, correo electrónico, video conferencia....

■[36] La Norma X-400: creada por el Comité Consultivo Internacional Telegráfico y Telefónico (CCITT) -órgano que forma parte de la UIT y este a su vez de la ONU, es un documento en el que

* Las de compensación EDIFACT (norma ISO 9735 elaborada por la CEE/ONU)[37].

* Las propias de la Administración, en particular la red SILNET, red que es propia del Ministerio de la Seguridad Social.

A estas especificaciones se unen un paquete de medidas tendentes a otorgar seguridad jurídica a la transmisión (apart.4 del Anexo III).

La Administración en desarrollo del art. 45.4 de la Ley 30/1992 va a difundir las características y en su caso, a dotar de los programas necesarios para el intercambio de los datos, son los siguientes:

* Programa de confección de nóminas. Este programa será aportado por el solicitante, desarrollado por el mismo o terceros siguiendo las instrucciones técnicas de la TGSS. Su cometido es la creación de un fichero, correspondiente a la relación nominal de trabajadores.

* Programa de transmisión/comunicaciones. Aportado por la RVA, debe cumplir las normas estándar de conexión del servicio RVA elegido. Se encargará de la marcación, enlace, identificación, envío, y recepción de acuse de recibo técnico como recepción de mensajes.

* Programa de validación, impresión y proceso. Facilitado por la TGSS y enlazado directamente con el programa de transmisión, se encarga de realizar la validación de los datos y su secuencia, de acuerdo con la instrucción técnica (la TGSS se reserva el correspondiente control). Su función consiste en la depuración de errores ántes de su transmisión, el análisis de datos, la impresión de datos a fin de una comprobación visual, y la realización de operaciones encaminadas a una mejora de la calidad de los datos transmitidos (supresión de espacios, ceros no significativos, cambio de estructuras y etiqueta interna de envío)

establece un estandar o normalización, cuya función es principalmente, eliminar las barreras técnicas que dificultarían la transmisión de mensajes.

■[37] EDIFACT: (EDI for administration, commerce and transport), es un estándar promovido por la ONU.

* Programa de impresión autorizada[38]. Como su propio concepto advierte, permite la impresión autorizada de la documentación transmitida por medios telemáticos, siguiendo las medidas de seguridad correspondientes. Documento que va a tener gran transcendencia respecto de terceros, de cara a los efectos que frente a éstos el documento ofrezca.

Existen otras medidas exigidas con el propósito de dotar al proceso de seguridad jurídica. Una de ellas es la implantación de mecanismos con la intención de evitar duplicaciones, de manera que el documento que sustituya a otro anterior debe de tener como elementos coincidentes: el CCC, período de liquidación, clase de liquidación y calificador de liquidación.

La RVA facilitará un recibo técnico al emisor para dejar constancia de haberse realizado el envío, adjudicándosele una fecha de presentación asignada por el sistema de mensajería. Los datos de la cabecera del mensaje deben de ser correctos para su aceptación por la RVA, quien remitirá el envío a la TGSS para su análisis. En caso de superar el análisis básico y morfológico[39], se remite un justificante de aceptación al emisor, en el que se contiene la lista de las empresas por las que se han presentado las relaciones nominales con sus respectivas cuotas, el número de trabajadores y la huella electrónica[40] (esta última estará en relación con el contenido, el número de segmentos y la fecha de presentación).

■[38] Impresión autorizada: "La que realizan los ordenadores de la Administración, a través de líneas telefónicas y sistemas informáticos del administrado, certificando que los datos impresos son reflejo de los originales. También se conoce como impresión remota". Véase Resolución de 23 de mayo de 1995. Anexo I

■[39] Análisis básico: "Verificación de que el remitente está autorizado a la presentación de datos por medios electrónicos, informáticos o telemáticos utilizando soporte magnético o EDI".

Análisis morfológico: "Verificación de que la estructura (ordenación de datos) del envío o soporte magnético es válida". Véase Resolución de 23 de mayo de 1995. Anexo I.

■[40] Huella electrónica: "Serie de caracteres calculada por un procedimiento algebraico por el que de cualquier documento, sea cual fuere su soporte informático y extensión, puede calcularse una serie de números y letras que define al documento original y permite determinar cualquier modificación del mismo, sea por incorporación, eliminación, transposición o rectificación de caracteres, palabras, líneas, párrafos o páginas. Recibe su nombre del símil con la huella digital humana". Véase Resolución de 23 de mayo de 1995, Anexo I.

Siguiendo con el contenido del mismo anexo, se recogen en el Apartado 5° de una manera específica, las condiciones que han de reunir las altas, bajas y variaciones de datos.

La transmisión de estos mensajes (con el formato y secuencia requerida) por medio del enlace telemático[41] RVA o SILNET al "buzón receptor", se puede hacer por medio del método de "remesas" o "teleproceso"

Por un lado, la transmisión por remesas (Apartado 5.3 Anexo III) (consistente en una "actuación informática por lotes de proceso o por actuación diferida en el tiempo" y caracterizada por ser contrapuesta al teleproceso), se puede aplicar en el supuesto de la utilización de los programas de confección de nóminas o en su defecto, de captura de datos entregados por la Administración. Este método también se puede utilizar con motivo del uso del programa de transmisión/comunicaciones para así poder transferir los datos de altas, bajas, variaciones de datos y consultas.

Por otro lado la transmisión mediante el teleproceso[42] del Ministerio de Trabajo y Seguridad Social, permite a través de la conexión a la red SILNET por medio del software del solicitante o el facilitado por la TGSS, proceder en tiempo real a comunicar altas, bajas y variaciones de datos, e incluso solicitar información sobre los códigos de información de los CCC autorizados, a lo que se adjunta la posibilidad de realizar la impresión autorizada por este sistema.

Precisamente, Resolución de 17 de enero de 1996, en su Resuelve 5°, recoge la implantación en todo el territorio del sistema RED (en desarrollo de la O.M. de 3 de abril de 1995) que permitirá transferir los datos relativos a la

■ 41 Conexión telemática: "Procedimiento de transmisión de datos informáticos a través de la red telefónica mediante señales eléctricas debidamente tratadas. Un emisor y un receptor ponen en contacto sus sistemas informáticos transfiriendo, intercambiando o accediendo a la información". Véase Resolución de 23 de mayo de 1995, Anexo I.

■ 42 Teleproceso: "Modalidad por la que, mediante los adecuados terminales informáticos, se accede a un ordenador central que dispone de los datos permitiendo consultas, altas, bajas y modificaciones inmediatas de los mismos. Estas acciones son procesos sobre los datos realizados a distancia de donde se deriva el nombre Tele-proceso. Constituye una modalidad de conexión telemática. Se contrapone a remesas.

afiliación, alta, baja, y variaciones así como los referentes a la cotización y recaudación.

Este sistema en palabras de la Resolución, permitirá a los empresarios y a los demás sujetos responsables del pago en general, "*el acceso directo a las bases de datos de la Seguridad Social para consulta de la información que directamente les afecte, respetándose las medidas de confidencialidad y seguridad*". Estos mismos sujetos -sigue diciendo la resolución-, podrán obtener información impresa en papel que surtirá efectos frente terceros (impresión autorizada) a través de la teleimpresión.

Unido a la implantación del sistema RED, estas innovaciones permiten también obtener información gracias a una tarjeta individual de carácter definitivo, sustituta de la antigua cartilla y de otra entregada de forma provisional, dotada de un microprocesador y prevista por primera vez en la Resolución de la SGTGSS de 3 de enero de 1993. En desarrollo de lo expuesto sobre esta herramienta en la Resolución de 17 de enero de 1996 y principalmente en el RD 84/1996 (Disp. Adic. 1ª), se ha dictado la resolución de 30 de abril de 1996[43] con la intención de reunir en un sólo texto toda la regulación existente sobre la materia.

Esta novedosa tarjeta contiene en su soporte informático, datos personales de uso exclusivo por parte del titular además de los que en su caso, sean necesarios para la gestión de las entidades gestoras de la Seguridad Social y el INEM, previa conformidad de la TGSS. También se entenderán incluidos los datos relacionados con la organización y gestión de la asistencia sanitaria.

La expedición de la tarjeta (Resuelve 3°, puntos 3 y 4) se inició el 1 de mayo del presente año en el territorio de las Comunidades Autónomas que hayan firmado el correspondiente convenio (recogido en la Disp. Adic. 1ª.2, RD 84/1996). En los demás casos, la expedición tanto geográfica como en el tiempo, queda a determinar por la TGSS.

■[43] Resolución de 30 de abril de 1996 (BOE de 13 de mayo), de la Secretaría General para la Seguridad Social, por la que se dictan instrucciones sobre la asignación y exigibilidad del número de la Seguridad Social y para la expedición de la tarjeta individual de la Seguridad Social.

Gracias a este instrumento, que permite el acceso a un determinado tipo de información, mediante los Terminales Automáticos de Información y Gestión (TAIG), se posibilita el dispensar a los ciudadanos personarse en las correspondientes oficinas.

Junto a estos elementos dirigidos a facilitar el acceso a la información, esta resolución permite también obtenerla por el cauce de la red Internet a partir del 15 de febrero del presente año (servidor "WWW.seg-social.es"), en cuya página WEB, encontramos los siguientes aspectos:

* Organización de la Seguridad Social .
* Guía de las prestaciones (/guía/index.html).
* Cotización de 1996 (/cotiza96/index.html).
* BEL o Boletín de Estadísticas Laborales (/bel/index.html).
* Directorio (/Director/index.html).
* La Seguridad Social en el Siglo XXI (/sigloXXI/index.html).

Nota: estas direcciones requieren poner a modo de prefijo la dirección www.seg-social.es.

Ej. www.seg-social/guía/index.html

Dentro de este apartado referido a los medios empleados, se debe de estar también al art. 51 del RD 84/1996, en el que se prevé la sustitución del Libro de Matrícula por otro sistema de documentación que ofrezca las mismas garantías, y donde tienen cabida las nuevas tecnologías, debiéndose justificar el por qué del cambio. Sobre este último aspecto existen otras referencias normativas, de la que alguna ya se ha dado cuenta.

LA VALIDEZ DE LOS DOCUMENTOS GENERADOS POR ESTOS SISTEMAS Y SU IMPLICACIÓN RESPECTO A TERCEROS.

El fundamento de la validación de los documentos lo encontramos en el último de los apartados del art. 45 y en la totalidad del art.46 de la Ley 30/1992. Se trata de un aspecto transcendental, pues ante la ausencia de ese requisito de validez, la apuesta por las nuevas tecnologías carece si no del todo, si en gran parte de sentido. Dicho de otra manera, el hecho de existir la posibilidad de que la Administración y el ciudadano se relacionen por estos MEIT, tendría una casi nula utilidad si los documentos nacidos de estas relaciones no se consideran válidos, pues la Administración se encontraría en una situación en la que no se investiría de seguridad jurídica a sus actuaciones.

El art. 45.5 de la Ley 30/1992 constata que los documentos generados a través de estos procedimientos por parte de la Administración ("*o las copias emitidas a partir de los originales almacenados en esos medios*") tendrán la validez y eficacia de documento original (como si de soporte papel se tratara), siempre que se garantice su autenticidad, integridad y conservación, a lo que se suma la necesidad de garantizar la recepción por el interesado en los casos que deba darse así. Este avance es un claro reflejo de la tendencia innovadora encaminada hacia la ruptura con el carácter burocrático y formalista de la actuación administrativa. De esta forma se mitiga la disociación existente entre las prácticas que se venían dando en la actuación administrativa mediante los MEIT y la regulación normativa.

La Ley 30/1992 autoriza que los documentos sean tratados de esta manera siempre que se den las garantías y requisitos establecidos por esta y otras leyes; garantías en las que se deben de incluir las relativas al aseguramiento y respeto de la intimidad y en particular, la denominada "privacidad". Esta última idea no hace sólo referencia a la LORTAD[44], sino a otras leyes de carácter sectorial como en materia estadística o fiscal.

Por su parte el art. 46 contiene en sus cuatro apartados una serie de apreciaciones sobre qué se entiende por validez y eficacia de los documentos,

■[44] Ley Orgánica 5/1992 de 29 de octubre (BOE de 31 de octubre) "de Regulación del Tratamiento Automatizado de Datos de Carácter Personal", en adelante LORTAD.

haciendo una especial reseña a las copias, para las que señala los requisitos que deben reunir, y quién tiene la competencia para expedirlas (concretada por vía reglamentaria).

El RD 263/1996 en sus arts. 6, 7 y 8 profundiza aún más en la validez de los documentos.

Por un lado, el propio art. 6, además de lo expuesto en el art. 45.5 hace una serie de precisiones interesantes, como es el hecho de regular de forma separada la emisión de documentos y de copias. Respecto de los primeros, recoge una importante matización al incluir junto a los requisitos de integridad, conservación... el de identidad del autor, cuyo significado no es equiparable al de autenticidad del art. 45 Ley 30/1992. La razón de la regulación se sustenta en la actuación administrativa, donde la autoría del acto no tiene por qué corresponder a una persona física únicamente, sino también a un órgano (por ejemplo, cualquiera de los integrados en la Seguridad Social). Otra diferencia destacable entre ambas regulaciones, es la ausencia en el Real Decreto de "la recepción por el autorizado de los documentos" la cual teniendo como función la de otorgar más seguridad, hubiera sido más conveniente su inclusión en la norma reglamentaria.

Por otro lado, el art.7 se refiere a la validez de las comunicaciones efectuadas por los MEIT. Para ser válidas tendrán que dejar constancia de su transmisión y recepción, de su contenido, y de la identificación del remitente y destinatario. Las fechas de transmisión y recepción acreditadas en las comunicaciones serán válidas a los efectos de cómputos de plazos y términos, a cuyos efectos se anotarán en los registros generales o auxiliares a los que hace referencia el art. 38 Ley 30/1992.

El art. 8 del RD 263/1996 está destinado a regular el almacenamiento de los documentos, medida cuya finalidad es introducir una mayor seguridad al igual que en el caso anterior.

Los artículos referidos a la validez del documento, están en conexión con la Recomendación del Comité de Ministros del Consejo de Europa [R (81) 20] relativa a "*la armonización de las legislaciones en materia de exigencia de un escrito y de*

admisibilidad de las reproducciones de documentos y de registros informáticos"[45]. En su anexo se establecen cinco artículos, que marcan las pautas a seguir para lograr la validez de este tipo de documentos, pudiendo adquirir (art.3) incluso la condición de prueba en los procedimientos judiciales.

El desarrollo normativo dentro de la Seguridad Social lo encontramos primeramente en la Orden de 3 de abril de 1995. El art. 2.2 enuncia de manera general la validez y eficacia de los datos transmitidos a través de los MEIT, y por ello, estos datos son generadores de derechos y obligaciones para la Administración en sus relaciones con el ciudadano. En esa misma línea también encontramos otra referencia en el art. 38.2 del RD 84/1996 de 26 de enero y más específicamente en el art. 52.3 del mismo texto.

El art. 4 de la Orden de 3 de abril se dedica en su totalidad a la regulación de la validación de estos documentos, como "*...actuaciones tramitadas y aceptadas a través de medios electrónicos...*" con intención de que estos surtan efectos frente a terceros.

Tales documentos en soporte papel, deberán de recoger como elementos de seguridad para su validación y efectos además del documento, la fecha del proceso (Resolución de 23 de mayo), el número secuencial del documento, la huella electrónica y la clave de identificación de la TGSS. Estos requisitos se hacen igualmente extensibles a los casos de impresión por vía telemática.

Fruto de estas garantías, los autorizados para ello podrán utilizar los métodos de impresión autorizada, que les faculta para certificar los documentos recibidos de la TGSS con sello y firma a fin de crear efectos respecto de terceros (en iguales términos esta eficacia frente a terceros se manifiesta en el Apart. 8° Anexo IV-A y apart. 12° anexo IV-B de la Resolución de 23 de mayo de 1985). La categoría impresiones autorizadas válidas, se establecerá por las sucesivas reglamentaciones procedentes de resoluciones de la DGTGSS con el propósito de adecuar paulatinamente los procedimientos.

■[45] Resolución número R (81) 20 del Comité de Ministros, adoptada por el Comité de Ministros el 11 de diciembre de 1981 durante la reunión de los Delegados de los Ministros.

Cuando la impresión sea realizada por medio del programa informático facilitado por la TGSS, los autorizados se van a comprometer a no hacer copias ni cederlo a terceras personas (en referencia al art.9.4 del RD 263/1996 que recoge la coordinación entre sistemas, etc.).

La autorización se hará extensible de una forma especial, además de a la empresa, profesional colegiado, agrupación de empresas, entidad u organismo con concierto de asistencia sanitaria autorizado, a las empresas con más de 2000 trabajadores en alta, siempre que se dé el cumplimiento de una serie de requisitos.

Otro aspecto más específico, es el referido a la consideración de copia autorizada. Lo encontramos en la Disp. Adic. 1ª de esta Orden, que considera copia autorizada de las relaciones nominales, la exposición o puesta a disposición de los trabajadores de sus datos a través de su prestación en la pantalla de un equipo informático.

El anexo V encuadrado en la Resolución de 25 de mayo de 1995 de la DGTGSS (que lleva por título precisamente "*De la impresión autorizada*"), desarrolladora de la Orden de 3 de abril en esta parcela, conforma ya de una manera fáctica, los procedimientos necesarios que deben de ejercitarse para consecución de los resultados buscados. El punto primero recoge las opciones a seguir en la obtención de la impresión, son tres:

La Teleimpresión: cabe realizarse por dos procedimientos:

a) impresión a distancia realizada a través del sistema informático del autorizado, conectado vía telefónica con el correspondiente registro,

b) y/o la impresión de datos por medio de la conexión a los ordenadores de la Seguridad Social.

De lo desprendido en este punto, entendemos que los datos se encuentran almacenados en los correspondientes registros y se utiliza indistintamente como periféricos los ordenadores del autorizado o de la Seguridad Social.

* Autorización administrativa: habilita al autorizado por medio de sus propios ordenadores, terminales, impresoras, toner... a imprimir los datos

correspondientes a la recaudación, altas, bajas, y variaciones en papel común sin tratamiento especial.

* Suministro por la Administración de un conjunto de datos de control (huella electrónica, número de secuencia..) y contraste.

El propio art. 4 Orden de 3 de abril de 1995 reconoce la potestad a la TGSS para realizar impresiones de contraste, con la intención de comparar los datos recibidos ante la solicitud proveniente de la autoridad o de terceros interesados convenientemente motivada.

Por último decir que en materia de altas y bajas también el RD 84/1996 de 26 de enero, regulador del régimen general (exposición de Motivos y art. 30.4) también otorga la validez y eficacia a la solicitud de éstas siempre que se sigan las garantías establecidas por la Administración, en consonancia con lo expresado en la mencionada norma.

EL ACCESO A LA INFORMACIÓN POR PARTE DE LOS CIUDADANOS.

Esta posibilidad se encuentra recogida en la exposición de motivos de la Ley 30/1992. La misma ley plasma este interés del legislador en el art. 37, al reconocer el derecho de los ciudadanos a acceder a registros y documentos de los archivos administrativos, respetando y en otras ocasiones limitando este derecho cuando los documentos.. contengan datos que incidan en la intimidad de las personas.

Este aspecto es examinado con mayor detenimiento en el art. 8 del RD 263/1996, el cual exige para hacer viable el acceso, la existencia de medidas de seguridad que protejan los datos almacenados. Estos requisitos se concretan en la exigibilidad de la identificación de los usuarios y en el control de los accesos[46].

■[46] véase página 25 en materia de protección de los derechos de los ciudadanos.

La Resolución de 17 de enero de 1996[47] según la directríz marcada por las normas anteriores, se centra precisamente en "la atención e información prestada al ciudadano", facilitando a este el acceso a sus datos personales obrantes en los ficheros del sistema de la Seguridad Social, "acceso" que se permitirá de forma progresiva a la todos los regímenes (está previsto en primer lugar para los afiliados incluidos en el Régimen Especial de Trabajadores por Cuenta Propia o Autónomos).

Mediante esta posibilidad se podrá obtener la información anual sobre las cotizaciones (Resuelve 2° punto 1°). Esta información queda complementada con la posibilidad de valorar las expectativas de derecho a las prestaciones económicas, así como conocer sus derechos y obligaciones básicas, normativa aplicable, los datos económicos o simplemente estadísticos que no tengan carácter personal, (resuelve 4° punto 2° y resuelve 7°), elemento este último encuadrado dentro de la protección de los derechos de los ciudadanos.

Las actividades administrativas que podrán acometerse por estos sistemas no se agotan en las anteriores. A través de ellos, se permitirá agilizar (a partir del 1-2-96) los trámites correspondientes a la solicitud de pensiones de viudedad, orfandad y del auxilio por defunción, derivadas de sujetos causantes que tuvieran la condición de pensionistas o de invalidez permanente [en lo sucesivo se extenderá a las demás prestaciones (Resuelve 3°)].

Esta novedosa regulación, evitará en lo sucesivo con el desarrollo e incorporación de las nuevas tecnologías de la información, la presencia física de los interesados en las oficinas de la Seguridad Social, en la medida de lo posible, con motivo de la realización de las actuaciones antes descritas.

El medio principal que va a ser empleado para canalizar todo este flujo de información será el de la red telemática (Sistema RED) que facilitará el acceso a cualquier individuo, empresa o experto (Resuelve quinto, puntos 1 y 2) a partir del 1 de enero de 1996. El instrumento que permitirá llegar a los datos a través de terminales automáticos de información y gestión (TAIG), será la tarjeta individual

■[47] Resolución de 17 de enero de 1996 (BOE de 19 enero), de la Secretaría General de la Seguridad Social, por la que se establecen nuevas medidas de mejora de la gestión de la Seguridad Social y de la atención e información prestada al ciudadano.

dotada de microprocesador. Concretando, se podrán realizar entre otras las siguientes operaciones:

* Obtener información general sobre: Normativa vigente de Seguridad Social, requisitos y trámites para el acceso a sus prestaciones, organismos de la Seguridad Social y dirección de los mismos.

* Obtener información personalizada sobre datos de afiliación e historia laboral con periodos en alta y demás características de cotización.

* Obtener certificados de pensiones y de retenciones a cuenta del IRPF.

* Realizar gestiones como comunicación de cambios de domicilio, modificación de la entidad financiera a través de la que se desea percibir las prestaciones, acreditaciones de vivencia o presencia...

* Solicitar prestaciones económicas gestionadas por el INSS.

A este sistema, se suman las prestaciones otorgadas por la Red Internet (información general) en el servidor "www.seg-social.es".

A partir del 15 de febrero de 1996 se facilitará información al público (sobre el sistema de la Seguridad Social, derechos..) a través de las redes de telecomunicación, información que tendrá como común denominador, la no afectación de datos de carácter personal.

Junto a la obtención de la información y la realización de los procesos arriba descritos, se debe de resaltar lo útiles que estos instrumentos pueden resultar en aspectos como el control parlamentario "a tiempo real" de los estados contables agregados, en los que se reflejan la ejecución de los presupuestos asignados a los Entes gestores y Servicios comunes de la Seguridad Social. Estos efectos beneficiosos también se extienden a las organizaciones sociales representadas en los órganos de participación en el control y vigilancia de la gestión de las entidades gestoras de la Seguridad Social que así lo soliciten.

BREVE REFERENCIA A LA APLICACIÓN DE LA LORTAD DENTRO DE LA SEGURIDAD SOCIAL.

El hecho novedoso de la introducción de los MEIT en el ámbito de la Administración de la Seguridad Social, como consecuencia práctica del proceso de adaptación derivado del Plan Integral de Modernización de la Gestión de la Seguridad Social, se constituye en un conjunto de actuaciones dirigidas a mejorar la calidad de los servicios de la Seguridad Social. Cambios que también permiten favorecer las relaciones con el ciudadano.

Para conseguir los objetivos arriba expuestos, se hace uso de una reordenación normativa, que partiendo de la Ley 30/1992 (art. 45 y RD 263/96 de 16 de febrero), y de la Ley Orgánica 5/1992 junto a otras disposiciones sectoriales (esta última referida a los derechos fundamentales de los ciudadanos), adapten los procedimientos de gestión de la Seguridad Social a los nuevos tiempos con sus correspondientes garantías.

La incorporación de nuevas tecnologías supone ventajas procedimentales y de gestión en el ámbito de la Seguridad Social, pero también riesgos respecto de los derechos de los trabajadores y de los individuos en general. Estos riesgos son los que se buscan mitigar con la normativa de reciente aparición; en concreto, en lo referente a la Inscripción, alta, baja, variaciones de datos de los trabajadores y accesos al sistema informático de la Seguridad Social.

Como primer punto a estudiar, merece la pena destacar cómo la LORTAD ha incidido en el RD 84/1996, insertado éste en el Plan de Acción de modernización de la Gestión de la Seguridad Social.

De manera indirecta su art. 52 hace alusión a la obligación por parte de la Administración del mantenimiento al día de sus registros, además de una genérica referencia al "cumplimiento de las garantías y requisitos" (donde queda incluida la LORTAD) en cuanto a las integridad, utilización, conservación... de asientos, datos y documentos etc.

Esta incidencia de la LORTAD en el RD 84/1996, aparece más claramente reflejada en el art. 53 del citado Real Decreto, al requerir que los datos que obren en los registros, serán utilizados por las Entidades gestoras y Servicios comunes de la Seguridad Social para los fines que les son propios, no pudiendo

ser cedidos estos a otras administraciones para el ejercicio de competencias diferentes o para competencias que versen sobre materias distintas, salvo que la cesión hubiese sido prevista en la disposición que creó el fichero o por una posterior que regule su utilización (ya sea de rango igual o superior), o bien se traten de datos de carácter personal que una Administración Pública obtenga o elabore con destino a otra [art.11.2 e) y 19 LORTAD]. Un claro ejemplo de cesión válida a otra Administración, es la realizada a la tributaria en virtud del art. 36.6 del RDL 1/1994, de 20 de junio.

En el supuesto de los ficheros de titularidad pública enlazando con lo ya expuesto, se deben de tener en cuenta las excepciones que realiza el art. 22 LORTAD, a los derechos vistos anteriormente.

Los responsables de los ficheros autorizados según el art. 53.3, quedarán sujetos al régimen sancionador del Título VII LORTAD y los números, informes, antecedentes y demás datos concernientes a personas físicas identificadas o identificables, quedarán también sujetos a la LORTAD sin perjuicio de que la obtención, cesión, rectificación o cancelación de los mismos relativos al ejercicio de las funciones recaudatorias encomendadas a la TGSS, se rija por el art. 36 del RDL 1/1994, texto refundidor de la LGSS.

En consonancia con lo anterior, la Orden de 17 de enero de 1996[48] (art. 6.4) reguladora del acceso al sistema informático de la Seguridad Social, enumera una serie de actuaciones (acceso a la información por el usuario no autorizado, realización de transacciones informáticas que no estén relacionadas con un objeto concreto de gestión...) que nuevamente darán lugar a las responsabilidades contenidas en el Título VII de la LORTAD.

Sobre el régimen sancionador de este Título, se tiene que hacer una importante apreciación conducente a la diferenciación entre ficheros privados y públicos, ya que mientras que para las infracciones (art. 43 LORTAD) cometidas en ficheros privados, el régimen sancionador será el contenido en la propia LORTAD, para el caso de las sanciones cometidas en ficheros de titularidad

■[48] Orden de 17 de enero de 1996 (BOE de 25 de enero) sobre el control de accesos al sistema informático de la Seguridad Social.

publica, el régimen será el disciplinario de las Administraciones Públicas (art.45 LORTAD).

En el segundo apartado del mismo art. 53 se reconoce el "derecho de información" de los empresarios, trabajadores y personas que acrediten tener un interés personal y directo en la información (consistente bien en una visualización, bien en una comunicación) solicitada, sobre los datos a ellos referentes que obren en poder de la Seguridad Social, así como el "derecho de acceso a los registros y archivos de aquella, siguiendo el tenor de los arts. 37 Ley 30/1992, art. 8 RD 263/96, y arts. 13 -"*Derecho de información*"- y 14 -"*Derecho de acceso*"- de la LORTAD.

Precisamente en torno al acceso, la Orden de 17 de enero de 1996, regula las actuaciones que se puedan realizar a través del sistema informático de la Seguridad Social, las cuales deberán salvaguardar la integridad, disponibilidad y confidencialidad de los datos contenidos en el sistema (art.2), teniendo en cuenta el art. 10 de la LORTAD por el que se manifiesta el deber de secreto de los responsables de los ficheros automatizados.

Para acceder a la información contenida en dicho sistema, cada usuario recibirá un perfil de las posibles acciones que puede realizar (autorización personal) de acuerdo con las funciones que realice, y será éste identificado y autentificado debiendo motivar su acceso. Este derecho de acceso se ejercerá en intervalos superiores a doce meses, a no ser que el afectado por tener y acreditar un interés legítimo, pueda efectuarlo antes.

La Gerencia de Informática de la Seguridad Social, responsable máxima en la administración del sistema de información de la Seguridad Social, otorgará la autorización inicial de acceso para cada aplicación a los Administradores de categoría máxima de la Entidad gestora o Servicio común responsable de la misma; a partir de aquí el resto de las autorizaciones se irán realizando conforme indica el art. 5 apart. 3 y 4 de la Orden de 17 de enero de 1996.

De conformidad con el artículo 3.d) de la Ley Orgánica 5/1992, los Directores Generales de las Entidades gestoras y Servicios comunes de la Seguridad Social serán los responsables de los ficheros automatizados de datos, y a ellos se les va a atribuir la titularidad de los mismos y la responsabilidad en su utilización dentro de la gestión de sus funciones (art.5).

A todos estos mecanismos de protección se deben de adjuntar los deberes asumidos por los usuarios. Responderán de todos cuantos accesos realicen y deberán mantener en secreto y bajo su custodia la contraseña de los que son titulares a lo que hay que añadir la existencia de una auditoría del sistema (art.7), a través de la cual, los Administradores de categoría máxima vigilarán el uso de las autorizaciones de acceso, y exigirán las correspondientes responsabilidades por su mala utilización.

El repertorio de derechos se complementa con el de rectificación y cancelación establecido en el art.15 LORTAD.

Por medio de todas las medidas expuestas (autorizaciones previas, sanciones..), se pretende salvaguardar con garantías la confidencialidad e integridad de los datos contenidos en el sistema informático de la Seguridad Social, y por consiguiente los datos personales de los ciudadanos.

Informática y Derecho en España

MANUEL ALVAREZ RICO

Universidad Pontificia de Salamanca en Madrid

LA INFORMATICA EN LA ACTUALIDAD

Es difícil decir algo sobre la importancia de la Informática en la actualidad que no suene a tópico. Baste recordar que la Informática está transformando nuestros sueños, nuestro trabajo, la sociedad misma, las relaciones de poder a través de lo que se ha llamado "la revolución silenciosa" o la "tercera ola" en frase de Toffler[1] radicalmente distinta de la primera, la agraria, y de la segunda, la industrial.

Desde otra perspectiva, se ha afirmado que la Informática, juntamente con la Genética es la "punta de lanza" del progreso científico moderno.

Pero, ¿supone -se pregunta el Profesor Barroso[2]- el advenimiento de una nueva edad del saber, de la cultura compartida y de la convivencia democrática más justa y participativa o sólamente un mundo repleto de riesgos sobre la vida de los individuos y las sociedades?.

Para que la respuesta a estas inquietantes cuestiones pueda ser positiva conviene recordar la sugerente observación de HABERMAS[3]: "al desafío de la

■[1] TOFFLER. La tercera ola. Plaza y Janés. Barcelona 1980.

■[2] BARROSO. Prólogo a la edición española de Deborah G. Johnson. Etica Informática. Madrid, 1996. Fac. de Ciencias de la Información de la Universidad Complutense de Madrid, pag. 18.

■[3] Cita tomada del Manual de Informática y Derecho. Antonio Perez Luño. Arie. Barcelona, 1996. pag. 81.

técnica no puede responderse sólo con la técnica". Son necesarios otros instrumentos entre los cuales ocupa un lugar de privilegio la Etica y el Derecho, añadimos nosotros.

ETICA Y DERECHO INFORMATICO

La Etica no es sólo el principio y el fin del Derecho. Es cierto que el análisis moral precede a la promulgación de una Ley y las propuestas para su modificación se basan en un juicio moral compartido sobre su bondad, pero la Ley no representa la última palabra, dice Johnson [4]. El debate sobre el aborto no cesó después de aprobarse la Ley del Aborto en España, pues los individuos siguen teniendo posiciones contradictorias sobre el particular. Y es que únicamente desde una plataforma ética cabe, en ultima instancia, la crítica, el cambio y la necesaria transformación del Derecho[5] ...

Pero estas relaciones entre Etica y Derecho no deben hacernos olvidar que lo característico del Derecho es el cumplimiento externo del mandato, mientras que en la Etica lo decisivo es el mayor grado de adhesión interior exigida. Ello no quita que también en el Derecho lo deseable sea lograr la adhesión interior a la norma disminuyendo así las posibilidades de incumplimiento.

Trasladado esto al campo de la Informática significa que la Etica no es necesaria sólo porque faltan leyes (vacio legal) o por las deficiencias de las que ya existen. El problema es más complejo. En algunos casos faltan leyes pero en otros son precisos códigos deontológicos o instituciones o varias soluciones al tiempo.

En este orden de ideas se tomó conciencia enseguida de la necesidad de proteger la intimidad de la vida privada de las personas, para lo cual la solución ética resultaba insuficiente, lo que no significa, en modo alguno que los principios deontológicos hayan perdido su valor fundamental.

■[4] Ver obra citada en la Nota 2 anterior, pág. 23.

■[5] DIAZ E. Sociología y Filosofía del Derecho. Taurus. Madrid 1989, pág. 17.

Buena prueba de ello es que las Leyes de Protección de Datos, en muchos países, entre ellos en España, Ley 5/1992, de 29 de octubre, sobre Regulación del Tratamiento Automatizado de Datos de Carácter Personal (LORTAD), en su artículo 31 recoge los códigos tipo a los que da el carácter de códigos deontológicos pero advirtiendo que no tienen carácter jurídico (coactivo).

Por tanto el incumplimiento de los mismos no lleva aparejada sanción alguna, como no sea la eventual separación o expulsión del grupo de quienes no se ajusten a ellos[6]. Por lo que esos códigos deontológicos no pueden ser alternativas a las disposiciones legales elaboradas por los órganos legislativos correpondientes, sino complementarios de los mismos.

Son necesarias otras soluciones como las técnicas de las que no vamos a ocuparnos y las jurídicas que es el objeto de nuestro análisis.

Pero eso no basta. El cumplimiento del Derecho no puede confiarse, en última instancia, a la conciencia, al estimulo ético del deber, el Derecho exige absolutamente el cumplimiento, puede exigirlo incluso por la fuerza (la coacción). Precisamente por esa cuasi omnipotencia del Derecho, demanda que esa coacción venga utilizada para fines justos y legítimos, que el individuo no se encuentre perdido ante esa fuerza, sino que posea garantías de defensa, seguridad y libertad; que la sociedad y los hombres que la conforman controlen esa terrible fuerza participando en la creación del ordenamiento jurídico y en la correcta aplicación de las normas. Dignificar, en definitiva, el necesario uso de la fuerza, haciéndola legítima, justa, poniendo el Derecho al servicio de fines humanos como la libertad, la paz , la justicia y el bienestar

Históricamente, la Informática empezó su andadura al margen del Derecho. En un primer momento, las relaciones entre los profesionales de la Informática eran las propias de un club. Esta solución tuvo su razón de ser en el contexto de los ordenadores de la segunda generación (1965) cuando los profesionales de la Informática eran pocos y depositarios de un saber hermético y casi exotérico. En esta situación la necesidad de protección jurídica no era acuciante .

■[6] VELAZQUEZ BAUTISTA R.- Protección Jurídica de Datos Personales Automatizados. Colex. Madrid, 1993, pag. 191.

Posteriormente, la difusión de la Informática cambió el panorama, Desapareció el espiritu de club y empezó a sentirse la necesidad de encauzar los eventuales riesgos que el mal uso de la Informática podía producir.

INFORMATICA Y DERECHO

La Informática plantea nuevos y complejos problemas jurídicos derivados del propio carácter de las nuevas técnicas para las que no son válidas las categorías conceptuales heredadas del pasado. Pero el jurista se siente más proclive a operar con materiales conocidos que a avanzar en la prospectiva.

Las relaciones entre Derecho e Informática son variadas, como puede fácilmente comprenderse y podrían diversificarse en ramas distintas, no obstante, entre nosotros a diferencia de lo que ocurre en otros países, se suelen distinguir dos grandes bloques: La Informática Jurídica y el Derecho Informático.

La primera se refiere a la utilización de las técnicas informáticas por los profesionales del Derecho (Abogados, Procuradores, Jueces, Secretarios etc.) y constituye una ayuda imprescindible para estos profesionales.

En cambio, el Derecho Informático alude a una disciplina emergente que aspira a formar parte de las ciencias jurídicas y se fundamenta en un conjunto de principios y reglas jurídicas que contemplan actividades llevadas a cabo por medio de sistemas informáticos.

En todo caso, conviene no olvidar que ambas disciplinas mantienen evidentes interrelaciones. Así la aplicación de la Informática al proceso plantea el problema del secreto de los datos lo que justifica que en algunos países -sobre todo anglosajones- se traten conjuntamente ambas disciplinas.

Aquí nos vamos a referir por razones de tiempo al Derecho Informático como Derecho emergente con unas características que le otorga su propia individualidad y que pugna por encontrar su puesto entre las disciplinas jurídicas ya "establecidas".

ASPECTOS NOVEDOSOS DEL DERECHO INFORMATICO

El Derecho Informático se caracteriza por ser un Derecho transversal o encrucijada que incide en casi todas las disciplinas jurídicas tradicionales: en el

Derecho Constitucional y Administrativo (libertad informática o defensa contra las eventuales agresiones perpetradas por la tecnología de la informática); Civil y Mercantil, en cuestiones tales como contratos informáticos que pueden afectar tanto al hardware como al software dando lugar una abundante tipología como los contratos de compraventa, alquiler, leasing, copropiedad, contratos EDI (CONTRATOS PERFECCIONADOS POR MEDIOS ELECTRONICOS) compensación electrónica, contratos acreditados y transmitidos por medios electrónicos, contratos negociados a distancia etc.; propiedad intelectual (protección jurídica del software) y penal (delito informático).

Todo ello suscita el problema de si se trata de un sector de normas dispersas y heterogéneas o un conjunto normativo homogéneo con un objeto delimitado y una metodología propia en cuyo caso estaríamos ante el nacimiento de una disciplina autónoma.

La contestación a esta pregunta -que por lo demás, es un problema común a muchas ciencias sociales- tiene mucho de convencional y pragmática, viene dada por los siguientes parámetros:

Acuerdo sobre el objeto, metodología propia, utilización de medios propios y diferenciados de enseñanza, difusión y diálogo científico, legislación, jurisprudencia y doctrina específica y denominación reinvindicada en común.

A) .- Delimitacion del objeto.

El objeto inmediato del Derecho Informático es la Informática pero su objeto mediato es la propia información y de ahí se derivan una serie de características del Derecho Informático pues la información es un bien inmaterial producto autónomo y anterior a todo procesamiento. La información puede ser objeto de transporte, depósito, alquiler, venta, transferencia etc. Así nacen, se modifican y extinguen los derechos sobre la información que pueden reconducirse a los mecanismos del Derecho.

B) .- La originalidad de la metodología del Derecho Informático significa que la comprensión correcta de los problemas informáticos exige el conocimiento y uso de unas categorías conceptuales y metodológicas aptas para alcanzar su contenido y significación. Un ejemplo. No puede abordarse el derecho de propiedad de la información desde la vieja óptica del derecho de propiedad, cuyas características son la exclusividad pues no se adecúa a la naturaleza de la

información, lo mismo que ocurre con el medio ambiente o el patrimonio artístico que concitan intereses colectivos y difusos cuya utilización no debe ser exclusiva y excluyente (la utilización de uno no impide la utilización por los demás). En esta línea la labor doctrinal es fundamental para que la producción legislativa alcance el máximo rigor y no sea dispersa y heterogénea.

Otra causa relacionada con la anterior consiste en que la normativa informática para adaptarse a la rapidez de los cambios que se operan y no quedar desbordada necesita utilizar conceptos amplios o cláusulas generales, para evitar reformas constantes y, contra lo que es habitual en Derecho, aceptar definiciones que eviten las discusiones y dudas permanentes a los órganos encargados de aplicar las normas.

Otro aspecto a tener en cuenta es que la información atraviesa las fronteras y en consecuencia el Derecho Informático debe ser "un Derecho común a todos los países".

C) Docencia y doctrina científica.

El nombre Derecho Informático es reciente en España. Tanto es así que no hace muchos años cuando yo empecé a impartir clases en la Facultad la asignatura se llamaba Legislación Informática y recuerdo que los libros publicados en España sobre la materia cabían en una cartera.

A partir de entonces y, sobre todo de la publicacion de la LORTAD (año 1992), asistimos a un auténtico boom de publicaciones en este área. En el año 1993 el Profesor Davara publica un libro que lleva el nombre de Derecho Informatico[7] y la doctrina en general admite la presencia de una disciplina autónoma con esta denominación.

Las publicaciones son numerosas como puede verse con la consulta de la base de datos de cualquier biblioteca. Se celebran Congresos Internacionales como los que han tenido lugar en Mérida en 1992 y 1995. Las mesas redondas, simposium y encuentros son numerosos, como el organizado anualmente por el Profesor DAVARA en la Universidad Pontificia de Comillas (ICADE).

■[7] DAVARA RODRIGUEZ, M. A.- Derecho Informático. Aranzadi. Madrid. 1993.

Recientemente tuvo lugar una reunión sobre Derecho Informático en el Colegio de Abogados de Madrid con motivo de la celebración del Cuarto Centenario de su fundación. La conocida Editorial Aranzadi publica una revista de divulgación que se titula "Actualidad Informática" y el Centro Regional de Extremadura de la Universidad Nacional de Educación a Distancia (UNED) en Mérida edita una revista con el titulo de "Informática y Derecho", debida al impulso del Profesor Carrascosa, habiendo aparecido ya el número 16; son frecuentes los artículos sobre Derecho Informático tanto en las revistas especializadas en Derecho como en las de Informática y en los diarios de información general.

En el ámbito de la docencia, aunque los Reales Decretos de Directrices Generales sobre los nuevos Planes de Estudio promulgados en 1990 no contemplan esta asignatura como troncal, es decir, obligatoria en todo el país es lo cierto que existen diversas Universidades, como la Universidad Pontificia de Salamanca, la Universidad "Jaume I" de Castellón, por ejemplo, donde el Derecho Informático luce como asignatura al amparo de la posibilidad que los citados Reales Decretos ofrecen de implantar asignaturas propias de cada Universidad en sus Planes de Estudios; la UNED, en su Centro Regional de Extremadura dedica especial atención al Derecho Informático en el ámbito de los Cursos de Verano; lo que significa un gran avance sin desconocer lo mucho que queda por hacer y las dificultades de todo tipo que existen, la falta de Cátedras de Derecho Informático y de tesis doctorales, los gigantismos de algunas universidades y la endémica falta de medios materiales son otros tantos inconvenientes para la incorporacion de esta especialidad a la Universidad. Pese a todo puede afirmarse que las perspectivas a medio plazo son moderadamente optimistas dado el ambiente creado y el fuerte impulso de las nuevas ideas y realidades.

D) .- Legislación.

Finalmente quiero referirme a la legislación española sobre Informática que es una cuestión fundamental a la hora de medir el desarrollo de cualquier rama del Derecho y que sólo por razones expositivas ha quedado relegada al final de mi intervención.

Lo primero que hay que decir es que la legislación sobre Informática en España es copiosa, producto de la pluralidad de ordenamientos jurídicos que inciden sobre la materia: el estatal, el autonómico y el de la Unión Europea por nuestra incorporación a la misma. Basta ver el volumen del libro publicado por el

Profesor Heredero y yo mismo el año 1994[8] y que ya ha quedado superado por la aparición de nuevas normas, de manera que estamos preparando una nueva edición. Su comentario aún refiriéndonos sólo a las más importantes, supondría someterles a un suplicio tan duro como inútil pues en otras intervenciones se tocará el aspecto legal en profundidad por lo que nos vamos a limitar a ofrecer una visión panorámica sobre las leyes más importantes o mejor sobre los sectores en los que se han dictado leyes que afectan a la Informática, para ello puede servirnos la estructura de la propia colección legislativa.

La Constitución española de 1978 actualmente vigente figura entre las Constituciones que han elevado a rango normativo fundamental la protección de datos. Así el artículo 18.4 dice: "La Ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos".

Sin embargo hasta 1992 no hemos dispuesto de una Ley Orgánica de Protección de Datos (la LORTAD). Lo cual no significa carencia absoluta de legislación sobre el tema pues, además de las disposiciones sectoriales, España se adhirió al Convenio 108 del Consejo de Europa de 28 de enero de 1981 el 27 de enero de 1984, (BOE de 15 de noviembre de 1985) que contiene lo que podíamos llamar derecho común o "núcleo irreductible" (principios básicos) de la protección de datos y las reglas especiales referentes a los flujos internacionales de datos.

En este orden es preciso hacer mención al Acuerdo de Schengen de 14 de junio de 1985, al que se ha adherido España el 16 de junio de 1990, sobre supresión gradual del control de fronteras comunes entre los países signatarios. Para ello regula el flujo de informaciones personales en función de la cooperación policial (SIS). Al igual que el convenio 108 del Consejo de Europa, exige para la tansmisión de datos que en el país receptor sus normas internas sobre protección de datos satisfagan los principios del propio Covenio.

En este campo tiene gran interés el sistema EDI sobre intercambios eletrónicos y sobre todo Internet que representa uno de los problemas pendientes ya que dada su novedad no existe norma que lo discipline. Una de las

[8] HEREDERO-ALVAREZ RICO .- Legislación informática. Tecnos. Madrid. 1993.

posibilidades podría tener su concreción a través de códigos deontológicos o soft law pues existe un sector doctrinal que se opone a su regulación legal por considerar que atentaría contra el derecho a la libertad de expresión. En todo caso la adopción de una postura sobre el particular es previa a su regulación legal; desde otro punto de vista, ha supuesto además de sus importantísimas ventajas un incremento importante de las formas de criminalidad al potenciar la difusión de los sabotajes y acceso indebido que entran en el campo del delito penal al que nos referimos más adelante. La LORTAD publicada en 1992 es la que fija con carácter general los principios a través de los cuales se pretende dar cumplimiento al mandato constitucional.

Como novedades de la nueva Ley pueden señalarse el establecimiento de unos principios para armonizar los valores fundamentales de respeto a la vida privada y la libre circulación de la Informática. Un aspecto importante a destacar es el papel que se le asigna al consentimiento del afectado en la recogida española en materia de Informática es el sistema de protección de las creaciones intelectuales en materia de Informática. Tanto la Ley 22/1987, de 11 de noviembre de Propiedad Intelectual, como el Texto Refundido aprobado por Real Decreto Legislativo 1/1996, de 12 de abril, que aclara y armoniza las disposiciones legales en la materia (entre ellas la Ley 27/1995, de 11 de octubre de incorporación al Derecho español de la Directiva 93/98 de la Unión Europea) equipara los programas de ordenador a las obras literarias constituyéndolos como objeto de propiedad intelectual frente a los otros sistemas utilizables, el de patentes y el sistema de protección especial.

Por lo que atañe a los derechos que dimanan de la propiedad intelectual distingue dos tipos: 1) Derechos morales (irrenunciables, inalienables) y 2) Derechos patrimoniales que llama de explotación. De todas maneras es preciso reconocer que la eficacia de estos mecanismos no es la suficiente debido tanto a la falta de técnicas legislativas adecuadas como a la lentitud de la Administracion de Justicia.

Los problemas sociológicos y el precio de los programas son otros elementos a tener en cuenta para valorar la eficacia del sistema legal español.

Otro bloque muy importante de la legislacion española en materia informática está constituido por los contratos informáticos donde se trata de evitar el desequilibrio entre las partes que intervienen a través de legislación de carácter sectorial como la Ley de Defensa del Consumidor de 1984 (Ley 26/84), legislación de defensa de la competencia o sobre el comercio minoritario y crédito al consumo.

Por lo que se refiere a los contratos públicos, ha de tenerse en cuenta el peso específico de la Administración como agente económico y la regulación especial de los contratos públicos que pueden significar algún tipo de contrapeso al desequilibrio contratual en este ámbito. El marco vigente actualmente en esta materia esta constituído por la Ley 13/1995, de 18 de mayo. A tenor de esta ley se incluyen dentro de los contratos de suministro los que tienen por objeto la adquisición y el arrendamiento de sistemas informáticos, sus dispositivos y programas así como su cesión (art. 173).

Como principio general establece la adquisición centralizada de equipos y sistemas informáticos así como elementos auxiliares (art. 184) por la Dirección General del Patrimonio, Ministro de Defensa, Organos Centrales de la Seguridad Social, etc. Con ello se pretenden garantizar unas condiciones generales comunes para la contratación así como una política informática que permita la plena compatibilidad de los sistemas y su coordinación. Un procedimiento especial para los contratos informáticos pretende asegurar las condiciones más ventajosas y los equipos más eficaces para la Administración.

La Informática es, tal vez, la última esperanza para la tan manida como inexistente reforma administrativa. De intento de incorporación de la Informática a la Administración cabe calificar a la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, la cual ya destaca en su Exposición de Motivos que la "informática es el soporte y tejido nervioso de las relaciones sociales y económicas".

Un aspecto innovador es la importancia que la Ley da a la Informática en la organización de los Registros y Archivos administrativos (art.36). La posibilidad de relacionarse con los ciudadanos a través de métodos electrónicos e informáticos y el reconocimiento de la validez de los documentos informáticos dentro del proceso (art. 45) siempre que quede garantizada la identidad, son ejemplos de este talante renovador de la Ley. Sin que ello signifique pasar por alto sus claras deficiencias que he puesto de relieve en otra ocasión[9].

■[9] M. ALVAREZ RICO e I. ALVAREZ RICO .- Derecho de acceso a los Archivos y Registros Administrativos. Revista de Administración Pública, num. 135 (1994).

Finalmente es obligado hacer una breve referencia al reciente Código Penal (Código Penal de la Democracia que sustituye al viejo Código de 1848) que como dice en la Exposición de Motivos pretende "tutelar los valores y principios básicos de la convivencia social. Cuando sus valores y principios cambian".

Dentro de estas directrices se ocupa de los delitos informáticos en varios pasajes: delitos contra la intimidad (título X), delitos contra los atentados informáticos (sabotajes), dentro de los delitos contra el patrimonio (artículo 248); la propiedad intelectual, concretamente los programas de ordenador se hallan protegidos contra quienes con perjuicio de sus autores y con ánimo de lucro, los reproduzcan, plagien o distribuyan o comuniquen pública o privadamente (artículo 270). Ademas se tipifica como conducta criminal la fabricación o tenencia de programas de ordenador especificamente destinados a la comisión de delitos (art. 400).

En función de estos principios en el Título X y dentro de los delitos contra la intimidad y contra el secreto de las comunicaciones, el artículo 197 castiga a quienes usan artificios técnicos de escucha o transmisión y registro de sonido. Castiga también a quien sin autorización utiliza o modifica datos personales o familiares reservados en soportes informáticos u otro tipo de sistema de registro sean públicos o privados. Se considera además como causa de agravamiento de la pena, entre otras hipótesis, (ap. 4), si estos hechos son realizados por los resposables de los archivos o registros informáticos. En otro orden de cosas, se sancionan determinadas conductas criminales realizadas por medios informáticos. Así la utilización ilícita o abusiva de las tarjetas electro-magnéticas considerándolas como robos con fuerza en las cosas o el artículo 248.2 que introduce la figura de estafa o fraude informatico.

En cuanto la propiedad intelectual, los programas de ordenador se hallan protegidos frente a quienes con perjuicio de sus autores y con ánimo de lucro los reproduzcan, plagien, distribuyan o comuniquen pública o privadamente (art. 270) y tipifica como conducta criminal la fabricación o tenencia de programas de ordenador específicamente destinados a la comisión de delitos de falsedad (art. 400).

CONCLUSIONES

1ª.- El Derecho Informático y la Etica son dos disciplinas complementarias, ambas necesarias como instrumentos para encauzar los riesgos que significa la utilización de la Informática.

2ª.- Los asuntos jurídicos relacionados con la Informática no son absolutamente nuevos (intimidad, responsabilidad, propiedad) pero ponen a prueba conceptos tradicionales y exigen la adaptación de los mismos a los nuevos retos que plantea la Informática. No basta para ello aplicar automáticamente los principios legales tradicionales, es necesario profundizar en su naturaleza.

3ª.- La legislación informática debe acompasarse a la rapidez de los cambios que se operan en este área para no quedar desfasada, utilizando siempre que sea posible conceptos ámplios y clausulas generales para evitar el continuo tejer y destejer legislativo. Con este fin se ha propuesto una nueva concepción del Derecho no fundamentada en la sanción judicial, sin valor obligatorio por sí mismo. Es el soft law, basado en la autorregulación que se recoge en las leyes de algunos países como Holanda, Reino Unido, España o Irlanda. Además debe tener en cuenta que la Informática atraviesa las fronteras y en consecuencia el Derecho Informático debe trabajar en la dirección de la busqueda de "un núcleo de Derecho común a todos los países".

4ª.- La doctrina científica y la reflexión teórica serán fundamentales para que la producción legislativa alcance el máximo rigor y no sea dispersa y heterogénea.

5ª.- El Derecho Informático es una disciplina emergente que reclama con fuerza su autonomía como nueva rama del Derecho al lado de las demás disciplinas jurídicas tradicionales. Cabe esperar, por tanto, que las dificultades que existen para su desarrollo en España sean superadas y colmadas las expectativas por la fuerte impulsión de las ideas nuevas. Debemos confiar que los próximos Planes de Estudio de las Universidades aprovechen la ocasión para que la enseñanza de la Informática ocupe el lugar que le corresponde por su importancia. Las carreras jurídicas no pueden sustraerse a las novedades tan profundas que la Informática ha supuesto (recordemos lo dicho sobre Internet). Es asimismo una disciplina básica para quienes como profesionales de la Informática deben conocer suficientemente el régimen jurídico de la Informática y los derechos y responsabilidades que se derivan de su actuación.

Finalmente, debe señalarse que es deber de los profesores o interesados por estos temas, suscitar vocaciones, alertar conciencias y sacudir inercias intelectuales.

Naturaleza jurídica y Valor Probatorio del Documento Electrónico. El caso de la declaración de importación electrónica o mensaje CUSDEC

RENATO JAVIER JIJENA LEIVA

Universidad Católica de Valparaiso (CHILE)

I. INTRODUCCION.

Hoy en día se realizan diversos actos jurídicos por medio de computadores, redes digitales o redes telemáticas, tales como la celebración de contratos, el libramiento de órdenes de pago y la transferencia electrónica de fondos. Hoy en día es también un hecho cotidiano la transmisión de documentos vía telefax. Esta realidad, empero, se contradice con el hecho de que aún estamos inmersos en "la cultura del papel", y frente a ella al derecho le compete armonizar dos intereses concurrentes: por un lado está la necesidad de permitir la más eficaz y la más vasta utilización de las nuevas tecnologías de la información -las NTI-; y por otra parte, será necesario tutelar adecuadamente la confianza de las personas en la autenticidad y seguridad de los documentos generados y transmitidos electrónicamente.

2. Desde la perspectiva del derecho o la ciencia jurídica, más concretamente del "Derecho Informático", y frente al tema de las redes telemáticas y el intercambio electrónico de datos, documentos estandarizados y valores, existen diversas cuestiones jurídicas de relevancia que deben ser analizadas. A modo ejemplar ténganse presente los siguientes problemas: a) la formación del consentimiento en las operaciones y contratos vía redes; b) la firma electrónica o digital como sustituto de la tradicional firma escrita; c) la seguridad y

privacidad de las transmisiones, sobre todo cuando los datos y los documentos sean de una especial naturaleza; d) la desmaterialización de los documentos escriturados en soporte papel; e) la naturaleza jurídica y la acreditación en juicio o valor probatorio de los documentos transmitidos a distancia; y f) las responsabilidades derivadas de la comisión de posibles ilícitos penales o delitos informáticos.

3. Las relaciones comerciales y jurídicas pueden realizarse también por la vía de los sistemas EDI o de "Electronic Data Interchange". En esencia, con este concepto se alude al intercambio electrónico entre sistemas computacionales de información estructurada, es decir, de datos y documentos y mediante formatos, mensajes o estándares acordados previamente por los usuarios. No es errado sostener que el EDI es un correo electrónico con protocolos comunes. Existen diversos estándares de EDI, uno de los cuales es el desarrollado por la ONU y denominado UN/EDIFACT, esto es, traduciendo, el intercambio electrónico de datos o documentos para la administración, el comercio y el transporte. Este es el estándar adoptado por Chile, por diversos países de Latinoamérica, Europa y progresivamente por EE.UU.

4. A propósito de la implementación de los sistemas EDI y del estándar EDIFACT en materia de comercio exterior y en el procedimiento de despacho aduanero de mercancías, el presente trabajo analiza la naturaleza jurídica de la denominada declaración de importación electrónica o "mensaje CUSDEC". Se pretende demostrar, teniendo como fundamento de derecho positivo o sobre la base de lo dispuesto genéricamente en el inciso segundo del artículo 93 de la Ordenanza de Aduanas y en el Decreto de Hacienda Nr.1015 -de febrero de 1995-, que el ordenamiento jurídico chileno ha creado formalmente un nuevo instrumento público electrónico en materia aduanera, al igual que ha ocurrido en otras disposiciones legales.

II. LOS DOCUMENTOS EMITIDOS POR MEDIOS ELECTRONICOS, MAGNETICOS O INFORMATICOS.

A. Concepto y clasificaciones de documentos o instrumentos.

1. En términos amplios debe entenderse por documento o instrumento a cualquier objeto que contiene una información, que narra, hace conocer o representa un hecho, cualquiera sea su naturaleza, su soporte o "continente", su proceso de elaboración o su tipo de firma. Los elementos propios de esta noción amplia son la existencia de un soporte en que constan, un medio que se emplea para grabar los signos, un lenguaje o idioma y un mensaje o "contenido".

En un sentido restringido, con la expresión documento sólo se reconocen a aquellos que están escritos en soporte papel y rubricados o firmados manualmente. Por cierto, esta es la acepción tradicional que hasta diciembre de 1989 imperaba en el ámbito del Derecho Penal chileno.

2. El derecho se ocupa de los documentos o instrumentos para clasificarlos, para regular su forma y valor probatorio, para exigirlos como requisitos de validez de ciertos actos jurídicos (v.gr. escritura pública para la compraventa de bienes raíces), para prevenir y castigar su adulteración, para tutelar la fe pública envuelta en ellos, para salvaguardar su autenticidad, para regular la forma de notificarlos o publicarlos, etc.

3. Atendiendo a su origen, los documentos o instrumentos pueden clasificarse en públicos y privados. Tienen esta segunda naturaleza aquellos que dejan constancia de un hecho sin solemnidad alguna -hay libertad formal-, en cuyo otorgamiento no interviene un funcionario en calidad de tal, y que no llevan en si ningún sello de autenticidad. La principal consecuencia de la distinción radica en que, tratándose de los públicos, en atención a que por la intervención de un funcionario competente y por el cumplimiento de las formalidades requeridas reúnen características de mayor seguridad, autenticidad, integridad y permanencia, el derecho les otorga el máximo valor probatorio. Los ejemplos tradicionales de instrumento público son las escrituras públicas, las sentencias judiciales, las partidas del Registro Civil, etc.

En Chile el inciso primero del artículo 1699 del Código Civil señala que instrumento público o auténtico es el autorizado con las solemnidades legales por el competente funcionario". Nuestra legislación no define a los documentos privados, quedando en consecuencia conceptualizados por exclusión y porque no llevan en si ningún sello de autenticidad.

El artículo 1700 del mismo Código señala que el instrumento público hace plena fe en cuanto al hecho de haberse otorgado y su fecha, pero no en cuanto a la verdad de las declaraciones que en él hayan hecho los interesados -salvo contra los declarantes-. Procesalmente hablando, los instrumentos públicos se prueban y se bastan por sí mismos.

Los instrumentos privados no demuestran, "prima facie", si en realidad han sido otorgados por las personas a quienes se les atribuyen ni tampoco tienen fecha cierta de otorgamiento, pero la legislación procesal admite la posibilidad de tenerlos legalmente por reconocidos. En efecto, el artículo 346 del Código de Procedimiento Civil contempla cuatro formas de establecer la autenticidad, sea expresa, tácita, judicial o extrajudicialmente.

La Corte Suprema ha resuelto que la persona que presente en apoyo de su demanda un documento público no está obligada a justificar la verdad del mismo, sino que la parte que lo refuta o impugna de falso debe acreditar su impugnación. A la inversa, la persona que exhibe un instrumento privado está obligada a probar que es verdadero si la otra parte lo niega.

4. Una "copia" es un documento que reproduce el contenido de otro denominado "original". Tanto el original de un instrumento público, como la copia dada u obtenida en conformidad a los requisitos legales, son instrumentos públicos (342 CPC).

B. Concepto de instrumento o documento electrónico.

1. Fundamentalmente por las operaciones con computadores o vía redes informáticas y telemáticas es que el formalismo jurídico, basado en la preeminencia del documento escrito en soporte papel, está en franca retirada.

2. Los documentos soportados en medios magnéticos no responden al concepto tradicional o restringido de documento manuscrito en soporte papel,

sino al amplio. Por exclusión, entendemos que constituye un documento no electrónico aquel que es elaborado por las formas tradicionales, sean estas manuales, mecanográficas o fotográficas.

Al hablarse de documentos electrónicos se alude a casos en que el lenguaje magnético constituye la acreditación, materialización o documentación de una voluntad ya expresada en las formas tradicionales, y en que la actividad de un computador o de una red sólo comprueban o consignan electrónica, digital o magnéticamente un hecho, una relación jurídica o una regulación de intereses preexistentes. Se caracterizan porque sólo pueden ser leídos o conocidos por el hombre gracias a la intervención de sistemas o dispositivos traductores que hacen comprensibles las señales digitales. El ejemplo quizás más común hoy en día lo constituyen los documentos expresamente construidos para el uso de los terminales de un sistema, como es el caso de las tarjetas magnéticas para acceder a las cuentas bancarias vía cajeros automáticos.

Los documentos electrónicos poseen los mismos elementos que un documento escrito en soporte papel: a) constan en un soporte material (cintas, diskettes, circuitos, chips de memorias, redes); b) contienen un mensaje, el que está escrito usando el lenguaje convencional de los dígitos binarios o "bits", entidades magnéticas que los sentidos humanos no pueden percibir; c) están escritos en un idioma o código determinado (v.gr. el estándar UN/EDIFACT); y, d) pueden ser atribuidos a una persona determinada en calidad de autor mediante una firma digital, clave o llave electrónica.

Cuando para referirse a los instrumentos magnéticos se utiliza la expresión "telemática", que resulta de la unión conceptual y técnica entre las telecomunicaciones y la informática, se quiere aludir al hecho de que un instrumento -por ejemplo la declaración aduanera- resulta de un proceso iniciado con su emisión electrónica desde un ordenador -el del agente- y que continua con su transmisión a otro computador remoto -el del Servicio de Aduanas-.

3. Todo lo dicho en el punto 2 es válido para los documentos electrónicos contenidos en soportes de naturaleza magnética o interna, o transmitidos vía redes telemáticas. Pero existe una segunda especie de documento electrónico, o una problemática particular que surge cuando ellos son impresos computacionalmente.

Por necesidad práctica, como ocurre específicamente con la declaración de importación aduanera que debe imprimirse para retirar las mercancías de los depósitos o pagar los derechos, el documento electrónico tendrá existencia en soporte papel o "estado externo" ("printout"). En este caso la firma digital desaparece, al no intervenir el hombre carecerá de firma manuscrita, y será difícil determinar su autoría, cuestiones que complican al sistema de prueba legal que rige en Chile. Pensemos, como ejemplo, en el caso de los registros en papel que se reciben una vez realizada una operación bancaria vía cajero automático.

Adelantándonos, digamos que en relación a los certificados que imprime el Registro Civil se estableció por ley que ellos eran un instrumento público no obstante estar sin firma manual; y que a propósito de las necesidades del despacho aduanero, se contempló la obligación de que el agente de aduana rubricara la impresión en soporte papel del mensaje "CUSDEC" previamente tramitado, obteniéndose una copia de instrumento público.

III.NATURALEZA JURIDICA Y VALOR PROBATORIO DEL DOCUMENTO ELECTRONICO EN GENERAL.

FACTIBILIDAD DE APLICAR LAS NORMAS SOBRE PRUEBA INSTRUMENTAL AL DOCUMENTO ELECTRONICO, O ADMISIBILIDAD PROBATORIA DEL SOPORTE MAGNETICO.

1. En la legislación comparada o en el derecho extranjero, nada obsta a que las partes intervinientes en un intercambio electrónico de documentos produzcan y los tribunales acepten como prueba el registro magnético de la operación, otorgándole el mismo valor que tendría un documento escrito no obstante que las firmas del emisor y del receptor sean claves digitales o electrónicas. En el evento de un litigio los tribunales no tienen inconveniente en admitirle mérito probatorio, por cuanto su sistema lo rige el denominado "principio del libre convencimiento, de la prueba libre o de la persuasión racional del juez en la valoración de las pruebas". Así ocurre en sistemas procesales como el italiano o el argentino.

2. Una convención como la recién consignada es repudiada por legislaciones como la chilena, donde los medios probatorios de los hechos sobre los cuales eventualmente se litigará y su grado de valor son señalados taxativamente por el legislador, sea en el Código Civil, en el Código de Procedimiento Civil, en el Código de Procedimiento Penal o en leyes especiales.

Por razones de orden público, estas leyes reguladoras de la prueba son inmodificables por la voluntad de las partes. Los sistemas probatorios descritos se fundamentan en el "principio de la valoración legal de los medios probatorios", y en estos, por ejemplo, las normas inhiben a los jueces para utilizar los medios electrónicos como medios de prueba, les imponen expresamente una determinada eficacia probatoria, o también pueden prever su admisibilidad sólo en el caso de faltar otros medios.

3. La prueba documental o instrumental es la que se produce por medio de documentos o instrumentos y en la forma prefijada por las leyes. Goza de gran confianza para el legislador en atención a la fijeza que al hecho a probar da el documento.

La legislación chilena confunde los términos "instrumento" y "documento", los que están en relación de genero a especie respectivamente. El segundo -coincidente con lo que hemos denominado acepción restringida- sería todo escrito que dejara constancia de un hecho sin que sea necesaria una firma manuscrita. El instrumento en cambio, que es equivalente al concepto de "objeto", sería toda cosa mueble, material, corporal, inmaterial o magnética capaz de representar un hecho.

4. Una eventual aplicación del ordenamiento jurídico general sobre la prueba instrumental, para validar o subsumir a los documentos magnéticos, y en caso que no existan leyes especiales sobre un medio electrónico específico, ...pasaría por entender que ambos conceptos aluden, en forma amplia, a todas las cosas en las cuales se expresa por medio de signos una manifestación del pensamiento, resultando indiferente el soporte o "continente" sobre el que dichos signos estén consignados. Esta propuesta se apoya en la denominada "doctrina analógica", y es la que habrían acogido los tribunales del crimen; ella acepta que la enumeración legal es taxativa pero genérica o amplia, de modo tal que cuando la ley habla de documentos o instrumentos alude a toda forma de representación. Esta opción permitirá asimilar los documentos magnéticos a los tradicionalmente existentes.

4.a) Argumentando en favor de la asimilación, puede concebirse que un documento electrónico tiene la naturaleza de "instrumento privado" -y el valor probatorio inherente- sólo en la medida que sea reconocido o mandado tener por reconocido en conformidad al artículo 346 del Código de Procedimiento Civil. Porque un documento electrónico tiene un "contenido" que

consta en un soporte o "continente" y concurren en el los requisitos de escrituración y firma, con las particularidades que el soporte es computacional, que se usan medios de escrituración tecnológica o lenguajes de máquina binarios, y que es atribuible a quien lo emita y digite las claves, llaves o códigos magnéticos (por cierto más seguros que las firmas manuscritas).

4.b) Para afirmar que un documento magnético tiene la naturaleza jurídica de "instrumento público o auténtico", se require que previamente se hayan establecido en un texto legal o reglamentario las formalidades para su otorgamiento o autorización por parte de un funcionario público competente. Anticipándonos al acápite IV, así ocurre con la declaración de importación electrónica o mensaje CUSDEC que validará y legalizará el Servicio Nacional de Aduanas, cuyo carácter de instrumento público es consagrado expresa o explícitamente.

5. Durante mucho tiempo en el ordenamiento jurídico chileno, tradicionalmente la expresión documento o instrumento estuvo reservada para aquellos escritos que constan en soporte papel y que consignan un hecho. Nuestra legislación había seguido la denominada "doctrina legalista", fundamentada en la circunstancia de que la ley enumera taxativamente los medios de prueba, quedando excluidos o sin valor todos los restantes.

Esta situación, y debido al acelerado desarrollo de las tecnologías de la informática y las telecomunicaciones, ha comenzado a revertirse. Si bien es cierto en Chile sólo existen dos artículos en el Código de Procedimiento Penal, y aún no una norma procesal genérica que reconozca la validez probatoria del documento electrónico o soportado en medios magnéticos, homologando su poder de convicción al instrumento tradicional en soporte papel, varias leyes especiales han establecido el carácter de instrumento público o privado para aquellos que obren en soportes magnéticos o que sean transmitidos vía redes "telemáticas". En el evento que se discuta judicialmente la efectividad de haberse realizado o el alcance de los hechos de que dan cuenta los instrumentos electrónicos (v.gr. que se cumplieron las obligaciones, que se envió una factura electrónica, que se emitió una orden de pago a un banco, que se declararon y pagaron las cotizaciones previsionales, que una declaración de importación fue legalizada, que se pagaron los derechos generados, etc.), los tribunales no deberían desconocer el mérito probatorio que por haber sido contemplados legalmente ya les corresponde.

6. En el evento de presentarse conflictos, de requerirse acreditar ante un tribunal hechos que consten en medios electrónicos y aunque las modificaciones legales no sean muchas, también corresponderá a los jueces interpretar las leyes de manera tal de admitirles valor probatorio, entendiendo, por ejemplo, que una firma escrita es el equivalente a una electrónica. Y en este sentido estaría perfilándose la jurisprudencia de los tribunales, de la mano o teniendo como argumentos los textos legales específicos que han abordado el problema y sobre todo en el ámbito de los procesos penales. Porque como se ha afirmado, lo verdaderamente importante no es el "continente" sino el "contenido" del instrumento o documento, la idea o concepto que se quiere reflejar, el mensaje transmitido, y la posibilidad cierta de que ese contenido pueda llevarse a proceso a fin de acreditar los hechos.

7. Las normas del Código de Procedimiento Penal referidas son los artículos 113 y 113 bis, ubicados en el Título relativo a la comprobación del hecho punible y a la averiguación o determinación del delincuente.

El artículo 113 preceptúa que, siempre que sea necesario para el esclarecimiento de los hechos, el juez podrá valerse de resultados obtenidos por medio de la computación, para lo cual, entre otras medidas, determinará la forma como se dejará constancia en el proceso de estas pruebas y podrá designar un asesor técnico que desarrolle o explique la prueba. El artículo 113 bis establece que podrán admitirse como pruebas películas cinematográficas, fotografías, fonografías y otros sistemas de reproducción de la imagen y del sonido, versiones taquigráficas y, en general, cualquier medio apto para producir fe. Sobre el valor probatorio establece que estos medios podrán servir de base a presunciones o indicios.

8. Los textos legales vigentes que en Chile definen la naturaleza jurídica de un instrumento electrónico o que permiten admitir como medios de prueba a los documentos emanados de sistemas informáticos y telemáticos, además de los artículos 113 y 113 bis del Código de Procedimiento Penal y del artículo 93 de la Ordenanza de Aduanas complementado por el Decreto Nr.1015 de febrero de 1995 que se analiza en el acápite IV, entre otros son los siguientes:

8.a) La ley 18.403 del 4 de marzo de 1985, que sancionaba el tráfico ilícito de drogas y estupefacientes, en su artículo 20 señalaba que en la sustanciación y fallo de los procesos por delitos a que se refiere esta ley, los

tribunales podían admitir como pruebas..., en general, cualquier medio idóneo apto y conducente para producir fe.

8.b) La ley 18.680 del 11 de enero de 1988 sustituyó el Libro III del Código de Comercio, relativo al comercio marítimo. En el Título IV sobre los sujetos de la navegación y el comercio, el inciso segundo del artículo 913 establece que las anotaciones que deben estamparse en el diario de navegación o libro bitácora pueden realizarse por medios mecánicos o electrónicos, siempre que éstos garanticen la fidelidad y permanencia de los datos consignados.

8.c) El Título V del Código de Comercio, sobre los contratos para la explotación comercial de las naves, regula en el párrafo tercero el contrato de transporte marítimo. El artículo 1014, sobre la documentación del transporte, señala que la firma en el conocimiento de embarque -documento que acredita la recepción por el transportador de las mercancías- puede ser registrada por cualquier medio mecánico o electrónico.

8.d) El Decreto Supremo del Ministerio de Relaciones Exteriores Nr.380, del 4 de agosto de 1982, promulgó el Convenio sobre Transporte Multimodal de Mercancías y su Anexo, adoptado por las Naciones Unidas el 24 de mayo de 1980. El artículo 5° y a propósito de la emisión de los documentos de transporte multimodal, señala en su numeral 3 que la firma en ellos podrá ser registrada por cualquier medio mecánico o electrónico, siempre que ello no sea incompatible con las leyes del país en que se emitan.

8.e) El Decreto Supremo Nr.114, del 19 de abril de 1989, es el texto legal que fijó el Reglamento del Sistema de Pronósticos Deportivos de Polla Chilena de Beneficencia, en consideración a la captación mecanizada de apuestas.

La norma que regula el registro computacional es el artículo 9, y señala que los pronósticos efectuados por el apostador en el volante serán leídos o captados por medio de los equipos que Polla determine, generándose inmediatamente un registro computacional de la información. De la apuesta realizada quedará constancia en un documento impreso denominado recibo, el que constituye el comprobante y el medio de prueba de la participación del apostador en el concurso. El inciso final del artículo establece que los registros computacionales de las apuestas son el medio válido para acreditar los pronósticos realizados por el apostador, y que toda anotación o señal que

aparezca en el recibo y que difiera de las asentadas en los registros computacionales es nula y de ningún valor.

8.f) Aunque aludiendo en definitiva a documentos impresos en soporte papel y no a uno electrónico, la ley 19.052 del 14 de abril de 1991 consagró explícitamente el carácter de instrumentos públicos de los certificados que el Servicio de Registro Civil expide en forma mecanizada, por medio del procesamiento electrónico de datos, sin intervención del hombre y sin firma manuscrita.

9. En materia de proyectos próximos o no tan próximos a convertirse en ley, cabe consignar los siguientes:

9.a) En 1987 una comisión ad-hoc del Ministerio de Justicia de la época elaboró un proyecto de legislación informática, en que se regulaban los temas del procesamiento de datos personales, de la criminalidad informática y del valor probatorio de los medios computacionales. Algunos artículos de este proyecto disponían que las pruebas informáticas consistentes en discos, en cintas o la reproducción de su contenido se admitirían y apreciarían en conformidad a las reglas que rigen la prueba documental, opción que confería expresamente a todos los documentos electrónicos el carácter de documento jurídico.

9.b) En 1995 se sometió a trámite parlamentario en la Cámara de Diputados un proyecto del Ejecutivo relacionado con el acceso de los particulares a la información administrativa (Boletín Nr.1511-07), el que, por cierto, una vez promulgado como ley regirá para el Servicio Nacional de Aduanas.

El artículo segundo de esta iniciativa legal acoge la noción amplia de documento o instrumento cuando señala, expresamente, que para los efectos de sus disposiciones se considerará como documento a todo escrito, correspondencia, memorándum, plano, mapa, dibujo, diagrama, documento gráfico, fotografía, microfilmes, grabación sonora, video, cualquier dispositivo susceptible de ser leído mediante la utilización de sistemas mecánicos, electrónicos o computacionales y, en general, todo soporte material que contenga información, cualquiera que sea su forma física o características, y las copias de aquellos.

9.c) Aunque desconocemos mayores detalles, sabido es que a partir de diciembre de 1995 el Ministerio de Justicia ha trabajado y estudiado el

tema del valor probatorio del documento electrónico. A consideración de la autoridad se sometió un anteproyecto que busca darle valor probatorio de modo general a los documentos electrónicos, en el cual se establece o propone que todo aquello que pueda hacerse en soporte papel debería tener la misma validez legal que si se hiciera en soporte magnético. Tal propuesta se consideró luego de comprobar o asumir lo complejo que resultaría trasladar el mundo del papel al electrónico, modificando el Código Civil y los Códigos de Procedimiento.

No parece fácil esta opción, que es similar a la del proyecto de 1987 recién comentado. Preferiríamos que las modificaciones o adaptaciones legales fuesen realizadas caso a caso, como ha ocurrido hasta la fecha, en consideración al ámbito en que operen y a la naturaleza, características y realidades propias de cada documento en soporte papel que se reemplace por uno magnético. Reivindicamos sí, la necesidad de confiar en el criterio interpretativo de los tribunales.

IV. NATURALEZA JURIDICA Y VALOR PROBATORIO DE LA DECLARACION DE IMPORTACION ELECTRONICA O MENSAJE CUSDEC.

ANALISIS DEL DECRETO 1015, DE LA MINUTA DEL DEPARTAMENTO NACIONAL JURIDICO DE FECHA 17 DE MAYO DE 1996, Y DEL PROYECTO DE RESOLUCION DEL SERVICIO NACIONAL DE ADUANAS.

Haciéndose eco de las leyes vigentes y los proyectos en estudio ya comentados, creemos que a propósito de la implementación de los sistemas EDI y del estándar EDIFACT en materia de comercio exterior y en el procedimiento de despacho aduanero de mercancías, el ordenamiento jurídico chileno ha creado formalmente un nuevo instrumento público electrónico -o si se quiere "telemático"-, al igual que ha ocurrido en otras disposiciones legales.

A efectos de poner de relevancia las características de la declaración de importación magnética que deben ser determinadas legalmente, consignemos que -"grosso modo"- el modelo de operación electrónica implementado es el siguiente:

a) El agente de aduana, desde su oficina principal y por regla general intermediado por una empresa VAN o red de valor agregado, presentará al

Servicio la declaración de importación electrónica o mensaje CUSDEC, firmada electrónicamente;

b) Si el Servicio de Aduanas rechaza el mensaje, ya sea por un problema normativo o por un problema en la sintaxis UN/EDIFACT, deberá enviar el mensaje CUSRES, especificando cuáles son las causales de rechazo del mensaje CUSDEC previamente enviado, para luego, el agente, iniciar nuevamente el proceso de presentación de la declaración corregida a través de un nuevo mensaje CUSDEC.

c) En el momento en que la declaración sea aprobada, validada y legalizada por el Servicio, éste le asignará un número de aceptación y la firmará electrónicamente -ya no se timbrará al recibirse para acusar recibo de su presentación-, generando un nuevo CUSDEC que será notificado al agente por el sólo hecho de depositarse el mensaje en la casilla electrónica que el despachador tenga en la VAN (numeral 5.10 del proyecto de Resolución del Servicio).

d) Enviado al agente él deberá imprimirlo, firmarlo manualmente y distribuirlo para que siga su curso normal en el procedimiento aduanero de despacho de mercancías.

A. La regulación legal de la declaración de importación electrónica.

El artículo 93 de la Ordenanza de Aduanas establece que la formalización de las destinaciones aduaneras debe hacerse mediante el documento denominado declaración, el que indicará la clase o modalidad de la destinación de las mercancías (importación, exportación, admisión temporal, etc.). La información que deben consignar las declaraciones de destinación aduanera está señalada, imperativamente, en el artículo 94 de la misma Ordenanza.

Un paso fundamental para la modernización de todo el comercio exterior chileno la constituyó la incorporación de un inciso segundo al artord. 93, a instancias de la Cámara Aduanera de Chile, en agosto de 1992 y mediante la ley 19.115. En su virtud, se facultó genéricamente al Director Nacional de Aduanas para autorizar que la formalización de las destinaciones aduaneras se efectúe por medio de la utilización, por los despachadores o agentes de aduana, de un sistema de transmisión electrónica de datos, ...en conformidad a las normas detalladas que establecería el Reglamento.

B. La regulación reglamentaria y administrativa.

1. Dando cumplimiento al mandato legal del artord. 93, el 19 de octubre de 1994 el Ejecutivo dictó el Decreto Supremo del Ministerio de Hacienda Nr.1015, que se publicó en el Diario Oficial del 11 de febrero de 1995, y que en sólo 16 artículos establece las disposiciones en virtud de las cuales el Director Nacional autorizará la formalización de las declaraciones electrónicas o magnéticas.

2. La primera parte del artículo 3 del Decreto 1015, abocado a la definición de los términos empleados en el Reglamento, señala que por formalización mediante un sistema electrónico se entenderán dos operaciones copulativas: la "transmisión" y la "recepción" en los sistemas del Servicio de Aduanas de aquellos mensajes estructurados que contengan todos los datos que sean exigibles para la confección de las distintas destinaciones aduaneras; tal es el caso del mensaje CUSDEC.

3. Perentoriamente, la segunda parte del artículo 3 establece que la formalización vía EDI o los mensajes electrónicos estructurados que posean las características indicadas "constituirán el documento declaración aduanera a que se refiere el inciso primero del artículo 93 de la Ordenanza". El tenor literal es claro: la declaración de importación formalizada electrónicamente o el mensaje CUSDEC es el equivalente legal de la declaración de importación en soporte papel, y porque son equivalentes, podrá hacerse valer en juicio y tendrá el mismo mérito probatorio que las actuales declaraciones timbradas. Siguiendo la tendencia de las diversas leyes consignadas en el acápite III de este informe, nuevamente el derecho positivo ha creado formalmente un instrumento público electrónico, cuyos fundamentos legales son el artord.93 complementado y desarrollado reglamentariamente por el Decreto 1015.

Para el ordenamiento jurídico chileno es instrumento público el otorgado por funcionarios competentes con las formalidades que establece la ley, y él da cuenta o hace plena prueba respecto al hecho de haberse otorgado, de la fecha en que se hizo y de las partes que intervinieron en su otorgamiento. Porque el inciso segundo del artord. 93 lo permite legalmente, y porque la reglamentación del Decreto 1015 ha detallado, precisado y preestablecido los requisitos para tal formalización electrónica, el mensaje CUSDEC o el documento magnético

estandarizado que se envía a los agentes una vez validado, aprobado, numerado y firmado electrónicamente por el Servicio posee las características propias de los instrumentos públicos. Sostener una posición contraria haría absolutamente inoperante la modernización lograda al modificarse el artord. 93 en 1992.

A mayor abundamiento, sería del todo conveniente que el Director Nacional de Aduanas, por la vía interpretativa, ratificara que una declaración electrónica legalizada y transmitida vía sistema EDI a los despachadores hace plena fe y constituye documentación auténtica.

En síntesis, ha habido un expreso pronunciamiento de los entes legislativos y administrativos, admitiendo que la formalización de las destinaciones aduaneras se haga en soportes magnéticos y se firme electrónicamente, y estableciendo que tal operatoria tenga el mismo valor que si se hiciera en soporte papel y con firmas manuscritas.

4. Por otra parte, no admitir la validez legal del instrumento público declaración de importación electrónica y preocuparse sólo por el valor de la copia del mensaje magnético aprobado por la Aduana, que conforme lo establece el artículo 11 del Decreto se origina con su posterior impresión en soporte papel y se certifica con la firma manual que haga en ella un agente de aduana -una nueva formalidad-, significa dejar sin regulación legal u originar una verdadera "zona de nadie". Puede ocurrir que el mensaje CUSDEC validado, numerado y firmado electrónicamente sea manipulado con posterioridad a su envío desde la Aduana, mientras esté almacenado en la casilla que administra la VAN o en el computador del agente de aduana, conductas modificatorias que, de ocurrir, sin lugar a dudas nos llevaría a encontrarnos con una alteración de un instrumento público, que de cometerse dolosamente podría ser subsumida por los delitos tipificados en la ley 19.223.

Aceptar que la posterior impresión en soporte papel del mensaje previa y válidamente recibido por los agentes sólo origina una copia de instrumento público, cuya matriz la constituye la declaración de importación electrónica creada legalmente por el artord. 93 y el artículo 3 del Decreto 1015, evita caer en el error jurídico de sugerir y proponer que se reafirme la validez y preeminencia de los datos contenidos en el documento magnético por la vía contractual o convencional. En este sentido, el Departamento Jurídico del Servicio de Aduanas ha propuesto incluir cláusulas en un contrato que supuestamente deberían suscribir los despachadores con el Director de Aduanas, lo que, como, luego

analizaremos, no es ni necesario ni procedente legalmente. A mayor abundamiento y como también se comentará, repárese en que la preeminencia se consagra expresamente en el artículo 14 del Decreto 1015.

5. Porque el mensaje CUSDEC no es sino una declaración de importación formalizada electrónicamente, que constituye o equivale a la declaración que actualmente se tramita en soporte papel, el artículo 4 del Decreto 1015 señala que la información que contendrán o de que darán cuenta los datos del mensaje está sujeta a un doble requisito.

En primer lugar, debe ser necesaria y precisamente aquella o la misma que exige consignar en las declaraciones de destinación aduanera el artículo 94 de la Ordenanza, en relación al consignatario, detalles, clasificación y valoración de las mercancías. En segundo lugar, la información contenida en los datos del mensaje estructurado debe cumplir con las mismas normas que establecen los artículos 95 al 103 de la Ordenanza para la confección de las declaraciones en soporte papel.

6. Enfrentados al tema de definir quiénes podrán acogerse al sistema de formalización electrónica, el artículo 6 del Decreto 1015 establece que hacerlo será una facultad de los despachadores de aduana. Para incorporarse y operar con el sistema, conforme lo establece el inciso segundo, ellos deberán solicitar previamente al Director Nacional de Aduanas la autorización correspondiente. Resulta adecuado, conforme lo señala el numeral 4.1.1 del proyecto de Resolución "marco", que al momento de solicitarse la autorización se señale la VAN con que se operará y la fecha en que se comenzará a hacerlo.

Con el único objeto de establecer y dejar constancia de las especificaciones técnicas en materia de normas de seguridad y de registro de códigos o firmas electrónicas, a las cuales se sujetará o de cuyo cumplimiento dependerá el otorgamiento de la autorización por parte del Servicio, el inciso tercero del artículo 6 establece que los despachadores y el Director Nacional de Aduanas deberán suscribir, formalmente, un "documento". Así lo reitera el numeral 4.1.1 del proyecto de la Resolución a que alude el artículo 16 del Decreto 1015, proyecto que sólo explicita que las especificaciones técnicas serán entregadas por el Departamento Nacional de Informática.

Es inadecuado considerar que en el Reglamento se obliga a que los despachadores de aduanas y el Director Nacional celebren un contrato, el que

haría surgir o establecería derechos y obligaciones contractuales para la autoridad y los usuarios del sistema EDI. Así lo ha sugerido el Departamento Jurídico del Servicio.

No puede olvidarse que la Aduana está actuando revestida de su imperio público y de sus potestades normativas y fiscalizadoras, en virtud de las cuales podrá decidir autorizar la formalización electrónica, negar la autorización, y posteriormente revocarla por ejemplo a modo de sanción. No puede olvidarse que las obligaciones para la interconexión electrónica estarán establecidas legal, reglamentaria y administrativamente, sin que tenga cabida la autonomía de la voluntad; y no puede olvidarse que los despachadores y el Servicio de Aduanas no son particulares que vayan a realizar intercambio comercial alguno: se trata de una autoridad fiscalizadora que regula la actuación de sus auxiliares en la función pública aduanera.

Conviene tener presente que en materia de despacho aduanero de mercancías no cabe la celebración de una especie de "Acuerdo General de Comercio e Intercambio Electrónico de Bienes y Servicios", contrato que se celebra entre usuarios particulares de EDI y que regula previamente los efectos jurídicos -derechos y obligaciones-de la contratación electrónica, de la transacción o intercambio electrónico. Estas modernas figuras de "contratación informática" sólo serán procedentes, por ejemplo: entre una AFP y el empleador que declara y paga las cotizaciones; entre un cliente y el banco que recibe una orden de pago; entre los comerciantes que se envíen facturas en forma electrónica; etc..

El "documento" a suscribir..., puede ser simplemente aquel en que el agente de aduanas se dé por notificado de la resolución que lo autoriza a formalizar las declaraciones electrónicamente, resolución en la cual, de manera general y amplia, se consignaría que las normas y procedimientos técnicos a que deberá sujetarse el despachador serán determinadas por el Departamento Nacional de Informática. La resolución que autoriza, además, podría consignar que el agente declara recibirlas y se compromete a cumplirlas, bajo sanción de que se cancele la autorización para operar en el sistema EDI.

7. El problema de las copias auténticas de la declaración de importación electrónica que, por conveniencia práctica, son impresas en soporte papel con posterioridad a la tramitación y legalización del mensaje CUSDEC.

El inciso primero del artículo 11 del Reglamento señala que las destinaciones aduaneras formalizadas conforme a lo dispuesto en el artículo 3 serán tramitadas electrónicamente al interior del Servicio de Aduanas. Cómo lógica consecuencia, se dispone que las operaciones de presentación, recepción, verificación, aforo, liquidación y legalización se efectuarán por la misma vía, y se establece que la realización electrónica o magnética de tales operaciones debe armonizarse con lo dispuesto en la Ordenanza.

La armonización referida, hay que consignarlo, no es fácil, por cuanto la Ordenanza establece los procedimientos para el despacho de las mercancías a propósito de documentos escritos contenidos en soporte papel o formularios. Por eso es que al artículo 11 se aboca en sus incisos segundo y tercero a realizar tal adaptación y regular dos situaciones concretas: la existencia de copias válidas en soporte papel del CUSDEC, y la realización del aforo físico de las mercancías conforme a la normativa vigente.

7.a) Partiendo de la base que no todas las operaciones del procedimiento aduanero de despacho de mercancías pueden automatizarse, es decir, aceptando que la implementación de sistemas EDI no puede ser total, el artículo 11 contempla una nueva formalidad propia de la formalización electrónica que autorizó el artord. 93. Se trata de que exista, legalmente, una copia en soporte papel del instrumento público electrónico.

La primera parte del inciso segundo establece que "legalizada la declaración y numerada" ella deberá notificarse electrónicamente al despachador, porque se trata del instrumento público electrónico que nace con la firma -también electrónica- de la Aduana. Esto guarda conformidad con lo dispuesto en los artículos 115 y 116 de la Ordenanza, por cuanto el trámite de notificación sigue siendo posterior a la legalización del documento. Lo señalado, en definitiva, importa cumplir con lo dispuesto en la parte final del inciso primero del artículo 11 del Reglamento, esto es, se está armonizando o adecuando la tramitación electrónica a la normativa actualmente vigente.

En atención a que posteriormente será necesario retirar las mercancías depositadas, pagar derechos en los bancos, etc., y porque dichos trámites aún no pueden realizarse electrónicamente (es ilógico esperar, por ejemplo, que Emporchi entregue las mercancías contra la presentación de un diskette), ...el artículo 11 del Decreto 1015 obliga a los agentes de aduana a que impriman la declaración electrónica previamente aprobada que reciben, a que nuevamente la firmen pero

ahora en forma manuscrita, y a que la distribuyan, todo en conformidad a las instrucciones que imparta el Director Nacional de Aduanas.

Esta solución legal y reglamentaria, que establece una nueva formalidad propia de la presentación electrónica de las declaraciones y una nueva obligación para los agentes de aduana, quienes con su firma están acreditando que se trata de la copia auténtica impresa en papel de un instrumento público ya legalizado por el Servicio, guarda total coherencia con una de las notas fundamentales del actual sistema aduanero, esto es, que el agente es ministro de fe y auxiliar de la función pública aduanera.

En consecuencia no sería procedente, como lo ha contemplado el Departamento Jurídico del Servicio, que la Autoridad y los despachadores establezcan contractual o convencionalmente que la impresión posterior del CUSDEC en papel haga plena prueba respecto de ellos, máxime cuando la Aduana que fiscaliza y el agente que tramita no son partes vinculadas contractualmente.

El proyecto de Resolución aborda este tema en el numeral 5.11. Agrega que la impresión deberá realizarse en la oficina central del agente, lo que apunta en beneficio del principio de la personalidad del despacho. Señala la Resolución propuesta que la impresión se realizará en un formulario proporcionado por el agente y confeccionado según el formato, contenido y número de ejemplares que para cada destinación determine el Servicio.

7.b) El mandato de adecuar la tramitación electrónica a lo dispuesto en la Ordenanza, contemplado en el inciso primero del artículo 11 en análisis, es particularmente importante en relación al artículo 227 de la Ordenanza. En efecto, allí se establece, precisamente, que las copias auténticas de una declaración de importación otorgadas por el agente deben corresponder a un documento previamente legalizado por el Servicio.

A mayor abundamiento y de forma complementaria, cabe considerar una indicación realizada a instancias de la Cámara Aduanera de Chile A.G. precisamente al inciso quinto del artículo 227 de la Ordenanza, con ocasión del actual debate del proyecto de ley que moderniza el Servicio Nacional de Aduanas. Esta indicación podría ser considerada en el Decreto con Fuerza de Ley que, a futuro, dictará el Presidente de la República en materia de implementación del sistema EDI.

La modificación propuesta fue la de reemplazar el inciso por el siguiente: "Se tendrán por auténticas, para todos los efectos legales, es decir, conforme con el valor de los documentos que se reproducen, las copias que los agentes de aduana otorguen sobre cualquiera de las actuaciones que comprende el despacho en que han intervenido o de los documentos que se requieren para este. Las copias podrán ser fotocopiadas, impresas por medios computacionales, contenidas en soportes magnéticos o en mensajes estandarizados aprobados por la Aduana, que los despachadores emitan directamente a través de sus sistemas computacionales".

8. Sobre la base de lo dispuesto en el artículo 3° del Reglamento, hemos sostenido que la presentación de documentos electrónicos estandarizados es una nueva modalidad de presentación de las declaraciones, llamada a reemplazar y con el mismo valor legal que la formalización manual o en soporte papel que actualmente opera. Tal hipótesis es expresamente corroborada por el artículo 12 del Decreto 1015, donde se establece que las exigencias de presentación y formalización de las destinaciones se entenderán cumplidas, para los efectos de lo dispuesto en los artículos 92 y 93 de la Ordenanza, a través de la transmisión electrónica de todos los datos que sean exigibles para la confección de las distintas declaraciones y su recepción en los equipos del Servicio de Aduanas.

9.a) El artículo 14 del Decreto 1015 establece que el Servicio de Aduanas, no otro ente, deberá conservar archivos magnéticos con las declaraciones electrónicas que ha legalizado y numerado, preservando su integridad e inviolabilidad.

De aquí que sea cuestionable lo señalado en el numeral 3.5.1 del proyecto de Resolución, donde se obliga a las empresas VAN a que en una "nueva casilla electrónica adicional" -distinta a la que debe mantenerse para el tráfico-, mantengan depositada por el plazo de un año la información enviada por el Servicio, aunque correspondan única y exclusivamente a "duplicados" -otras copias pero ahora electrónicas y no impresas en papel- de los mensajes que la Aduana hubiese enviado a los despachadores.

La Resolución va más allá de lo establecido en el Decreto 1015, porque si bien es cierto autoriza a que pasado el año la VAN elimine la información, exige además: que previamente ella sea traspasada a un medio externo de respaldo que estará a disposición del Servicio por un plazo de cinco años calendarios; que se

asegure el acceso en línea a esta casilla adicional (3.5.2); y que se cuente con los mecanismos para que la información depositada en la casilla adicional sea consultada por el Banco Central, la Tesorería General de la República y el Servicio de Impuestos Internos (3.5.3). Antes, en el numeral 3.3.3., la Resolución propuesta obliga a las VAN's a que velen por la confidencialidad de la información del Servicio.

En el evento que lo establecido en los numerales referidos signifique que el Servicio no almacenará una versión de los mensajes que legalice y notifique, creemos que tal opción se opondría o vulneraría la prohibición del artículo 16 del Decreto 1015, esto es, que el Servicio de Aduanas estaría traspasando a terceros facultades -más precisamente obligaciones- que las leyes le han entregado a la Autoridad.

9.b) Pero además este artículo despeja toda duda acerca de la preeminencia del instrumento público electrónico o mensaje CUSDEC legalizado, notificado y almacenado por el Servicio, ya sea respecto de los archivos de la VAN, de los archivos de los agentes o de las copias que estos impriman en papel en conformidad al artículo 11. La norma establece, expresamente, que la declaración conservada en archivos magnéticos por el Servicio "servirá de base para los efectos de las revisiones y/o fiscalizaciones que procedan".

Sobre todo en el evento que sea necesario realizar un cotejo entre la copia impresa por un agente y el documento electrónico archivado magnéticamente en la base de datos del Servicio, nadie podría desconocer la preeminencia del segundo. Por ende, nos parece equivocado lo afirmado en la minuta del Departamento Jurídico cuando considera "viable" que, por la vía contractual o convencional, se establezca que un funcionario de la Aduana deba imprimir y autorizar una copia de instrumento público que haría plena prueba en contra del agente y primaría por sobre la copia que él debe imprimir.

Valor Probatorio del Documento Electrónico. Su autenticidad a través de la Criptología

JOSE MANUEL NUÑEZ JIMENEZ

Doctorando Curso "Valor Probatorio de los Documentos Electrónicos" dirigido por el Profesor Carrascosa López. UNED.

I. INTRODUCCIÓN

La aplicación de las nuevas tecnologías en todos los ámbitos de nuestra sociedad lleva consigo un cambio en multitud de aspectos de la vida diaria y profesional que hasta épocas recientes se habían mantenido prácticamente inalterables.

Así, con el empleo del ordenador, se hace posible recopilar una amplia información sobre cada persona, reuniendo un conjunto de datos que aisladamente nada dicen, pero que al ser presentados en forma sistematizada, pueden dar lugar a una información que el afectado no se imagina ni le agradaría ver en poder de otros. Tengamos presente que un ordenador puede clasificar y relacionar rápidamente, por ejemplo, nuestros datos laborales, económicos, legales, sanitarios, etc, construyendo un detallado perfil de cada individuo.

El desarrollo actual de la tecnología ha provocado el surgimiento de diversos instrumentos que, por sus características, se apartan de los tradicionales; así desde los más simples hasta los más sofisticados: máquina de escribir,

telégrafo, teléfono, fonógrafo, cinematógrafo, dictáfono, cinta magnetofónica, fotocopiadora, contestadores telefónicos automáticos, procesadores de textos, correo electrónico, videotex, telefax, télex, satélites de comunicación. Dentro de esta proliferación es evidente que existe una fagocitación de los medios más modernos respecto a los más antiguos, de modo que van sustituyéndose unos a otros.

La utilización de todas estas herramientas de forma cada vez más frecuente por empresas, particulares e incluso las Administraciones Públicas, plantea la necesidad de llevar a cabo un proceso de adaptación, tanto en el campo operativo de la técnica como en el conocimiento y valoración de las consecuencias de su implantación. Es en este último sector donde existe mayor número de lagunas, tomando una relevancia más destacada en el ámbito del Derecho, donde casi siempre existe un gran desajuste entre la realidad y su regulación legal.

España se incorporó a todo este panorama de forma tardía e insegura, de todas formas, actualmente se han dado pasos hacia el futuro aceptando la contratación por télex o fax, el uso de tecnologías como el sistema EDI, Internet, Infovía, etc, habiéndose manifestado, ya, la jurisprudencia acerca de su validez y aceptación.

El uso de estas tecnologías ha hecho resentirse la seguridad jurídica en el campo procesal, ya que en caso de acudir a los tribunales, surge una enorme dificultad probatoria en torno a todos estos avances.

Hasta ahora la doctrina se había ocupado de estudiar como "*nuevos campos probatorios*" la llamadas pruebas técnicas y científicas, a modo de casos de laboratorio de repercusión sectorial.

Por el contrario, con las técnicas de funcionamiento digital y enlace a distancia, con lo que se ha dado en llamar "*documento electrónico o informático*", no se está ya ante casos relativamente poco aplicables, sino que nos enfrentamos con la necesidad de tener que validar como medio probatorio una nueva forma de expresión del pensamiento y de la actividad humana.

Se trata de una nueva técnica, cada vez más potente y masiva, que en el plano social y económico va sustituyendo al papel, hasta este momento portador documental por excelencia, por lo que sobrevendrán consecuencias jurídicas de enorme calado.

Con la invención de la imprenta por Gutemberg, fue el papel, la forma más común de registrar definitivamente las actividades entre los hombres. Su empleo adquiere especial relevancia al incorporarle la firma, que denota la autoría, paternidad y veracidad del contenido, constituyéndose, así, el papel como el garante de la fehacencia y credibilidad, es decir, como válido y probatorio para la ley.

Sin embargo, en las sociedades actuales, se está pasando de esta forma tradicional de registro y comunicación, a otra que potencia el intercambio de información eliminando barreras de espacio y de tiempo.

Gran número de autores no dudan en afirmar que no hay inconveniente en considerar al **documento electrónico** como **documento escrito**, ya que, **contiene un mensaje** (texto alfanumérico o diseño gráfico) **en lenguaje convencional** (el de los bits) **sobre soporte** (cinta o disco) y **está destinado a durar en el tiempo**.

Al convertirse el ordenador en el único instrumento capaz de satisfacer las necesidades sociales, jurídicas y económicas, va a existir una gran cantidad de documentación desarrollada en forma automatizada lo que provoca el problema de su seguridad jurídica.

Así en la esfera procesal, además de otros campos de influencia, surgió un desequilibrio acerca de la aceptación del documento electrónico como mecanismo de prueba.

El problema se planteó en lo que se refiere a si los nuevos soportes electrónicos o informáticos se podían considerar enmarcados dentro de la clasificación de medios de prueba establecidos en los art. 1215 del Código Civil, art. 47 del Código de Comercio y art. 578 de la Ley de Enjuiciamiento Civil.

Evitando entrar en el farragoso debate doctrinal, la mayoría de los autores considera que los soportes utilizados en el área de la informática, no pueden calificarse de autónomos medios de prueba, sino que se engloban dentro de la prueba documental y, más concretamente, en el concepto de "*instrumentos, archivos, asientos o papeles privados*" a que se refiere el art. 1228 del Código Civil o el art. 578 de la Ley de Enjuiciamiento Civil.

Esta aceptación es, ante todo, coherente con el devenir de la humanidad, ya que negar la utilización procesal de estos nuevos instrumentos y técnicas puestos al servicio de los hombres, sería cerrar los ojos ante el mundo que nos rodea, hecho por el que la historia nos juzgaría.

Supongamos que tanto jueces como abogados no hicieran uso de estos medios. Se llegaría a tal descoordinación entre la práctica judicial y la vida social, que podría llegar a hablarse de indefensión.

Una interpretación coherente del art. 24 de la Constitución de 1978, que ponga en relación el párrafo 1, en lo relativo a la prohibición de la indefensión, y el párrafo 2, que reconoce el derecho a utilizar los medios de prueba pertinentes para la defensa, debe llegar a la conclusión de que en el proceso han de ser admisibles como prueba, todos los nuevos descubrimientos y avances técnicos; por lo tanto, su inadmisión debe abrir la posibilidad de interponer recurso de amparo ante el Tribunal Constitucional.

Diferentes sentencias del Tribunal Supremo y del Tribunal Constitucional reconocen y aceptan la utilización de estos medios, como modalidad independiente y singular de la prueba documental.[1]

II. VALOR PROBATORIO DEL DOCUMENTO ELECTRÓNICO

El documento electrónico es el documento proveniente de la elaboración electrónica. Debe tener una serie de características como, ser inalterable, legible gracias a un procedimiento adecuado, debe ser identificado respecto al lugar y al tiempo y debe ser estable.

La admisión del documento electrónico como prueba en un proceso exige reunir una serie de requisitos :

■[1] **STC 128/88 de 27 de Junio y STC 190/92, de 16 de Noviembre**: *"no cabe negar valor probatorio a las transcripciones de una cinta magnetofónica cuando, han sido incorporadas a los autos, no han sido impugnadas en todo o en parte, y se dan por reproducidas en el acto del juicio oral".*

STS de 24 de Marzo de 1994, Sala Primera : *"...el concepto de documento ofrece una mayor amplitud en cuanto referido al medio u objeto a través del cual se manifiesta un pensamiento o idea... lo que viene amparado por el art.1215 del Código Civil, al emplear el término de instrumentos en lugar del de documentos".*

a) que pueda demostrarse por quien pretende valerse del mismo, que el equipo utilizado para la creación del documento funciona correctamente.
b) que sea demostrable la bondad de los procedimientos de datos utilizados en la entrada de la información al ordenador, de modo que quede asegurada la exactitud de los registros en todo su recorrido.
c) que sean comprobables los medios de almacenaje, tratamiento y elaboración de la información y de preparación de su salida a fin de garantizar la fiabilidad del registro.
d) que sea un caso en el que el documento electrónico viene a hacer prueba en contra de su titular o propietario.
e) que la veracidad de la información pueda ser corroborada por otros medios complementarios
f) que puedan llegar a identificarse con precisión los sujetos participantes y las operaciones realizadas por cada uno de ellos en el proceso de elaboración del documento electrónico

La jurisprudencia ha abierto la mano en lo relativo a la admisibilidad probatoria de las fuentes de prueba de naturaleza electrónica. Así el Tribunal Supremo, en sentencia de la Sala 2ª, de lo Penal, de 5 de Febrero de 1988, abordando el problema del valor probatorio de la grabación telefónica, señala la legitimidad de tal prueba, afirmando que las relaciones de medios probatorios de las leyes de procedimiento no tienen el carácter de exhaustivos, por lo que las innovaciones tecnológicas deben incorporarse al acervo jurídico procesal.

Después de todo un debate sobre la naturaleza del documento electrónico como medio de prueba, la mayor parte de la doctrina considera que los soportes en el área de la informática, se enmarcan dentro de la prueba documental en el concepto "*instrumentos, archivos, asientos o papeles privados*".

Esta problemática sobre la admisión de los documentos electrónicos como medios de prueba, ha sido obviada en otros ordenamientos en los que el legislador, haciéndose eco de su realidad, ha decidido incorporarlos de modo directo al Derecho positivo.

Este es el caso del **Código Civil Italiano**, cuyo art. 2712 sí recoge, en relación al art. 261 del Código de Procedimiento Civil, tales medios de prueba.

Esta misma postura ha sido adoptada por el **Código Civil Portugués**, el cual los ha incorporado en su art. 362, que introduce un concepto jurídico de documento extraordinariamente amplio.

Respecto a la **normativa francesa**, el art. 1348 del Código Civil admite desde 1980 una vía que posibilita la admisión como prueba, en los casos en los que el original no exista, de una copia, siempre que sea definitiva y fehaciente, lo cual podría ser la impresión de un documento electrónico si se prueba que la misma es auténtica, en el sentido de que coincide con el documento electrónico y no ha existido manipulación alguna.

Si bien queda claro la admisión del documento electrónico como medio de prueba, aquél puede presentar estas manifestaciones :

a) el documento en soporte electromagnético (disco, disquete..)
b) el documento sobre papel preparado mediante ordenador, lo que conduce, bien a buscar nuevas técnicas de autenticación, bien a configurar un concepto jurídico que los acepten tal como salen del ordenador.
c) el documento transmitido de ordenador a ordenador o de terminal a terminal

El valor probatorio depende de la clase de prueba documental que el documento electrónico constituya. Si el documento se ha efectuado en presencia de un fedatario público, será documento público la transcripción por impresora o el documento transmitido.

Cuando las modalidades se han confeccionado privadamente, el problema se agudiza, pero la autenticidad del documento puede quedar establecida por su admisión por la otra parte, por su reconocimiento bajo juramento a la presencia judicial y por la prueba pericial.

El documento, electrónico o no, es un medio de prueba tasado que el juez debe valorar de acuerdo con lo establecido con las normas legales, aunque la jurisprudencia del Tribunal Supremo y la regulación del recurso de casación han hecho de esta prueba una más de valoración libre.

III GARANTÍAS DE LA AUTENTICIDAD DEL DOCUMENTO ELECTRÓNICO

III.1. Derecho Español

La utilización del documento electrónico como medio probatorio exige la necesaria y precisa adveración y certificación de autenticidad, veracidad y fidelidad que encuentra cauce procesal adecuado mediante el reconocimiento judicial, sometido a las reglas de procedimiento y valoración previstas.

La consideración como documento o no a efectos procesales es un aspecto relevante puesto que esa calificación lleva consigo la aplicación a su vez de las normas de valoración propias de los documentos, sin que en ese caso pueda tener entrada la libre apreciación del juez.

Si ambas partes reconocen el contenido de un documento electrónico como tal, éste produce prueba entre las partes, sin que en estos casos pueda el juez llevar a cabo una apreciación libre del mismo. Por el contrario, si una de las partes no reconoce la autenticidad del documento, habrá que pasar a la prueba de peritos y, si ello no fuera posible, a la de reconocimiento judicial.

Si éste es el aspecto procesal de la autenticidad del documento electrónico, su problemática mayor es la aparente facilidad con la que pueden modificarse. Es esta característica la que crea una mayor inseguridad, puesto que en muchas ocasiones dichas modificaciones no dejan rastro alguno, por lo que el poder probar que el documento objeto de litigio sigue siendo el mismo que cuando ocurrieron los hechos puede llegar a convertirse casi en una prueba diabólica y de imposible consecución.

Por ello, el objetivo de las partes debe ser acreditar que el sistema informático es seguro, de modo que sea posible seguir la pista de cualquier modificación que el documento haya sufrido. Si es posible acreditar este extremo, no hay duda de que la tarea de llevar al juez a la convicción de que aquél sigue siendo auténtico no será tan ardua.

Hoy en día existen un gran número de métodos para evitar las alteraciones que supone la ausencia de autenticación. Así podemos encontrar el doble tecleo, programas de control, la verificación del mensaje, la utilización del

testing, programas de pa idad y disparidad sobre cada carácter, y posteriormente sobre todos los bytes que tienen la misma posición dentro del carácter transmitido, controles y registros en la actividad de los posibles intervinientes, en la elaboración y transmisión de un mensaje...

Las **técnicas de autenticación** del documento electrónico son:

a) la criptografía o criptología : es objeto de análisis en el apartado IV,
b) el código secreto o de ingreso : supone una combinación determinada de números o de letras que sólo es conocida por el titular del mismo,
c) métodos basados en la biometría : se puede entender la identificación de un determinado operador a través de datos físicos o biológicos, si bien, necesitaríamos un sistema auxiliar para verificar la autenticidad del contenido del documento.

Las técnicas de autenticación y su fiabilidad determinarán la fuerza probatoria del documento electrónico, que obligará a las partes, vinculándose éstas, a la inalterabilidad del documento. Las normas deben propugnar la admisión de las formas de autenticación de los documentos electrónicos.

Estas nuevas técnicas son tan aceptables como la tradicional firma manuscrita. Al igual que con ésta, la signatura informática es un medio para identificar al titular o propietario del documento electrónico.

La **signatura electrónica** supone ser elaborada a través de procedimientos criptográficos, llevar un resumen codificado del mensaje y de la identidad del emisor y del receptor. Son características de la signatura electrónica :

- debe permitir la identificación del signatario,
- no puede ser generada más que por el emisor del documento, infalsificable,
- las informaciones que se generen a partir de la signatura electrónica deben ser suficientes para poder validarla, pero insuficientes para falsificarla,
- la aposición de una signatura debe ser significativa y va unida indisociablemente al documento a que se refiere,

• no debe existir dilación de tiempo ni de lugar entre aceptación por el signatario y la aposición de la signatura.

No existirá signatura sin intervención humana.

III.2. Derecho Comparado

La **normativa inglesa**[2] proporciona una regulación más detallada que la española. Establece dos criterios que confieren una valoración a la prueba aportada. El primero de ellos se centra en determinar si la información fue facilitada o archivada en el ordenador al tiempo en que los hechos ocurrían. El segundo de ellos se resume en conocer si la persona que en ese momento operaba el sistema o introducía los datos tenía algún motivo para falsear los hechos.

La mejor arma para convencer a un tribunal de la autenticidad de un documento electrónico es la posibilidad técnica de poder determinar la propia historia del documento desde su génesis, es el denominado "*audit trail*". Éste debería ser capaz de determinar cuándo el documento tuvo entrada en el ordenador, qué operador lo manejaba en ese momento, en qué ocasiones se accedió al mismo y por quién, si se modificó y qué extremos fueron modificados.

La seguridad del proceso en el Reino Unido ha hecho que se redactase por la Asociación Británica de Estándares, un catálogo de recomendaciones a seguir para aquellos que pretendan asegurar del mejor modo posible, de acuerdo con la técnica, las posibilidades de utilizar documentos electrónicos dotándoles de validez jurídica.

En el **Derecho norteamericano** son necesarios estos requisitos para considerar que un determinado sistema informático tiene implantado un proceso seguro de autenticación :

■[2] Civil Evidence Act.

- **conservación de archivos**: los documentos electrónicos deben conservarse durante, al menos, el mismo período de tiempo que si fueran documentos en papel.
- **seguridad e integridad de los datos**: se debe estar en posición de demostrar que a los documentos electrónicos no puede accederse sin control previo.
- **sistema de documentación**: el sistema de archivo electrónico debe estar debidamente documentado, incluyendo descripción física y lógica de la estructura de los programas, así como de las entradas y salidas de la información.
- **sistema de archivo de copias**: se debe tener en soporte físico aquellos documentos sobre los cuales una normativa específica obligue a ello (escrituras públicas, contratos con la Administración...).
- **accesibilidad del sistema**: los documentos electrónicos deben poder ser accesibles a través de su lectura o visualización en la pantalla del ordenador.

No obstante, el satisfacer los anteriores requisitos no constituye una garantía absoluta de autenticidad, si bien no hay duda de que puede mejorar sustancialmente la valoración que de los mismos lleve a cabo un tribunal.

IV. LA CRIPTOGRAFÍA O CRIPTOLOGÍA COMO GARANTIA DEL DOCUMENTO ELECTRÓNICO

Como he señalado anteriormente, se trata de una de las grandes categorías de las técnicas de autenticación del documento electrónico.

La protección que brinda el ordenamiento jurídico es una protección "*a posteriori*" que, por las características de la información, y la propia naturaleza de la tecnología informática, en muchos casos resulta insuficiente para el logro efectivo de la protección del derecho de secreto para los datos sensibles, por lo que, además de la protección jurídica, se requieren medidas de prevención que, "*a priori*", impidan materialmente el éxito de las amenazas contra la información almacenada, tratada o transmitida electrónicamente.

La criptología se incorpora al sistema de información una vez determinado qué ha de protegerse y con qué niveles. Se puede definir como un sistema de codificación de un texto con unas claves confidenciales y de procesos

matemáticos complejos (algoritmos) de forma que resulte incomprensible para el tercero que desconozca la clave descodificadora.

La criptología ha venido siendo utilizada tradicionalmente en los ámbitos militar, diplomático y comercial. Actualmente, se ha ampliado a otro usos mucho más próximos aunque con niveles de exigencias diferentes, entre los que son cada vez más frecuentes, las aplicaciones destinadas a la protección de los derechos y libertades.

La forma tradicional de preservar la confidencialidad de una red de comunicaciones ha sido la protección criptológica, que implica la utilización de técnicas que permiten llevar a cabo el ocultamiento de la información protegida a personas no autorizadas. Siendo esto así, la criptología se convierte en una exigencia imprescindible.

La protección criptológica presenta diversos grados de infalibilidad, según se trate de intereses de extrema importancia, o de intereses de menor relevancia, es decir, según se trate de comunicaciones públicas o privadas. Mientras que en las primeras la regla general es la transparencia, en las segundas prima el imperio del secreto profesional. Esto nos llevaría a la necesidad de protección sistemática de las comunicaciones privadas y, excepcionalmente, de las públicas.

A modo de ejemplo, **en el ámbito nacional,** la Ley 30/1992, de 26 de Noviembre, de Régimen Jurídico de las Administraciones Públicas y Procedimiento Administrativo Común, contribuye a la definición de ámbitos necesitados de protección. En este sector, y debido a los principios de cooperación, coordinación y colaboración entre Administraciones Públicas, se hace imprescindible la intercomunicación y la transmisión telemática de registros, lo que dificulta la protección exhaustiva de los datos asentados.

También la Ley Orgánica 5/1992 de 29 de Octubre sobre Regulación del Tratamiento Automatizado de Datos de Carácter Personal, deja cabida a la protección criptológica[3].

■[3] Art.9. *"1.- El responsable del fichero deberá adoptar las medidas necesarias para garantizar la seguridad de los datos de carácter personal.2.- No se registrarán datos de carácter personal en ficheros automatizados que no reúnan*

En el ámbito comunitario, hay referencias a la protección criptológica en la Decisión del Consejo de 31 de Marzo de 1992, relativa a la seguridad de los sistemas de información; en la Recomendación del Consejo de la OCDE de 26 de Noviembre de 1992, que contiene las líneas directrices para la Seguridad de los Sistemas de Información; en el Convenio de 28 de Enero de 1981 para la protección de las personas con respecto al tratamiento automatizado de los datos de carácter personal y en la Propuesta de Directiva del Consejo relativa a la protección de datos personales y de la intimidad, en relación con las redes públicas digitales de telecomunicación, y, en particular, la Red Digital de Servicios Integrados y las Redes Móviles Digitales Públicas.

La protección criptológica de los datos "*sensibles*", se sitúa en el contexto de la aplicación de las nuevas tecnologías de la información en el entorno social, jurídico y político de una sociedad democrática, donde encuentra su reforzamiento y legitimación, pero también sus límites. Globalmente considerada, requiere la adecuación de los niveles de protección a la naturaleza de la información protegida, de forma que haga posible el juego de los distintos derechos afectados.

Todo derecho tiene sus límites en relación a los derechos fundamentales que establece la Constitución. La protección criptológica debe respetar la Norma Suprema, evitando posibles colisiones con derechos y libertades que gozan de protección específica. Este es el caso de entrar en polémica con los derechos al honor, la intimidad y la propia imagen.

Estas garantías de no intromisión de las prácticas criptológicas en los derechos fundamentales, están reflejadas en normas internacionales (art.29.2[4] de la

las condiciones que se determinen por vía reglamentaria con respecto a su integridad y seguridad y a la de los centros de tratamiento, locales, equipos, sistemas y programas.".

Art.20.2. "*La recogida y tratamiento automatizado para fines policiales de datos de carácter personal...deberán ser almacenados en ficheros específicos establecidos al efecto, que deberán clasificarse por categorías, en función de su grado de fiabilidad.*".

■[4] "*En el ejercicio de sus derechos y en el disfrute de sus libertades toda persona estará solamente sujeta a las limitaciones establecidas por la ley, con el único fin de asegurar el reconocimiento y el respeto de los derechos y libertades de los demás, y de satisfacer las justas exigencias de la moral, del orden público y del bienestar general en una sociedad democrática*".

Declaración Universal de Derechos Humanos, art. 19.2[5] y art. 19.3[6] del Pacto Internacional de Derechos Civiles y Políticos y el art.10 del Convenio Europeo para la Protección de Derechos Humanos y Libertades Fundamentales.

Por otro lado, existen dos grandes técnicas criptológicas :

a) **sistemas simétricos** : el emisor, como el destinatario de un mensaje disponen de la misma clave para el cifrado y descifrado de aquél.
b) **sistemas asimétricos** : funcionan por la combinación de dos tipos de claves, una pública y otra secreta que se corresponden.

Uno de los grandes inconvenientes de la protección criptográfica es su coste tan elevado. Si bien, y a pesar de esto, las ventajas que supone la transmisión electrónica, aunadas con las garantías de seguridad que nos ofrece la criptología, superan con mucho el inconveniente anterior.

En los llamados "***sellos del software***", es el mismo ordenador el que asocia a cada instrucción un valor numérico, y así, si el programa se modifica, el valor de las instrucciones que lo componen se altera, y es el mismo ordenador, el que comprobando la desigualdad entre las claves y el valor numérico del programa, rechazaría la ejecución del mismo, señalando sus alteraciones.

El uso de la criptología para la codificación de la información en ordenadores y redes, al igual que los sistemas de control de accesos mediante *passwords*, suponen un obstáculo técnico para la investigación de los hechos presuntamente delictivos, pero es la única forma, también, de preservar la intimidad y propiedad de la información. Dilema, éste, que cebe ser resuelto a

■[5] "*Toda persona tiene derecho a la libertad de expresión; este derecho comprende la libertad de buscar, recibir y difundir informaciones e ideas de toda índole, sin consideración de fronteras, ya sea oralmente, por escrito o en forma impresa o artística, o por cualquier otro procedimiento de su elección*".

■[6] "*El ejercicio del derecho previsto en el párrafo 2 de este artículo entraña deberes y responsabilidades especiales. Por consiguiente, puede estar sujeto a ciertas restricciones, que deberán, sin embargo, estar expresamente fijadas por la Ley y ser necesarias para: a) asegurar el respeto a los derechos o a la reputación de los demás; b) la protección de la seguridad nacional, el orden público, la salud o la moral públicas*".

tenor de conceptos genéricos tales como la Justicia y la Seguridad, bajo la perspectiva de nuestra Constitución y de todo el Ordenamiento Jurídico.

Por lo tanto, es conveniente que los países vayan incluyendo en sus leyes la regulación y consecuencias de las prácticas criptológicas, ya que éstas no son inocuas. Utilizadas de forma abusiva o fraudulenta, puede, no sólo atentar contra la libertad de información, sino obstaculizar el normal desenvolvimiento de la sociedad y el Estado, a través de la creación de reductos impenetrables.

CONCLUSIONES

Partiendo del hecho de que el documento electrónico está admitido mayoritariamente en la doctrina, como otro medio de prueba más en el proceso, nos encontramos con que, a diferencia del soporte papel, aquél plantea el inconveniente de su fácil modificación, incluso en ocasiones, sin dejar rastro.

En estas situaciones, intentar probar la autenticidad de un documento se convierte en algo de imposible consecución.

El principal escollo, por tanto, será la admisión de una prueba por el juez. Para demostrar la autenticidad del documento hay que retrotraerse al origen del problema, es decir, plantear seriamente el tema de la seguridad de los datos sensibles y demás clases de datos. Su abordaje se hará, no sólo, desde una perspectiva eminentemente legislativa, sino también desde un prisma práctico de concreción de medidas.

Los esfuerzos deben ir encaminados a que todas las declaraciones de intenciones que aparecen en las leyes, se tornen en auténticas tomas de postura contra el mal empleo de los datos personales y los intentos de infringir las leyes.

La lucha contra la inseguridad informática, debe venir dada por la aportación de una serie de mecanismos capaces de impedir el falseamiento, modificación y la utilización fraudulenta de los datos contenidos en soporte electrónico.

Uno de esos mecanismos, quizá el más efectivo, es la criptología, técnica no muy desarrollada y que de generalizarse su empleo, forzaría su regulación, supliendo el vacío legal hasta hoy existente. Con las técnicas criptográficas se protegería la seguridad y autenticidad de los datos, debiendo tener en cuenta el legislador el peligro, en el ámbito delictivo de estas técnicas, ya que crean reductos impenetrables.

BIBLIOGRAFÍA

- ALMAGRO NOSETE y otros, (1990) "*Derecho procesal. Parte general, proceso civil. Tomo I, volumen I*" Editorial Tirant lo Blanch, 5ª ed., Valencia.

- CARRASCOSA LÓPEZ, Valentín (1995) "*Valor probatorio del documento electrónico*" *Informática y Derecho* nº9, 10, 11 UNED Mérida.

- DARÍO BERGEL, Salvador (1995) "*Contratos informáticos en el Derecho Privado*" Informática y Derecho nº8 UNED Mérida.

- DAVARA RODRÍGUEZ, M. A. (1992-1993) "*La Ley Orgánica de Regulación del Tratamiento Automatizado de Datos de Carácter Personal*" Editorial Aranzadi. Encuentros sobre Informática y Derecho. Madrid.

- GALLARDO, M.A. (1993) "*Garantías criptológicas de las firmas electrónicas*". Actualidad Informática Aranzadi. Enero. Pp 5-6.

- GONZÁLEZ AGUILAR, A. y otros. (1991) "*El derecho de la prueba y la informática. Problemática y perspectivas*" Informática y Derecho nº1 UNED Mérida.

- HEREDERO HIGUERAS, M. (1996) "*La Ley Orgánica, 5/1992, de Regulación del Tratamiento Automatizado de Datos de Carácter Personal. Comentario y textos*" Editorial TECNOS. Madrid.

- MOLINA MATEOS, J.M. (1996) "*Libertad informática y criptología*" Informática y Derecho nº 12, 13, 14, 15 UNED Mérida.

- PÉREZ LUÑO, A.E. (1992) "*Del habeas corpus al* habeas *data*". Informática y Derecho nº1 UNED. Mérida.

- ROUANET MOSCARDÓ, J. (1992) "*Valor probatorio Procesal del documento electrónico*" Informática y Derecho nº1 UNED Mérida.

SANCHO RODRÍGUEZ, J. y MORANT RAMÓN, J.L. (1993) "*Garantías de la firma electrónica de contratos y autentificación de las partes*". Editorial Aranzadi. Encuentros sobre informática y derecho. Madrid.

Terminología inglesa más recurrente en el acceso y recuperación de la información en bases de datos bibliográficas

ALEJANDRO CURADO FUENTES

Profesor de lengua Inglesa. Universidad de Extremadura

La formación y clasificación de glosarios que versan sobre temas tanto del mundo de la Informática "física" como de la"lógica", dos términos empleados más comúnmente en inglés como **software y hardware**, reúnen como requisitos importantes una serie de aspectos puntuales que tienen que ver con cómo el análisis de los distintos vocablos y sintagmas puede contribuir a facilitar, que no dificultar, la labor del usuario, estudiante o simple aficionado de la Informática. En concreto, dicho cometido responde a la necesidad de definir, en muchos casos, previamente, el contexto informático en que se plantea y relaciona una terminología específica de la lengua inglesa de corte científico-técnico. Siguiendo un orden o clasificación, los autores agrupan los términos generalmente según se tomen distintos criterios de morfosintaxis y semántica en la medida adecuada y el entorno o contexto que interese. De este modo, la importancia del manejo y consulta de vocabularios específicos ajustados y actualizados, se muestra cada vez mayor en el terreno de las áreas técnicas, campos como es el caso de la Informática, que se abonan continuamente con productos anglosajones acuñados a una ratio muy elevada.

Un filósofo de la Lingüística, prof. Robert de Beaugrande, sobre la tipología del concepto y la palabra, se pronuncia de manera un tanto compleja,

mas en aras a clarificar la relación entre léxico y contexto, su discurso resulta bastante útil. En su análisis, en efecto, contenido y gramática, concepto y lexis, se relacionan entre sí dentro de la dinámica del texto.[7] La implicación de la unidad textual, de hecho, aparece con asiduidad en su trabajo, no sólo como elemento de enfoque y análisis, sino como nivel estructural e interactivo en que se consolidan los diversos apartados funcionales y nocionales del lenguaje. Sin adentrarnos demasiado en la profundidad de Beaugrande, sin embargo, para centrar el objeto de estudio que interesa, se desprende del trabajo mencionado la referencia al índice discursivo y la "correlación preferente entre el nivel gramatical y el conceptualista" (traducción mía).[8]

Mediante la conciencia del apartado léxico-gramatical, por tanto, se pone de relieve manifiesto la búsqueda del lenguaje específico, adecuado a un área concreta y ajustado a un fin de conocimiento detallado. Basta mencionar la cuantiosa y, en muchos casos, valiosa aportación de la crítica textual y lexicográfica en torno a la elaboración de vocabularios específicos de inglés científico-técnico[9] para proponer una referencia obligada a la hora de elaborar una disciplina o filosofía que fije con rigor el análisis de las entradas léxicas. Así, por tanto, no resultaría demasiado complicado recopilar y trasladar en una lista referencial aquellos elementos léxico-gramaticales que dentro de un contexto reflejan una posición semántica funcional determinada. Dicho de otro modo, y aplicándose lo dicho al caso que a continuación se elabora, la inclusión de los distintos términos responde a su función en contextos claramente definidos, y de cuya definición general parten otras muchas más concretas que no podrían prescindir de la global.[10] En nuestro ejemplo o modelo, se trata de dos contextos

■[7] BEAUGRANDE, R. Text, Discourse and Process. Norwood, NJ: ABLEX, 1993. Págs. 80-81.

■[8] Beaugrande, op. cit., pág. 88: "...that there be preferential correlations between the grammatical and the conceptual level".

■[9] Destacan, por citar una mínima representación crítica, las aportaciones de lingüistas y estudiosos como John Swales, Louis Trimble, Pauline Robinson, J.R. Cowan, M.A. Snow, J.C. Richards, etc.

■[10] Podría dicha distribución compararse con el relato meteorológico televisado después del telediario, donde se comenta en primera instancia cómo es el tiempo en rasgos generales por toda España para dedicar, a continuación, un comentario concreto sobre las características de cada región o zona.

claros: El acceso a la información automatizada y su recuperación posterior en una base de datos.

En el primer caso, sobresalen aquellos verbos y sustantivos que denotan el proceso de acceder a la información a través de las redes informáticas. Son ejemplos palabras como **browse** (examinar, navegar), **search** (buscar, búsqueda), **subject** (campo temático, área), **site** (emplazamiento, zona), **research** (investigar, investigación), **seek** (rastrear, localizar), **source** (fuente de información), **on-line** (en red, electrónico), **sample** (muestra, ejemplo), etc.[11] En el contexto de la recuperación informática destaca, de otro lado, una terminología clave que alude a dicha actividad: **retrieve** (recuperar), **save** (almacenar, guardar), **link** (enlazar, enlace), **display** (mostrar, visualizar), **fetch** (coger, traer), **add** (añadir), **sort** (resolver, clasificar), **tool** (herramienta)...[12]

Como se ve y podrá comprobarse si se consulta un diccionario general de inglés-español, la mayoría de los términos tienen, si no el mismo significado específico que el general, uno muy aproximado. De hecho, poseer un vocabulario de nivel intermedio en el idioma bastaría en gran medida para resolver el significado de muchos de estos vocablos. No apunta, en consecuencia, el estudio de las terminologías por contexto al mero cometido de traducir los términos. Como se ha dicho, es de interés analizar, a continuación, el grado contextual de cada forma, cuándo y cómo aparece, y qué referencia semántica especial contiene en cada caso.

La ordenación por bloques léxico-gramaticales relacionados entre sí de los vocablos, puede ser de gran utilidad a la hora de formar un compendio terminológico. En este sentido, cabría analizar, por ejemplo, la aparición del verbo **browse** y su relación con **subject** o **search**:

Search in **browser**

Open **file** in **browser**

■11 Véase la columna izquierda del apéndice A.

■12 Véase la columna derecha del apéndice A.

Subject browser

Pump up your **browser**!

Browsable menu

Se comprueba que la mayoría de las veces, según las bases de datos consultadas, aparece el sustantivo browser en lugar de browse.[13] Se desprende, por tanto, que cumple la función de "navegar, examinar" la base de datos; **browser** indica, además, en estos sintagmas, que permite la realización de una búsqueda o investigación así como que se creen ficheros.

La primera locución apuntada **search in browser** nos llevaría según esta clasificación de los sintagmas, a otro bloque semántico, el del término **search**. Su combinación con otros elementos es también variopinta como puede comprobarse:

Net/Web search

Search engine

Search sampler

Search for...

Search under...

Site search

El término puede presentarse como verbo o sustantivo, al igual que el anterior. Según los sintagmas apuntados, la acción de "buscar" o "búsqueda" parece contener un matiz especial relacionado con la identificación o localización de **items** documentales precisos. También podría añadirse el significado de "investigación" en este caso. Nótese que, empleado como verbo, aparece seguido

■[13] Deliberadamente, sólo he marcado en negritas aquellos vocablos de la lista. No he subrayado la "r" de browser tampoco para demarcar su diferenciación morfológica del verbo.

de las preposiciones **for** y **under** según se quiera indicar objeto de búsqueda y circunstancia respectivamente.

Algunos ejercicios y actividades que pudieran diseñarse en torno a este vocabulario son aquellos que persiguen la fluidez y familiaridad en su utilización en contexto. Se trata de un ejercicio de combinación y memoria para, de un lado, equiparar con el significado más escueto al vocablo en cuestión, y, de otro, entablar mentalmente la asociación de términos más habitual en sintagmas y locuciones.[14]

El estudio morfosintáctico del lenguaje especializado en lengua inglesa, por tanto, no supone solamente la revisión a grandes rasgos de los llamados campos científico-técnicos. La tarea de análisis conduce también a una inmersión en el adentro de la terminología recurrente de los medios tecnológicos más avanzados. Aunque pueda parecer redundante apuntar significados que ya conocemos, la creación de pequeños glosarios muy concretos posibilita la formación más exaustiva del usuario atendiendo al contexto en que opera y a la hora de utilizar y manejar la información en inglés de los medios.

■[14] Véase ejemplos de estos ejercicios en Apéndice B.

APENDICE A

BROWSE	RETRIEVE
SEARCH	SAVE
SUBJECT	FILE
SITE	RESOURCE
RESEARCH	DATA
SAMPLE	HANDLE
TOPIC	MANAGE
SERVER	TOOL
NET	DISPLAY
SEEK	ADD
ITEM	FETCH
SOURCE	PRINT
CLICK	LINK
WEB	BOOKMARK
FIND	HOMEPAGE
FIELD	VIEW
LOCATE	SHOW
KEY	LOAD
SCREEN	BOOT
ON-LINE	ENGINE
OFF-SITE	SORT OUT
SUMMARY	HOLD ON
TYPE	BACK UP
PRESS	RETURN

APENDICE B

1. Relacionar cada grupo de palabras con el significado más apropiado de **link**.

Web link	**I.** Enlazar, conectar, referir
Relationship **link**	
Forge **links** with...	
Upwards **link**.	**II.** Enlace, eslabón.
Linking device	
Added **link**s	**III.** Operador de relación.
Updated **links**	
Linking up	**IV.** Referencia a términos o descriptores bajo un mismo nivel jerárquico.

2.Rellenar las casillas con el término que mejor se ajuste de la columna izquierda.

SUBJECT
RESEARCH
SITE
SOURCE
ON-LINE
SORT OUT
RETRIEVAL
FILE
FETCH

_____ item from menu

_____ data

_____ name

_____data base

_____ arrangement

_____ findings

_____ on the net

Reference _____

Carry out a _____

_____ tool

_____ display

back _____

_____ journal

_____ sites

Store search in disk _____

Computerized Information _ system

La Directiva 95/46/CE como criterio unificador

JESUS MARIA PRIETO GUTIERREZ

Licenciado en Derecho

INTRODUCCION

El panorama existente con anterioridad a la aprobación de la "Directiva 95/46/CE, del Parlamento Europeo y del Consejo de Europa, 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 adelante, Directiva-, era de absoluta carencia de criterios comunes por parte de los Estados miembros en la materia, hasta el punto de existir algunos países, como Italia[1] y Grecia, los cuales, ni siquiera disponían de una normativa interna, todo lo cual repercutía, no solo en la falta de unanimidad de criterios a la hora de proteger la Intimidad de las personas físicas como bien de especial protección, sino

■[1] En la Gaceta Oficial de la República Italiana de 8 de enero de 1997, se publica la "Ley de 31 de diciembre de 1996, nº 675 "Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali". Así como la Ley de 31 diciembre 1996, n. 676 por la que "Delega al Governo in meteria di tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali", estableciendo el art. 45 de la Ley núm. 675 que la misma entrará en vigor a los veinte días de su publicación.

también, dificultando la transferencia de datos, no sólo a terceros países, sino entre los propios Estados miembros.

Por otra parte, la única norma internacional vinculante en materia de protección de datos personales -PDP-, era el "Convenio 108 del Consejo de Europa, de 28 de enero de 1981, para la protección de las personas con respecto al tratamiento de datos con carácter personal", hecho en Estrasburgo -en adelante, Convenio- el cual fue reconocido como el modelo a seguir por las legislaciones internas, contemplando un "núcleo irreductible" consistente en lograr un mínimo nivel equivalente de protección entre los Estados. Asimismo, marcó las bases de una nueva generación de normas de protección de datos -PD- en las legislaciones internas de los Estados miembros. No obstante y a pesar de resaltar estos aspectos positivos, con el transcurso del tiempo se comienza a plantear la insuficiencia de su contenido, dado el amplio margen de actuación que contempla para los Estados miembros y la tardanza de su incorporación al Derecho interno de éstos, así como la falta de concreción de su regulación, lo que unido al inimaginable desarrollo e incidencia que las "nuevas tecnologías", especialmente la informática, iban a tener en la materia, provoca el que se forme una conciencia generalizada, que pasa por la ineludible necesidad de elaborar una norma de ámbito comunitario que responda a los problemas surgidos en el marco del panorama que acabamos de esbozar.

Esta inquietante realidad se intenta solventar con la aprobación de la Directiva, la que apunta en tal sentido al contemplar en sus Considerandos 7 a 11, los Principios Básicos de regulación normativa, procurando evitar las diferencias que en materia de protección de datos personales puedan surgir entre los Estados miembros (Considerando 7), pretendiendo un tratamiento equivalente entre los mismos (Considerando 8), sin que ello conlleve una minoración de la protección (Considerando 10). Sin embargo, para conseguir tales objetivos, no se pretende establecer una regulación exhaustiva, de modo que se prive a los Estados miembros de arrogarse ciertas facultades, sino que por el contrario, la Norma comunitaria contempla un "margen de maniobra" (Considerando 9) a fin de que éstos puedan establecer sus propias excepciones, limitaciones o simplificaciones, que les permita una eficaz regulación acorde a sus peculiaridades internas.

Dado el corto rodaje de la Directiva y la ausencia de transposición de su contenido al Derecho interno de los Estados miembros, hasta el momento no existe la experiencia suficiente que nos permita corroborar si dicha norma responde a las expectativas que tanto legisladores como estudiosos del tema,

esperan de ella. No obstante y dado su contenido, surgen ya algunos interrogantes que pueden hacer dudar de su plena efectividad. En este sentido, cabe preguntarse, si el margen de maniobra atribuido a los Estados miembros es lo suficientemente amplio como para permitirles adaptar la Directiva a sus circunstancias internas, o si por el contrario, estas facultades son demasiado amplias y, en consecuencia, puede conllevar el que las regulaciones internas que surjan en aplicación de la Directiva, diverjan de tal manera, que deje vacía de contenido la pretensión comunitaria de adoptar la Directiva como criterio unificador de dichas legislaciones y, por tanto, sin que suponga un verdadero reforzamiento de la protección de los Derechos y Libertades de las personas físicas, frente al TDP que les conciernen.

2. ESTUDIO COMPARADO DIRECTIVA 95/46/CE - CONVENIO 108

Resulta conveniente el estudio de estas normas de carácter internacional, por ser las que han influido de forma decisiva en el ámbito de la Comunidad Europea en materia de protección de datos.

Partiendo de lo establecido en el Considerando 11 de la Directiva, por el que se pone de manifiesto el carácter más amplio y la precisión de los principios de protección de derechos y libertades de las personas, con relación a la regulación contemplada por el Convenio; encontramos el primer punto de apoyo al considerar la Directiva, como norma que nace ante la insuficiencia del Convenio.

Siguiendo a Martín-Casallo[2], éste afirma, que tanto si se atiende al campo de aplicación de ambas normas, como al contenido de sus disposiciones, no se encuentra coincidencia alguna en el contenido de ambos instrumentos, constatando, que en cuanto al ámbito de aplicación, el Convenio tiene un mayor campo de aplicación que la Directiva, por supeditarse la aplicación de ésta, al hecho de que las actividades del responsable del tratamiento de datos personales se desenvuelvan dentro del ámbito de aplicación del Derecho Comunitario

[2] MARTÍN-CASALLO LOPEZ, Juan José "Implicaciones de la Directiva sobre protección de datos en la normativa española" Actualidad Informática Aranzadi, núm.. 20, pág. 2, Madrid, julio de 1996.

(Considerando 12). En este sentido y en atención al principio de aplicabilidad directa de las normas comunitarias se atribuye a los Estados miembros la responsabilidad de aplicar la Directiva, mediante la norma que al efecto establezcan, incluso mediante el establecimiento de normas específicas para determinados sectores (Considerando 68), contemplando toda una serie de supuestos que puedan plantearse en cuanto al responsable del tratamiento de datos personales (Art. 4 D.C.), entendemos, que con la finalidad de evitar un conflicto de competencias entre los Estados, que les pudiera dejar inermes ante la actuación de los responsables del tratamiento, al escudarse éstos en la ubicación de su sede o el lugar de desarrollo de sus actividades, a fin de eludir la aplicación de la norma comunitaria.

La Norma Comunitaria, en cuanto a su ámbito de aplicación, introduce en su art. 3 la importante novedad de referirse tanto al tratamiento automatizado o no de DP destinados a ser incluidos en ficheros, sobre la base de lo cual, deja bien claro que lo realmente importante es el TDP, independientemente de que dicho tratamiento sea automatizado o manual. Al respecto, establece una serie de excepciones, a las que no son de aplicación la Directiva (art. 3.2.). En cuanto a la utilización de la expresión "ficheros" hay que resaltar la apreciación que hace López-Muñiz[3] en cuanto a la regulación establecida en la LORTAD, la cual exclusivamente hace referencia a ficheros, siendo que, desde el punto de vista técnico, hubiera sido más acertado haber empleado el término de base de datos, por ser más amplio. Apreciación que es extensible a la Directiva por utilizar, al igual que la LORTAD, exclusivamente el término de ficheros.

Por lo que respecta al Convenio, únicamente permite, con carácter general, excluir de su ámbito de aplicación aquellos ficheros que no estén sometidos a una legislación interna en matera de PD (art. 3.2.1.), dejando a las partes la posibilidad de regular los ficheros manuales (art. 3.2.c)), así como otras posibilidades contempladas dentro del amplio margen de actuación que permite a los Estados miembros.

Igualmente importante, por novedoso y por garantizar la figura de un sujeto al que le puedan ser atribuidas las responsabilidades que en su caso se

■[3] LÓPEZ-MUÑIZ GOÑI, Miguel "La Ley de Tratamiento Automatizado de los Datos de Carácter Personal" en Informática y Derecho, núm. 6-7, pág. 98, UNED Mérida 1994.

deriven del TDP, es la medida establecida en su art. 4, por el que se determina en cada supuesto, cuál sea el Derecho nacional aplicable, atendiendo para ello, al responsable del tratamiento o representante en el que éste delegue. El Convenio, en este sentido, no contiene regulación alguna.

Dentro del ámbito de aplicación de la Directiva, se recoge, lo que para muchos autores, como Rafael Velázquez[4], era imprescindible regular dada su incidencia en nuestro tiempo, nos estamos refiriendo al sonido y la imagen como datos relativos a las personas físicas, sobre los que pueda incidir cualquier manipulación (Considerando 14), si bien, hay que tener en cuenta, la limitación introducida por el Considerando 15, al limitar su aplicación a los supuestos en que el tratamiento sea automatizado o se encuentre en un archivo estructurado, o destinado a tal fin. Por otra parte, dichos datos no se entenderán incluidos dentro del campo de aplicación de la Directiva, cuando éstos se obtengan como consecuencia de la grabación por cámaras de vídeo, a fin de garantizar la seguridad pública, la del Estado o su defensa, así como a actividades relacionadas dentro del ámbito del derecho penal (Considerando 16). También se contempla una restricción en el Considerando 17 cuando dichos datos sean aplicados con fines periodísticos, lo que obedece a la pretensión comunitaria, de conciliar el derecho a la intimidad con la libertad de expresión (art. 9).

Cabe resaltar en este sentido, las reflexiones de Martín Casallo[5], por la gran trascendencia que reconoce a esta innovación introducida por la Directiva, al expresar:

"El reconocimiento de la voz y el sonido como datos personales efectuado por la Directiva, va a potenciar los mismos en aras a la salvaguardia de la intimidad personal (...) lo que necesariamente supone dar plena eficacia al principio del dominio permanente establecido en favor de la persona a la que afectan las informaciones y a la necesidad del cumplimiento de la denominada obligación de seguridad"

■[4] VELAZQUEZ BAUTISTA, Rafael "Protección Jurídica de Datos Personales Automatizados" pág. 217 Conclusiones, Ed. COLEX, Madrid 1993.

■[5] MARTIN CASALLO-LOPEZ, Juan José "Implicaciones sobre la Directiva ..." ob. cit. pág. 6

Por lo que respecta a los llamados "datos sensibles" ambas normas, establecen una regulación similar, si bien no coinciden en su contenido, pues mientras la Directiva se refiere a los que revelen el origen racial o étnico, las opiniones políticas, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, así como los relativos a la salud o vida sexual. El Convenio establece la misma regulación, si bien omitiendo la referencia a los sindicatos y añadiendo lo relativo a condenas penales. También coinciden en establecer la imposibilidad de tratar dichos datos, salvo por las excepciones que se contemplan al respecto, remitiéndose el Convenio a las excepciones que puedan establecer los Estados miembros siempre que se contemplen las medidas adecuadas, a las que también se refiere la Directiva, si bien, añadiendo "por motivos de interés público" lo que no deja de ser una remisión en blanco. La Directiva contempla una amplia casuística de excepciones al principio general de prohibición.

Por lo que al objeto de protección se refiere, partiendo de lo establecido en el Art. 1 del Convenio 108, se habla de Derechos y Libertades Fundamentales de las personas físicas, haciendo hincapié en el término de privacidad, al señalar de forma expresa "...concretamente su derecho a la vida privada". Término que según señala Marchena Gómez.[6]

"La superación de una visión de la intimidad centrada en la esfera personal resulta inevitable ante la constatación de un fenómeno en expansión de la privacy, que se traduce en una idea de privacy política, que reclama desde un significado garantista, la protección de otros bienes jurídicos, respecto de los cuales la garantía de privacy constituye una garantía de ejercicio efectivo"

Dicho término, ha dado lugar a no pocas interpretaciones doctrinales, considerándose por muchos, que el mismo es atribuible a la obra de Warren S. y Brandeis R "The right to Privacy" con la intención de esbozar el derecho de estar sólo (To be let alone). Pero no todos los autores comparten la oportunidad de diferenciar entre intimidad y privacidad, entre otras razones, como señala López-Muñiz[7] porque "muchos datos personales pueden tener el carácter de íntimos

■[6] MARCHENA GOMEZ, Manuel "Intimidad Informática: La Protección Jurisdiccional del Habeas Data" Boletín Informativo del Ministerio de Justicia, núm. 1768, págs. 9 y 10 Madrid 1996.

■[7] LÓPEZ-MUÑIZ GOÑI, Miguel "La Ley de Tratamiento Automatizado..." ob. cit. pág. 100.

para unas personas y carecer de tal para otras". Por ello entendemos que todos los derechos y libertades de las personas físicas pueden ser objeto de protección frente al tratamiento de datos personales. En este sentido, la Directiva, también en su Art. 1, se refiere a las Libertades y Derechos Fundamentales de las Personas Físicas, pero a diferencia del Convenio, incide en el derecho a la intimidad.

En otro orden de cosas, para la Directiva no se considera incompatible el tratamiento posterior con los fines determinados, siempre que se utilicen con fines históricos, estadísticos o científicos y se establezcan las garantías adecuadas. El Convenio no se pronuncia al respecto.

Como particularidad introducida al regular el Derecho de Acceso, si bien con un margen de efectividad muy limitado, se contempla la posibilidad del Bloqueo de los datos, con la obligación de notificar el haber practicado tal actividad conforme a lo solicitado por el interesado, con una salvedad, que ello no resulte imposible o suponga un esfuerzo desproporcionado. El Convenio se limita a hacer referencia tácitamente al derecho de acceso y expresamente al de rectificación y borrado.

La Sec. 7ª de la Directiva contempla el Derecho de Oposición del interesado, novedad que no es recogida por el Convenio, si bien la efectividad de tal derecho queda limitada a unos cuantos supuestos muy concretos. A su vez dentro de este derecho introduce un término nuevo de "la prospección" para el cual se establece una regulación del derecho de oposición con importantes garantías.

En cuanto al tratamiento, cada normativa establece una regulación diferente, en este sentido, el Convenio no establece distinción alguna en las medidas de seguridad aplicables al tratamiento automatizado de datos personales (TADP). En cuanto a la Directiva comunitaria, además de contemplar el reforzamiento del tratamiento de los datos especialmente protegidos, introduce una novedad, al hacerlo extensivo a la transmisión de datos dentro de una red. Para Martín Casallo[8], esta diferente regulación obedece al tiempo en que cada

[8] MARTÍN-CASALLO LOPEZ, Juan José "Discurso Apertura" de la Conferencia sobre Seguridad, Privacidad y Protección de datos, celebrada en Madrid del 30 nov. al 1 dic., pág. 8, Agencia de Protección de Datos.

norma ha sido aprobada.

La Directiva en su Sec. 9ª, bajo el epígrafe "Notificación" viene a establecer con carácter general la necesidad previa de notificar a la Autoridad de Control la intención de realizar un tratamiento de datos personales, atribuyendo al responsable del tratamiento o, en su caso, al representante, la responsabilidad de cumplir con tal obligación. También dentro de la Sec. 9ª, en su art. 21, la Directiva alude a la Publicidad de los tratamientos, atribuyendo a los Estados miembros la obligación de velar por su cumplimiento, así como de cuidar por que la autoridad de control lleve un Registro en el que se inscriban las notificaciones que se vayan realizando y en consecuencia facilitar la consulta por cualquier persona que tenga interés. Respecto a estas obligaciones de notificación y publicidad a que se refiere la Directiva, el Convenio 108 guarda absoluto hermetismo.

En cuanto a los recursos, la Directiva en el art. 22, hace referencia a dos clases de recursos, los contemplados en vía administrativa y los relativos a la vía judicial, dejando libertad a los Estados para aplicar lo relativo a este tema y en concreto para determinar el procedimiento a sancionar. Asimismo contempla la reparación del perjuicio sufrido por el interesado atribuyendo tal responsabilidad al responsable del tratamiento, salvo que justifique que la causa del perjuicio es ajena a su actividad. El Convenio 108, alude a la necesidad de establecer recursos y sanciones, pero sin que especifique los mismos, remitiéndose a los Estados miembros para su regulación cuando vulneren las disposiciones de derecho interno.

La Directiva comunitaria en cuanto al "flujo transfronterizo de datos" establece una regulación bipartita, según se refiera la transferencia a la realizada entre los propios Estados miembros (Considerandos 3 a 9) o a terceros países (Arts. 25 y 26) atendiendo, en el primer supuesto, a un nivel de protección equiparable, que evite la obstaculización de la libre circulación entre los Estados miembros y, en cuanto a terceros países, se tiene en cuenta el nivel de protección adecuado de estos, estableciendo para su determinación un conjunto de consideraciones y atribuyendo a la Comisión su valoración, en colaboración con los Estados miembros (Art. 25 D.C.). La regulación contemplada por el Convenio es muy pobre, estableciendo como regla general la imposibilidad de oposición entre los Estados partes.

En cuanto a las excepciones a los principios en materia de transferencia

de datos, en que se basa cada norma, la Directiva establece una regulación muy permisiva, hasta el punto de contemplar la posibilidad de prescindir de las excepciones a que se refiere el art. 26.1 de la misma, cuando el responsable del tratamiento establezca las garantías suficientes, con la única condición, de que se informe a la Comisión y a los demás Estados miembros. Las excepciones enunciadas en el Convenio se centran en los supuestos para los que no se contemple una regulación equivalente entre los Estados miembros, o que la transferencia se lleve a cabo por el territorio de otra parte, con destino a un Estado no contratante.

La Directiva dedica una amplia regulación a los llamados Códigos de Conducta al referirse a los mismos tanto el Art. 27, como el Considerando 61, definiéndolos como acuerdos establecidos por las asociaciones profesionales y demás organizaciones representantes de responsables de tratamiento, para la correcta aplicación de las disposiciones nacionales adoptadas por los Estados miembros en aplicación de la presente Directiva. Dichos Códigos pueden ser sometidos a examen del Grupo de protección, sin que exista obligación de su registro. El Convenio guarda silencio al respecto.

Asimismo, el Convenio no establece regulación alguna respecto a otro órgano, la Autoridad de control, al que la Directiva comunitaria considera como un elemento esencial a contemplar por cada Estado miembro, haciendo hincapié en la necesidad de su independencia en el ejercicio de sus funciones, a fin de garantizar la protección de las personas en materia de tratamiento de datos personales, mediante el ejercicio de las labores de investigación e intervención y, procurando en todo momento, la transparencia del tratamiento y la ayuda mutua entre los Estados miembros (Considerandos 62 al 64 D.C.).

Otro órgano de gran importancia contemplado en la Directiva es el Grupo de protección, el cual, de responder a las expectativas depositadas en él por la regulación establecida en la norma comunitaria, estaría destinado a ser el gran catalizador entre los Estados miembros de la C.E., tal como esboza el Considerando 65 de la Directiva, al considerar, que actuará con total independencia, a fin de asesorar a la Comisión y contribuir a la importante misión, de la aplicación uniforme de las normas nacionales adoptadas en aplicación de la Directiva y contribuir a la aplicación homogénea de la Directiva, evitando diferencias entre los Estados miembros. El Convenio, hace referencia al Comité consultivo, en unos términos similares al papel atribuido al Grupo de protección creado por la Directiva, si bien, con unas funciones no tan determinadas.

Por último la Directiva se refiere al Comité como órgano encargado de asistir a la Comisión en su función de ejecución de las medidas que en cada caso hayan de adoptarse. El Comité, formado por representantes de los Estados miembros y presidido por el representante de la Comisión, deberá pronunciarse sobre los proyectos de dichas medidas, mediante la emisión de un dictamen. Para el caso de que dichas medidas sean aplicadas en sentido contrario a lo establecido en el dictamen, se contempla la particularidad, en el Art. 31, único en este Capítulo, de que entren en juego tres órganos comunitarios, los dos ya citados, y el Consejo, que será el órgano encargado de dirimir la cuestión. El Convenio por el contrario no hace referencia alguna a este órgano.

3. LA DIRECTIVA 95/46/CE

3.0. INTRODUCCION

Como ya hemos tenido ocasión de exponer, los Principios Básicos de la Directiva aparecen contemplados en los Considerandos 7 a 11, los cuales hacen referencia a aspectos que, hasta el momento, constituían el caballo de batalla entre los Estados miembros de CE en materia de PD, dada la disparidad de criterios como consecuencia de la insuficiencia del Convenio 108 como única norma de carácter internacional, que si bien había sido ratificado por todos los Estados de la CE, sin embargo, dada la nueva realidad planteada con las nuevas tecnologías y la falta de concreción de conceptos, resultaba insuficiente, para lograr unos criterios de unidad entre los Estados ratificantes del Convenio en materia de PD.

La Directiva en principio nace con la vocación de unificar los Derechos internos de los Estados miembros, contemplando al efecto unos Principios básicos y dejando a los Estados un margen de maniobra para concretarlos en sus respectivas legislaciones, procurando en todo caso, que ello redunde en un reforzamiento de la protección de las personas físicas frente al TDP y evitando de este modo, que puedan ser alegados criterios de disparidad por los Estados miembros en materia de transferencia de DP entre los mismos y, ello, a pesar de que el legislador comunitario es consciente, de que el margen de maniobra atribuido a los Estados, puede ser motivo de disparidad en la aplicación de la Directiva (Considerando 9).

3.1. OBJETIVOS

Visto lo que resulta el estudio comparado realizado en el apartado anterior entre el Convenio 108 y la Directiva 95/46/CE y en congruencia con el conjunto de los Principios Básicos contemplados en los Considerandos 7 a 11 de la Directiva, a los que ya hemos tenido oportunidad de referirnos[9]. Por una parte y con carácter general, resulta evidente, que la regulación establecida en la Directiva responde al objetivo de cumplir con uno de sus principios básicos contemplado en el Considerando 11, pues la norma comunitaria precisa y amplía lo establecido en el Convenio. Por otra parte y limitándonos a lo establecido en el Considerando núm. 9, cuyo contenido hace referencia a "que los Estados miembros dispondrán de un margen de maniobra(...)dirigido a mejorar la protección que proporciona su legislación en la actualidad", es obvio la doble finalidad de dicho considerando, con el que se pretende, de una parte, dejar un margen a los Estados para que, dentro del marco determinado por la Directiva, estos dispongan de la suficiente autonomía a fin de adaptar dicha norma, en la medida que les sea posible, a sus peculiaridades internas. Por otra parte, procurando que dicha potestad se ejerza de forma que suponga una mejora de la legislación hasta el momento existente, con objeto de establecer un mayor grado de protección de las personas físicas frente al TDP.

Para nivelar la relación existente entre las dos pretensiones señaladas, resulta imprescindible que, a su vez, la Directiva arbitre las garantías necesarias a fin de evitar el conflicto entre ambas y, en consecuencia, impedir que prevalezca una con el consiguiente menoscabo de la otra. Es decir, se trata de lograr un tratamiento equivalente entre los Estados miembros (Considerando 8), para evitar que surjan diferencias entre los mismos (Considerando 7). En este sentido cabe señalar como garantías fundamentales introducidas por la regulación establecida en la Directiva, amén de otras que resultaría prolijo relacionar, la que se sustenta básicamente en los Organos contemplados en la Directiva, los cuales, grosso modo, por un lado tienen la finalidad de llevar a buen fin la protección de las personas físicas en materia de TDP y, por otro, la de velar por una aplicación homogénea entre los Estados miembros evitando que surjan diferencias entre los mismos. También constituye una garantía de gran importancia, la de atribuir al

[9] Vid pág. 3 en el Capítulo 1. Introducción.

Responsable del Tratamiento o, en su caso, el Representante en que éste delegue, la responsabilidad que en cada supuesto pueda derivarse del tratamiento de datos personales.

3.2. PRINCIPIOS BASICOS DE PROTECCION DE DATOS Y DERECHOS

3.2.0. Introducción

El Convenio bajo los epígrafes "calidad de los datos" y "Garantías" viene a establecer de forma escueta el modelo básico, el cual, en términos generales, es seguido y ampliado por las legislaciones europeas, siguiendo también esta línea la Directiva, con la denominación de Principios y Derechos, a los que, con cierta ironía, se les podía haber añadido "y sus excepciones", pues como luego analizaremos, son tal el número de las mismas en ambas normas, que hacen peligrar su efectividad, por lo que los Principios, que se constituyen como garantes para hacer valer los Derechos reconocidos a toda persona física, pueden resultar insuficientes si quedan anulados por las excepciones, motivo por el cual, la LORTAD está afecta de cuatro Recursos de Inconstitucionalidad aún pendientes de resolver y a los que la Directiva puede venir a dar respuesta.

Como decíamos, en cuanto a la calidad de los datos, el art. 5 del Convenio 108 los relaciona de forma escueta en los siguientes: que sean obtenidos y tratados leal y legítimamente, registrados con finalidades determinadas y legítimas, sin que puedan utilizarse de una forma incompatible con dichas finalidades; serán adecuados, pertinentes y no excesivos; exactos y puestos al día; conservados de forma que sea identificable la persona concernida... por un tiempo determinado que no exceda de las finalidades para las que fueron obtenidos.

Por lo que respecta a las Garantías, pues el Convenio no habla de Derechos, su art. 8 las relaciona también telegráficamente, al establecer que cualquier persona deberá poder conocer la existencia de un fichero automatizado de datos de carácter personal, sus finalidades y la identidad y residencia habitual de la autoridad controladora; obtener la confirmación de la existencia o no de un fichero automatizado de datos de carácter personal que concierna a dicha persona, su comunicación de forma inteligible, el derecho de rectificación o el borrado... y, por último, la posibilidad de hacer uso de un Recurso, para el caso de que no se hubiera atendido a las peticiones anteriores.

Sin embargo, estos Principios Básicos que para la protección de datos contempla el Convenio bajo la denominación "Calidad de los Datos y Garantías", quedan a voluntad de cada parte, mediante la regulación que al respecto establezca en su derecho interno, queriendo suavizar tal prerrogativa de los Estados, fijando una fecha tope para su regulación (Art. 4). Para más abundamiento, en su Art. 9, a pesar de comenzar prohibiendo cualquier excepción al respecto, establece la posibilidad de una excepción tan amplia como vaga, al referirse en su apartado 2º, a la posibilidad de establecer excepciones por las partes a la Calidad y Garantías (Principios y Derechos) de los datos, con la formula "cuando tal excepción(...) constituya una medida necesaria en una sociedad democrática", amén de otras excepciones que en términos generales coinciden con las establecidas en la Directiva y la LORTAD.

La Directiva al regular los Principios básicos de protección de datos y Derechos, a diferencia de la regulación establecida en el Convenio, donde los Principios y Derechos se recogen de forma separada, en la Directiva aparecen contemplados bajo el epígrafe "Condiciones Generales para la licitud del tratamiento de datos personales", limitándose a establecer el marco dentro del cual los Estados miembros precisarán las condiciones de licitud. (Art. 5 DC). Dicho marco viene determinado por la distinción que al respecto establece la Directiva entre Principios relativos a la calidad de datos (Sec. 1ª), los relativos a la legitimación del tratamiento de los mismos(Sec. 2ª) y los que da en llamar, Categorías Especiales de tratamiento (Sec. 3ª), que no son otra cosa que los "datos sensibles" a que se refiere el Convenio 108, siguiendo la regulación con el principio de Información del Interesado (Sec .4ª) dentro de la cual, cabe distinguir, entre los datos recabados del propio interesado y los que no lo han sido. Seguidamente y sin sucesión de continuidad, establece la regulación de los Derechos, haciendo referencia al Derecho de Acceso (Sec. 5ª), Excepciones y Limitaciones (Sec. 6ª), Derecho de Oposición (Sec. 7ª), Confidencialidad y Seguridad del Tratamiento(Sec. 8ª) y por último Notificación (Sec. 9ª). Regulación que en un principio no parece estar estructurada de forma clara, pues no se comprende el motivo por el que iniciada la regulación de los Derechos en la Sección Quinta, esta repentinamente se ve interrumpida en la Sección Sexta, para contemplar las excepciones y limitaciones a los Principios y Derechos sin haber finalizado de relacionar estos.

3.2.1. Principios relativos a la calidad de los datos

Como ya he tenido oportunidad de señalar, cabe resaltar la novedad

introducida por la Directiva en su Art. 6, con relación al Convenio, al atribuir a los responsables del tratamiento la obligación de garantizar el cumplimiento de los principios generales reconocidos en toda norma de protección de datos, es decir, tratamiento lícito y leal, recogida de datos con fines determinados, explícitos y legítimos y que con relación a estos fines los datos sean adecuados, pertinentes y no excesivos, así como exactos y conservados por un periodo no superior al necesario.

Parece deducirse, a nuestro modo de ver, que en cuanto al mantenimiento de la exactitud de los datos, en la Directiva no sólo se considera la posibilidad de que se establezca de oficio, como expresamente establece la LORTAD en su Art. 4.4, sino que por el contrario, cualquier interesado puede instar su actualización. De cualquier manera, la LORTAD igualmente viene a reconocer tal posibilidad a los afectados, si bien dentro de la regulación que al efecto establece, al contemplar los derechos de los interesados, pudiendo instar éstos su rectificación (Art. 15 LORTAD).

En otro orden de cosas, para la Directiva no se considera incompatible el tratamiento posterior con los fines determinados, siempre que se utilicen con fines históricos, estadísticos o científicos y se establezcan las garantías adecuadas. En este sentido, la LORTAD únicamente se refiere a los utilizados con fines históricos por lo que se hace necesario su ampliación a los otros dos supuestos. Surge la duda de los fines mencionados, distintos a los determinados inicialmente, constituyen una relación estanca, siendo los únicos admisibles o, si por el contrario, cabe entender que cualquier otro fin compatible con los fines determinados inicialmente es admisible.

3.2.2. Legitimación del Tratamiento

La Directiva, en el Art. 7, viene a establecer el principio general del consentimiento del interesado de forma "inequívoca", si bien y según se deduce del tenor literal del artículo, parece dejar vía abierta a la posibilidad del consentimiento tácito. Sin embargo, lo realmente chocante, es el modo de establecer excepciones a tal principio, ya que no llega a utilizar tal expresión, sino la conjunción disyuntiva "o", seguida de la frase, "cuando sea necesario para..." y haciendo uso de conceptos jurídicos indeterminados, tales como "interés vital", "misión de interés público", "interés legítimo perseguido", conceptos estos, que habrán de ser concretados en cada caso por la Autoridad de Control, y sin que todo ello beneficie en modo alguno a los interesados, pues se les priva de la

garantía de saber a priori, qué limitaciones son las que se contemplan con la utilización de tales términos, los cuales, en realidad no son otra cosa, sino excepciones al principio general del consentimiento.

3.2.3. Categorías especiales de datos

Bajo este epígrafe se recogen los denominados "datos sensibles" regulados en la Sec. 3ª, Art. 8 DC., reconociendo como tales, el origen racial, étnico, las opiniones políticas, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, así como los datos relativos a la salud o la sexualidad. Esta relación amplía las anteriormente contempladas por el Convenio y la LORTAD, aunque no recoja los datos relativos a la religión y creencias a que se refiere esta última en su art. 7, sobre la base de lo establecido en el art. 16 C.E.

La Directiva, por otro lado, establece la particularidad de prohibir el tratamiento de los mismos, aunque posteriormente, flexibiliza tanto tal prohibición, que acaba convirtiéndola en la excepción, pues la misma queda desvirtuada cuando se obtiene el consentimiento explícito del interesado, atribuyendo a este respecto, una potestad a los Estados miembros, de impedir el levantamiento de tal prohibición, aunque se cuente con dicho consentimiento. Asimismo queda sin contenido, cuando se plantean supuestos como los ya calificados de conceptos jurídicos indeterminados, tal como el "interés vital" o recurriendo a ambigüedades como "cuando haya que respetar las obligaciones y derechos(...)del responsable del tratamiento en materia laboral".

No obstante, entendemos que lo realmente peligroso dentro de estas excepciones a la prohibición inicialmente establecida, es lo relativo a las fundaciones y asociaciones de determinado carácter sin fin lucrativo, a las que conforme al Art. 18.4 de la DC, se les puede eximir de la obligación de notificar a la Autoridad de Control o simplificar la misma, lo que, a nuestro modo de ver, puede dar lugar a facilitar la actividad de las sectas que se amparen en alguna de la finalidades mencionadas en el Art. 8.2.d) DC.

Siguiendo con los supuestos que escapan a la prohibición del tratamiento de datos sensibles, el apartado 3º del mismo artículo, establece una excepción a la necesidad del consentimiento del interesado en cuanto a temas médicos, si bien estableciendo ciertas garantías que vienen a justificarla.

De excesivo se puede calificar el margen permitido a los Estados

miembros por la Directiva, al permitirles que amparados en "motivos de interés público importantes", lo que no es más que una remisión en blanco, puedan establecer otras excepciones a las ya contempladas para el tratamiento de datos sensibles, eso sí, siempre que dispongan las garantías necesarias, las cuales no llega a especificar, y sean notificadas a la Comisión, pero sin determinar si ésta en su caso puede oponerse a las mismas, con lo que en definitiva viene a intentar suavizar esta prerrogativa de los Estados, consciente de que tal vez pueda ser un margen demasiado excesivo. Tampoco supone ninguna garantía el que dichas excepciones puedan establecerse mediante la legislación interna del Estado o por decisión de la Autoridad de Control, ya que en ambos casos estarán determinadas por influencias políticas, pues no conviene olvidar, que en nuestro país el Director de la APD es nombrado por el Gobierno (Art. 35.1 LORTAD).

Los registros de condenas penales, medidas de seguridad e infracciones, habrán de ser llevados bajo el control de los poderes públicos, así como las sanciones administrativas o procesos civiles. En la Lortad los datos relativos a dichas materias aparecen excluidas del ámbito de aplicación de la misma, aunque para el caso de que se hubieran incluido, a buen seguro que se hubiera hecho dentro de la regulación establecida para los Ficheros de titularidad pública, por lo que, en tal caso, cabría hablar del control de los poderes públicos respecto de dichos registros, en el sentido de que, tanto la titularidad, como su gestión, sería atribuida a dichas autoridades. Sin embargo, es ineludible preguntarse, qué quiere decir la Directiva, cuando emplea la expresión, "bajo el control ". A este respecto, cabe varías interpretaciones, por un lado, que los datos estén incluídos en ficheros de titularidad privada y que a la Administración le corresponda establecer las medidas de control; en otro sentido, que estos datos sean tratados en ficheros de titularidad pública y por lo tanto gestionados y controlados directamente por la Administración, o bien, que independientemente de que sean tratados en ficheros públicos o privados, lo cierto es que el control estaría atribuido en todo caso a los poderes públicos. La consecuencia más importante de este planteamiento, es que tácitamente estaría distinguiendo entre ficheros públicos y privados, lo que vendría a avalar la tesis, de que la Directiva no se opone a la existencia de tal distinción, sino que incluso la contempla indirectamente.

Dos novedades más introduce la Directiva, de una parte, el atribuir a los Estados miembros la potestad de establecer las condiciones de regulación en cuanto a los documentos de identificación, lo que significa que pueden ser objeto de tratamiento y por lo tanto sin que la Directiva se oponga a su existencia (Art. 8.7 DC). En este sentido y siguiendo la regulación que al respecto establece la

Constitución Portuguesa de 1976, en la que se prohibe expresamente la posibilidad de identificar a sus ciudadanos por un número de identificación documentado, conforme a lo establecido en la Directiva, sus legisladores se verán obligados a reformar la Constitución al objeto de levantar tal prohibición, independientemente de que se llegara a identificar a sus ciudadanos con dicho documento, pues tampoco se deduce del tenor literal de la Directiva, que sea obligatoria la existencia del mismo.

Por otra parte y también como novedad en una norma sobre protección de datos, contempla la Directiva, la posibilidad de establecer excepciones y exenciones en cuanto al tratamiento de datos personales con fines periodísticos, artísticos o literarios, a fin de conciliar el derecho a la intimidad con las normas que rigen la libertad de expresión (Art.9 DC). También se contempla una restricción en cuanto a los datos referentes al sonido e imagen (Considerando 17) cuando dichos datos sean aplicados con fines periodísticos, lo que obedece a esta misma pretensión comunitaria.

3.2.4. Principio de Información del interesado

Contemplado en la Sec. 4ª del Cap. II, se establece la distinción, entre los datos recabados del propio interesado y cuando éstos no lo han sido, sin que entre ambas regulaciones se establezcan grandes diferencias, atribuyendo al responsable del tratamiento o a su representante, la obligación de informar al interesado, salvo que ya hubiera sido informado, en el primer supuesto, en el momento de recabar los datos y en el segundo, en el momento del registro o de la primera comunicación a un tercero. Tal información consiste en poner en conocimiento del interesado una serie de aspectos que le garanticen la posibilidad de saber la finalidad que tiene la recogida de los datos que le son solicitados, quien sea el responsable del tratamiento de los mismos y, en definitiva, saber de la existencia de un fichero, en el que sus datos van a ser tratados y los derechos que puede ejercitar frente a ese tratamiento si a su derecho interesa.

Para este Principio, como viene siendo la regla general, también se contemplan algunas excepciones (Art. 11.2 DC), en concreto y con cierta justificación, cuando el tratamiento se realice con fines estadísticos o de investigación histórica o científica. Sin embargo, no se pueda predicarse lo mismo cuando añade "o resulte imposible o exija esfuerzos desproporcionados", ya que puede servir en cualquier caso de excusa para eludir la obligación de informar al interesado dada la dificultad de demostrar lo contrario. También se excepcionan,

cuando el registro o la comunicación a tercero esté expresamente prescrito por la ley, y como suele ser lo habitual, con la obligación de establecer las garantías apropiadas, las cuales tampoco en este caso llega a especificar.

Resultaría incongruente, salvo para el caso en que se haya hecho uso de las excepciones mencionadas, contemplar la posibilidad de que el interesado no esté informado, pues es un deber, que como ya hemos dicho, atañe en todo caso al responsable del tratamiento o a su representante.

Llama poderosamente la atención, en cuanto a las excepciones mencionadas, el que las mismas se recogen exclusivamente para el supuesto en que los datos no se hayan recabado directamente del interesado, ya que en realidad, precisamente por no haber sido informado en el momento de la recogida de los datos, es lo que debería justificar, el que la Directiva hubiera puesto mayor empeño en que la información se hiciera efectiva en estos supuestos.

En este sentido, si como dice Martín-Casallo[10], la distinción entre ficheros que establece la Directiva, es en función de que los datos sean recabados del propio interesado o de los obtenidos de forma distinta, sin que por otro lado, la Directiva haga referencia a la distinción entre ficheros de titularidad pública y los de titularidad privada, pero sin oponerse expresamente a tal distinción siempre que ello no conlleve una minoración de los derechos del interesado. Conforme a esta argumentación, cuya base emana de la propia Directiva, nos encontramos con que en la distinción recogida en la misma, se establecen unas excepciones que afectan sólo a los ficheros cuyos datos no son recabados directamente del interesado, por lo que en atención al razonamiento esgrimido por dicho autor para entender derogado el Art. 19.1 de la LORTAD, habría que predicar lo mismo de la distinción establecida por la norma comunitaria y, por lo tanto, dado que la excepción contemplada en el Art. 11.2 de la Directiva, provoca una minoración de los derechos del interesado en contraposición con los supuestos del Art. 10 de la misma norma, habría que considerar la revisión del Art. 11 o, en su caso, hacer extensible las excepciones contempladas en el mismo al Art. 10.

■[10] MARTIN CASALLO-LOPEZ, Juan José "Implicaciones sobre la Directiva..." Ob. Cit. pág. 6

3.2.5. Derecho de acceso

La Directiva inicia la regulación de los Derechos en la Sec. 5ª con el Derecho de Acceso, ampliando con más detalle lo recogido en el Convenio y en la LORTAD, y siendo a su vez menos restrictiva que estas, en el sentido de que, al contrario de lo contemplado en la LO, no establece limitaciones en cuanto a su ejercicio, aunque haga referencia a una "periodicidad razonable", pero sin que se concrete en un periodo de tiempo determinado. No se priva de incluir un concepto técnico al referirse al conocimiento de "la lógica utilizada" en los tratamientos automatizados.

Como particularidad introducida al regular el Derecho de Acceso, se contempla, lo que en la LORTAD aparece regulado de forma independiente como Derecho de Rectificación y Cancelación (Art.15), añadiendo además la posibilidad del Bloqueo de los datos y contemplando la obligación de notificar el haber practicado tales actividades conforme a lo solicitado por el interesado, con una salvedad, que ello no resulte imposible o suponga un esfuerzo desproporcionado, con lo cual, queda en manos del responsable el practicar efectivamente la notificación, ya que siempre podrá escudarse en la dispensa mencionada, para eludir tal obligación.

3.2.6. Excepciones y Limitaciones

Como esbozábamos al comentar la estructura establecida en la Directiva, al determinar los Principios y Derechos de protección de datos personales, nos encontramos con que, seguidamente a la regulación del Derecho de Acceso, se contemplan, en la Sec. 6ª, las Excepciones y Limitaciones, particularidad que nos llamaba la atención, por no hallar un argumento que justificase plenamente tal proceder, pues parece que lo más oportuno hubiera sido finalizar la relación de Derechos y a posteriori establecer las excepciones. Tal vez pueda encontrarse cierta justificación en el hecho de que dichas excepciones y limitaciones se refieran en gran parte a determinados Principios y Derechos ya relacionados con anterioridad a éstas, pues tal referencia se centra en los recogidos en el Art. 6.1 (Calidad de los datos), Art. 10 (Información...datos recabados del propio interesado), Art. 11.1 (Información de datos recabados de forma distinta), Art. 12 (Derecho de Acceso) resultando, que el único no enunciado hasta el momento, es el contemplado en el Art. 21, referido a la Publicidad de los tratamientos.

Entendemos, que con tales medidas se trata de salvaguardar una serie de intereses, tanto de carácter general, como particular, justificando las relativas a la Seguridad del Estado, la Defensa y la Seguridad Pública, en cuanto son intereses generales que deben prevalecer por encima de los particulares en beneficio del conjunto de la Comunidad. Sin embargo, no compartimos tal justificación, al privar al interesado de unos derechos y de unas garantías con relación al tratamiento de sus datos personales, los que pueden afectar, entre otros Derechos, a su propia Intimidad, frente a unos intereses que afectan a infracciones penales o deontológicas, intereses económicos o financieros "importantes" o a funciones de control, inspecciones o reglamentarias relacionadas con las anteriores. Intereses estos, que habría que examinar caso por caso, a fin de determinar si realmente han de prevalecer por encima del Derecho del interesado o no.

También es excepcional, a fin de garantizar la protección del interesado o de los derechos e intereses de otras personas, es decir, se limita unos derechos, que pueden ser Fundamentales, para proteger otros, que en principio no aparecen definidos.

Por último, en el número 2 del mismo Art. 13 D.C. y, por si fueran pocas las excepciones contempladas, se deja la vía abierta a los Estados miembros para limitar, mediante una disposición legal, los Derechos de Acceso, Rectificación, Cancelación, Bloqueo y Notificación del Art. 12, con fines de investigación científica o, en su caso, sean guardados en forma de archivos de carácter personal con fines estadísticos, sin establecer una limitación temporal concreta, ya que se limita a referirse a un periodo que no supere el tiempo necesario.

3.2.7. Derecho de Oposición

Enlazando de nuevo con la regulación de los Derechos, la Sec. 7ª contempla el Derecho de Oposición del interesado, novedad introducida por la Directiva en cuanto a su regulación con carácter general, pues la ley francesa de "Informática, Ficheros y Libertades" contemplaba ya la posibilidad de oposición del sujeto afectado, siempre que no se tratara de ficheros de titularidad pública.

Este derecho sería de gran importancia si realmente se contemplara en el sentido amplio de la palabra, sin que así sea, pues nada más iniciar la redacción del Art. 14 donde se recoge el mismo, se dice "Oponerse al menos en los casos contemplados en las letras e) y f) del Art. 7... a que los datos que le conciernan sean objeto de tratamiento..." lo cual sugiere, ya de entrada, la limitación de la

efectividad de tal derecho a unos cuantos supuestos muy concretos, y, tal vez, con el ánimo de mitigar el amplio margen contemplado como excepción al principio del consentimiento del Art. 7 donde, como decíamos, se utilizan expresiones muy vagas de amplio contenido.

La deficiencia mencionada no es la única tacha en cuanto al margen de efectividad del Derecho de Oposición contemplado por la Directiva, pues también otorga a los Estados miembros la potestad de dejarlo sin contenido si en la legislación interna de los mismos se decide establecer otra cosa. Después de lo mencionado y a pesar del reducidísimo ámbito de aplicación a que queda limitada la oportunidad de hacer efectivo este derecho, la Directiva, como con cierta ironía, recoge la imposibilidad de tratar los datos sobre los que se haya mantenido una oposición justificada.

El párrafo b) del Art. 14 correspondiente al Derecho de Oposición que acabamos de analizar, hace referencia, de forma más amplia y facilitando la actividad del interesado, a los datos recabados y que le conciernan destinados a la "prospección", término que según el Diccionario de la Real Academia Española es definido como "...exploración de posibilidades futuras basada en indicios presentes. Prospección de tendencias de opinión..." Actividad desarrollada por el responsable del tratamiento o por un tercero al que le son cedidos los datos con dicha finalidad y la cual es contemplada por la Directiva con cierta cautela, pues no es lo habitual otorgar tal amplitud y facilidades de acción al interesado, incluso, obligando a los Estados miembros a establecer las garantías necesarias para garantizar a los interesados su conocimiento, lo que no deja de resultar, cuanto menos, curioso, dado, que según la línea seguida por la Directiva, parece como si las limitaciones sólo estuvieran contempladas para imponerlas al interesado, si bien, previo el reconocimiento de unos derechos o principios.

Dentro de la regulación del Derecho de Oposición y bajo el epígrafe "Decisiones individuales automatizadas" en el que se contempla el reconocimiento al interesado de no verse sometido a una decisión con efectos jurídicos basada en el tratamiento automatizado de datos destinados a evaluar su personalidad, derecho que será garantizado por los Estados miembros, salvo que ello se haya contemplado en un contrato, con ciertas condiciones, o también, que el Estado lo autorice legalmente siempre que establezca medidas que justifiquen el interés legítimo del interesado. La LORTAD al respecto, reconoce tal Derecho en el art. 12 sin que por el contrario establezca excepciones al respecto, por lo que en este sentido es más restrictiva la Directiva.

3.2.8. Confidencialidad y Seguridad del tratamiento

La Directiva en su art. 16, dentro de la Sec. 8ª correspondiente a la Confidencialidad y Seguridad del tratamiento, viene a resaltar nuevamente la figura del responsable del tratamiento como el catalizador de la responsabilidad que pueda dimanar de todo lo relativo al tratamiento de los datos personales, limitando la actuación de terceras personas al mandato de éste o salvo que por imperativo legal se establezca otra cosa.

3.2.8.1.- En cuanto a la Seguridad del Tratamiento recogido en el Art. 17 de la Directiva, los legisladores comunitarios, conscientes de la limitación de los conocimientos técnicos y del alto coste que supone un sistema de seguridad, hacen referencia a una "seguridad adecuada" a los riesgos del tratamiento y a la naturaleza de los datos.

Esta problemática viene a ponerse de manifiesto en la "Conferencia sobre Seguridad, Privacidad y Protección de Datos..." donde en el discurso de apertura, el Director de la APD, Martín-Casallo[11], expone, que si bien en toda la normativa que venimos analizando se hace referencia a las medidas de seguridad, sin embargo, ninguna de dichas normas(Convenio, LORTAD y Directiva) da una definición de lo que deba entender por las mismas, ni en qué número deben establecerse, lo que viene motivado, en cierto modo, por el carácter provisional que siempre tendrá la medida de seguridad.

Steve Mathews,[12] en la misma Conferencia, resalta el contraste entre la ley y las tecnología de la información, pues mientras la primera se establece por encima del tiempo, con frases vagas y que lo engloben todo, de modo que duren en el tiempo, sin embargo, las T.I. tienden a ser muy precisas tanto en su definición como en su utilización. Sobre la base de ello, la normativa existente se limita a contemplar unos "tipos legales abiertos" que permitan todo tipo de reglas

■[11] MARTÍN-CASALLO LÓPEZ, Juan José "Discurso Apertura" de la Conferencia...loc. cit.

■[12] Mr. MATHEWS, Steve "Protección de Datos ¿Proceden Nuevos Estándares de Seguridad?", La Conferencia sobre Seguridad, Privacidad y Protección de Datos, celebrada en Madrid del 30 nov. al 1 dic., pág. 121, Agencia de Protección de Datos.

dirigidas a evitar la destrucción accidental o ilícita, la pérdida accidental y la alteración, difusión o acceso no autorizado, como medidas prioritarias.

3.2.8.2.- En cuanto al tratamiento, cada normativa establece una regulación diferente, en este sentido, el Convenio no establece distinción alguna en las medidas de seguridad aplicables al tratamiento automatizado de datos personales.

La LORTAD, por su parte, viene a reforzar las medidas de seguridad en cuanto a los datos especialmente protegidos o "datos sensibles" remitiéndose a un desarrollo reglamentario, que efectuado, en principio, por Real Decreto 1332/94[13], no ha respondido a las expectativas creadas, en cuanto no incide en las medidas de seguridad, por lo que la falta de desarrollo reglamentario en este sentido, impide la aplicación del régimen sancionador previsto en el Tít. VII de la LORTAD y en consecuencia la imposibilidad de llevar a cabo una tutela efectiva de la intimidad personal. De cualquier manera, independientemente de que por vía reglamentaría aún no se halla desarrollado el art. 9 de la LORTAD, hay que resaltar, como se establece en la Memoria de la APD de 1994[14], el que dicha ley sí

"proporcione un sistema de objetivos y criterios en materia de seguridad de datos personales compatible con los principios y criterios generalmente aceptados en el mundo de la seguridad de los sistemas de información y que, aplicado de modo sistemático y complementado en lo necesario con las reglas, técnicas y procedimientos imperantes en dicho mundo, puede permitir discernir la aceptabilidad del conjunto de medidas de protección adoptadas en cada caso, hasta tanto no se plasmen criterios en una regulación detallada como la prevista en los apartados 2 y 3 del Art. 9 de la Ley Orgánica".

En cuanto a la Directiva comunitaria, además de contemplar el reforzamiento del tratamiento de los datos especialmente protegidos, introduce una novedad, al hacerlo extensivo a la transmisión de datos dentro de una red.

■[13] Agencia de Protección de Datos "Análisis y valoración de diversos problemas de la protección de datos a escala Nacional - Problemas relativos a las Medidas de Seguridad- " vid. Pág. 189 y ss de la Memoria de 1995.

■[14] Agencia de Protección de Datos "La seguridad en el tratamiento de datos personales" vid. Pág. 62 y ss de la Memoria de 1994.

Para Martín Casallo,[15] esta diferente regulación obedece al tiempo en que cada norma ha sido aprobada, de este modo, la Directiva apuesta por seguir luchando en favor de la privacidad frente a los recientes avances tecnológicos y en concreto hay que referirse a los Pcs, los que según Steve Mathews,[16] constituyen el aparato de almacenamiento y procesado de datos más poderoso de todos los procesadores de datos personales, sin que por otro lado, exista una normativa que los regule, ni tampoco una postura consensuada sobre los mecanismos criptográficos y su gestión, a fin de procurar la confidencialidad de la información.

3.2.9. Notificación

Por último y dando por concluído el Capítulo II, la Directiva en su Sec. 9ª, bajo el epígrafe "Notificación" viene a establecer con carácter general la necesidad previa de notificar a la Autoridad de Control la intención de realizar un tratamiento de datos personales, atribuyendo nuevamente al responsable del tratamiento o, en su caso, al representante, la responsabilidad de cumplir con tal obligación.

Siguiendo la línea marcada habitualmente por la Directiva, se contempla la posibilidad de suavizar tal obligación, mediante su simplificación o incluso llegando a su omisión, atribuyendo tal posibilidad a los Estados miembros, dentro de unos supuestos que, en principio, no aparecen bien delimitados, pues cuando se hace referencia a "categorías de tratamientos que no puedan afectar a los derechos y libertades de los interesados" se está dejando a los Estados vía abierta para su libre interpretación, cuando, de cara a la protección de los interesados, hubiera resultado más seguro el establecimiento de un número cerrado de supuestos, evitando así el uso de tal expresión. Asimismo, se contempla la misma potestad estatal, cuando el responsable del tratamiento tanga un encargado de la protección de los DP y actúe con arreglo al Derecho nacional al que esté sujeto.

Siguiendo con las excepciones a la obligación de notificación, también se contempla tal posibilidad para los supuestos, a los que la LORTAD da en llamar "fuentes accesibles al público", a que parece referirse el Art. 11, 2, b) de la

■[15] MARTÍN-CASALLO LOPEZ, Juan José "Discurso Apertura" loc. Cit. pág. 17.

■[16] Mr. MATHEWS, Steve "Protección de Datos..." ob. Cit. pág. 132.

LORTAD, los cuales, si bien la LO las excluye de su ámbito de aplicación, la Directiva no sólo las contempla, sino que además, dado su carácter, otorga a los Estados la posibilidad de dispensarlos, no sólo de la obligación de notificación del art. 18.1, sino también, de la obligación de publicidad a que se refiere el Art. 21.1. Excepción esta, esgrimida por Martín-Casallo[17], como uno de los argumentos que vienen a imponer la eliminación de la exclusión del ámbito de aplicación de la LORTAD de los ficheros automatizados de titularidad pública cuyo objeto legalmente establecido sea el almacenamiento de datos para su publicidad con carácter general (Art. 2.2.a) LORTAD) y a los ficheros de información tecnológica y comercial a que se alude el art. 2.2.c) del mismo cuerpo legal. Considerando dicho autor, que si cabe establecer excepciones para estos ficheros con relación a estas obligaciones, implícitamente, la Directiva está admitiendo la aplicación del resto de su contenido a esta clase de ficheros.

Por último y dentro de la Sección dedicada a la notificación, en su art. 21 la Directiva alude a la Publicidad de los tratamientos, atribuyendo a los Estados miembros la obligación de velar por su cumplimiento, así como de cuidar por que la autoridad de control lleve un Registro en el que se inscriban las notificaciones que se vayan realizando y en consecuencia facilitar la consulta por cualquier persona que tenga interés. En tal sentido, la LORTAD crea el Registro General de Protección de Datos (Art. 38 LO) como órgano integrado en la Agencia de Protección de Datos a cuyo cargo está la autoridad de control, que no es otra, que el Director de la Agencia de Protección de Datos.

3.3. RECURSOS

En cuanto a los recursos, tanto la LORTAD en su art. 47, como la Directiva en el art. 22, hacen referencia a dos clases de recursos, los contemplados en vía administrativa y los relativos a la vía judicial. La Directiva deja libertad a los Estados para aplicar lo relativo a este tema y en concreto para determinar el procedimiento sancionador. Asimismo, ambas normas contemplan la reparación del perjuicio sufrido por el interesado, la Directiva atribuyendo tal responsabilidad al responsable del tratamiento, salvo que justifique que la causa del perjuicio es ajena a su actividad. En tal sentido se pronuncia la LORTAD respecto del responsable del fichero, pero sin dejar claro quién sea el que ha de hacer efectiva

■[17] MARTIN CASALLO-LOPEZ, Juan José "Implicaciones sobre la Directiva..." loc. cit.

la indemnización (Art. 17,3). El Convenio 108 alude a la necesidad de establecer recursos y sanciones, pero sin que especifiquen los mismos, remitiéndose a los Estados miembros para su regulación cuando vulneren las disposiciones de derecho interno.

3.4. FLUJO TRANSFRONTERIZO DE DATOS (FTD)

Como dice el profesor, Ripoll Carulla[18], "la característica común a todos los textos sobre protección de datos, es la de contemplar el movimiento internacional de datos como una cuestión autónoma, en la que se establece un principio general, modulado por circunstancias especiales y acompañado de determinas excepciones". Asimismo, añade, "que la solución jurídica arbitrada, es la de admitir que la información deberá circular tan libremente cuando el nivel de protección otorgado sea similar".

3.4.1. FTD a Terceros Países.

La Directiva Comunitaria establece como requisito para hacer posible la transferencia de datos personales a países terceros, el que dicho país garantice un nivel de protección adecuado, atendiendo para su determinación a un conjunto de consideraciones y atribuyendo a la Comisión su valoración, en colaboración con los Estados miembros (Art. 25 D.C.), en este sentido cabe destacar lo dicho por Mensbrubbhe:[19]

"Los Estados miembros y la Comisión se informarán recíprocamente de los casos en que consideren que un tercer país no garantiza un nivel de protección adecuado. Así la Comisión puede constatar este hecho, sin la demanda del Estado interesado. Una vez que el Estado notifique esta situación a la Comisión o que la misma lo compruebe, bloqueará toda transmisión de datos del país tercero con la Unión Europea. La Comisión así después de haber comunicado a los otros

■[18] RIPOLL CARULLA, Santiago "El Movimiento Internacional de Datos en la Ley Española de Protección de Datos" Informática y Derecho 6-7, La Protección de Datos Personales, pags. 314 y 315, UNED, Mérida 1994.

■[19] MENSBRUGGHE, Patricia van der "Flujos transfronterizos de datos en la Directiva 95/46 de las Comunidades Europeas" Actualidad Informática Aranzadi, núm. 20 pág. 14, Ed. ARANZADI, Madrid julio de 1996.

Estados comunitarios la situación, entrará a decidir si el Estado tercero cumple o no el nivel de protección adecuado"

El principio del "nivel de protección adecuado" no es inexpugnable, ya que la Directiva admite la posibilidad de que los Estados miembros dispongan la transferencia a terceros países, aún sin contar con dicho requisito, condicionándolo al hecho de que se den determinadas circunstancias, enumeradas como excepciones en el Art. 26.1 de la norma comunitaria, incluso, se contempla la posibilidad de prescindir de dichas excepciones, cuando el responsable del tratamiento establezca las garantías suficientes, con la única condición, de que se informe a la Comisión y a los demás Estados miembros (Art. 26.2. D.C.), los cuales pueden oponerse a la transferencia, siempre y cuando justifiquen debidamente los motivos, correspondiendo a la Comisión la determinación de las medidas a adoptar sobre la base de lo establecido en el Art. 31.2 de la Directiva.

A nuestro modo de ver, no encontramos suficientemente justificado el hecho de establecer una serie de excepciones al principio general cuando la transferencia se refiera a determinadas circunstancias, en algunos casos, referidas a relaciones contractuales, lo que es admisible, pero en otras, a la salvaguardia de un interés público importante o a un interés vital y, más aún, para el reconocimiento, ejercicio o defensa de un derecho, en las cuales, precisamente por la importancia de estos intereses y derechos, lo razonable es que se dieran todas las garantías por parte de los terceros países y por lo tanto sin que se admitiera excepción alguna si no se da el nivel de protección adecuado. En otras palabras, es cierto que el nivel de protección adecuado se establece, entre otras razones, para proteger unos derechos y en concreto el Derecho a la Intimidad, pero no es menos cierto, que con la excepción a la efectividad de dicho principio, se trata de permitir el ejercicio de otros derechos, los cuales, pudiendo ser en su caso tanto o más importantes que el propio derecho en principio protegido, sin embargo, no cuenta con las mismas garantías que éste, puesto que al establecer la excepción, se está partiendo de la base de que el país tercero no garantiza un nivel de protección adecuado, lo que puede conllevar a la falta de efectividad del derecho que se pretende ejercitar por vía de acudir a la excepción o a vulnerar el protegido por el Principio general o, incluso, a la vulneración de ambos.

Punto de vista que, entendemos, es compartido por Mensbrugghe[20] al manifestar:

Así, si bien la Directiva se explica por razones de protección de la vida privada de las personas, nos parece evidente que existen también intereses estatales para proteger las informaciones de las personas más allá de la frontera europea o, si es el caso, impedir su salida del territorio comunitario. Nos referimos de una parte a motivos de seguridad pública, de defensa y de seguridad del Estado..."

Con ello, la autora parece mostrarse a favor del flujo transfronterizo de datos siempre que se respete un nivel mínimo de protección, sin embargo, entiende que éste debe ceder a intereses estatales en los que se puede justificar la transferencia, ahora bien, se está refiriendo a datos que quedan fuera del ámbito de aplicación de la norma comunitaria, dada su trascendencia, como pueden ser los relativos a la seguridad pública, la defensa y seguridad del Estado, por lo que fuera de estos supuestos, debemos entender que no admite excepciones al nivel mínimo de protección exigible.

Tal vez una omisión ciertamente criticable en la regulación de la Directiva, la cual ya se detectaba en la LORTAD y el Convenio, siguiendo las palabras de Ripoll Carulla[21], sea el hecho de que sólo se contemple el supuesto de la exportación de datos, sin que se haga alusión alguna a los casos de importación de los mismos, lo que puede llevar a ciertas incongruencias.

3.4.2. FTD entre Estados Miembros

Expuesto lo relativo a la parte dispositiva de la norma comunitaria respecto al flujo transfronterizos de datos, también los Considerandos de la Directiva recogen ampliamente este tema, no sólo respecto a lo establecido respecto a terceros países, Considerandos 56 a 60, en los que se viene a predecir prácticamente la regulación establecida en el articulado de la Directiva, sino que también resulta interesante adentrarnos en su contenido, por contemplar

■[20] MENSBRUGGHE, Patricia van der "Flujo transfronterizo de datos..." ibid. pág. 13.

■[21] RIPOLL CARULLA, Santiago, "El Movimiento Internacional de Datos..." ob. cit. pág. 317.

ampliamente el tema desde la perspectiva exclusiva de los Estados miembros (Considerandos 3 al 9).

En atención al establecimiento de un mercado interior, que entre otras cosas, implicará un aumento de los flujos transfronterizos de datos personales, se debe garantizar la libre circulación de los mismos, incidiendo en el respeto de los Derechos Fundamentales de las personas y contemplando las nuevas tecnologías, así como la coordinación de las nuevas redes de telecomunicaciones, como medios que faciliten el intercambio de datos personales. Para el logro de todo lo cual se considera necesario que la Comunidad intervenga a fin de superar la disparidad de criterios, mediante el establecimiento de un nivel de protección equiparable, que evite la obstaculización de la libre circulación entre los Estados miembros, y ello, independientemente de que se contemple un margen de maniobra para estos, siempre que se desarrolle en el contexto de la Directiva. Al respecto, el legislador comunitario es consciente de que dicho margen puede implicar el resurgimiento de disparidad de criterios al interpretar la norma.

Por nuestra parte y respecto a este margen de maniobra, entendemos, que puesto que el legislador comunitario es consciente de la disparidad de criterios que pueden surgir entre los Estados miembros como consecuencia de no establecer al respecto una regulación taxativa y siendo una de las pretensiones de la Directiva, el no obstaculizar la libre circulación de datos y el lograr una regulación equivalente entre los Estados, lo más prudente hubiera sido no contemplar dicho margen, evitando así la incertidumbre de futuros conflictos.

3.5. CODIGOS DE CONDUCTA

Tanto el Art. 27, como el Considerando 61 de la Directiva, vienen a definir lo que dan en llamar Códigos de Conducta, como acuerdos establecidos por las asociaciones profesionales y demás organizaciones representantes de responsables de tratamiento, para la correcta aplicación de las disposiciones nacionales adoptadas por los Estados miembros en aplicación de la presente Directiva. En este sentido, la LORTAD, adoptando la denominación de Códigos Tipo, con el que encabeza la regulación del Art. 31, habla de acuerdos sectoriales o decisiones de empresa, a los que califica de códigos deontológicos o de buena práctica profesional, recogiendo todo un conjunto de aspectos en los que se puede concretar su contenido, pero circunscribiéndolo exclusivamente a los responsables de ficheros de titularidad privada, circunstancia no contemplada por la Directiva.

Por otra parte, la Directiva recoge la posibilidad de que los Códigos puedan ser sometidos a examen del Grupo de protección a que se refiere el art. 29 de dicha norma, pudiendo la Comisión efectuar una publicidad adecuada de los que hayan obtenido el directamente favorable de dicho Grupo, pero sin que establezca la obligación de su registro. La LORTAD en cambio, no sólo contempla la obligación del registro de los Códigos tipo, sino también, el supuesto de que el Director de la APD pueda requerir a los solicitantes, para que efectúen las correcciones oportunas.

Vista la disparidad de criterios entre la regulación establecida en la Directiva y la LORTAD, es evidente que la regulación más inquisitiva y sectorial prevista por la LORTAD, deberá acoplarse a la más flexible establecida por la Directiva en el momento de la transposición de ésta al Derecho interno español.

3.5.1. Efectividad práctica de los Códigos de Conducta

La experiencia de la efectividad práctica de los Códigos tipo en nuestro Derecho, conforme a las inscripciones realizadas, de las cuales se hacen eco las Memorias de la APD de los años 94, 95 y 96[22], publicadas hasta el momento, refleja la escasa actividad en este sentido por parte de las asociaciones profesionales y demás organizaciones. Así, en el año de 1994 se presentaron para su inscripción en el Registro General de Protección de Datos dos proyectos de códigos tipo, uno por Telefónica de España S.A., el cual resultó ser el único inscrito, y otro por la asociación ASEICO, justificando dichas peticiones, la primera por el importante volumen comercial y la incidencia de su actividad en el tema de protección de datos y, la otra, por desenvolver su actividad en materia de prestación de servicios sobre solvencia patrimonial y crédito recogida en el Art. 28 de la LORTAD. Esta actividad de registro, si de por sí había resultado escasa en el año de 1994, se vio en decremento durante 1995, al haberse solicitado e inscrito un único código tipo, precisamente el presentado por la Asociación de Empresas de Servicios de Informes Comerciales (ASEICO), la que no había logrado la inscripción en el año anterior. Siendo nula dicha actividad durante el año de 1996,

■[22] Agencia de Protección de Datos, "Códigos Tipo" págs. 89, 141 y 179 de las Memorias de 1994, 1995 y 1996 (respectivamente)

en el que no se produjo ninguna inscripción.

La escasa efectividad reseñada anteriormente de los Códigos Tipo, es achacada por la APD, de una parte, a la falta de efectividad de la imposición sancionadora y de otra, a la escasa aceptación por parte de los grupos afectados. Por lo que, si a esto unimos el carácter voluntario que con la transposición de la Directiva tendrá su inscripción, es predecible, salvo que se establezcan otros mecanismos de motivación, la desaparición de los mismos.

3.6. AUTORIDAD DE CONTROL

La Directiva Comunitaria, ya en sus Considerandos, resalta la importancia de la Autoridad de Control, al considerarla como un elemento esencial a tener en cuenta en la regulación de cada Estado miembro, haciendo hincapié en la necesidad de su independencia en el ejercicio de sus funciones, a fin de garantizar la protección de las personas en materia de tratamiento de datos personales, mediante el ejercicio de las labores de investigación e intervención y, procurando en todo momento, la transparencia del tratamiento y la ayuda mutua entre los Estados miembros (Considerandos 62 al 64 D.C.).

La parte dispositiva de la Directiva, en el Capítulo VI, dedica el extenso Art. 28, a reiterar lo ya plasmado en los considerandos de la misma respecto a la Autoridad de control, matizando ciertos aspectos, como lo relativo a la posibilidad de que cada Estado pueda establecer varias autoridades, o determinando lo que haya de entenderse por la capacidad de investigación e intervención. También contemplando otras funciones como la capacidad procesal para el supuesto de producirse infracciones a la normativa de transposición, así como entender de aquellas solicitudes planteadas por cualquier persona, especialmente en cuanto a la licitud del tratamiento.

Asimismo se contemplan una serie de obligaciones, como la de presentar un informe periódico sobre sus actividades, el secreto profesional, incluso después de su cese y, por último, el ejercitar las competencias que se le hayan atribuido dentro del territorio de su Estado, con la particularidad, de que ante una posible pasividad de ésta, podrá ser instada por la autoridad de otro Estado, para ejercer sus funciones.

Es reprochable al legislador comunitario, el que no haya aprovechado la extensa regulación de la Autoridad de Control, para haberse pronunciarse sobre

un tema tan controvertido como el de la independencia de la Autoridad de Control, limitándose a resaltar la importancia de tal característica.

La regulación establecida al efecto por la LORTAD, se ciñe a la Directiva, atribuyendo la consideración de autoridad de control a la Agencia de Protección de Datos, personalizada por el Director, el cual la dirige y representa. Dedica todo el Título VI, desarrollado a su vez por Real Decreto 428/1993, de 26 de marzo, por el que se aprueba el Estatuto de la Agencia de Protección de Datos, el cual, determina a su vez la estructura orgánica, conforme al mandato del Art. 34.2 y Disposición Final Primera de la Ley Orgánica.

3.6.1. Independencia de la Autoridad de Control

Dada la extensión de su regulación, no consideramos oportuno realizar un análisis pormenorizado de su contenido, aunque sí es ineludible hacer referencia a la "independencia" predicada de la autoridad de control por la Directiva y la LORTAD. En este sentido, la Lortad, tal como establece en su articulado, atribuye la referida independencia a la APD, al señalar en su Art. 34.2 "... que actúa con plena independencia de las Administraciones Públicas en el ejercicio de sus funciones..." , reiterado en el Art. 1.2 del Estatuto, el cual añade "y se relaciona con el Gobierno a través del Ministerio de Justicia".

Desde nuestro punto de vista, difícilmente se pude predicar la independencia de un órgano que es nombrado por el Gobierno, lo cual, si bien no se recoge expresamente en la LORTAD, sí se deduce de su contenido, cuando establece que el nombramiento se hará mediante Real Decreto (Art. 35.1 LO y 14.1 R.D.). También se atribuye al Ejecutivo la potestad de cesarlo, si bien, mediante la instrucción del correspondiente expediente y en los limitados supuestos ya previamente determinados (Art. 35.3 LO y 15.2 R.D.). A este mar de sospechas que planea sobre la predicada independencia, hay que añadir que la relación del Director con el Gobierno se hará a través del Ministerio de Justicia (Art. 1.2 R.D.), por lo que, tácitamente, se está sometiendo a este órgano, al conducto de procedimiento reglamentario y por lo tanto dentro del orden jerarquizado de la Administración.

Por todo ello e independientemente de que se trate de un Ente de Derecho Público, con personalidad jurídica propia y plena capacidad pública y privada (Art. 34.2. LO) y tenga la consideración de alto cargo (Art. 35.4), resulta incuestionable que la independencia política de la APD cuanto menos, quede en

entredicho.

Por lo expuesto y con relación a este aspecto concreto, la obligada transposición de la Directiva al Derecho interno español, brinda la oportunidad de aclarar las dudas que planean sobre este polémico tema.

No obstante lo dicho, hay autores que entienden perfectamente determinada la independencia de la Agencia de Protección de Datos, tal es el caso de la profesora De la Serna Bilbao[23], la cual, partiendo de la regulación legal establecida en los Arts. 34.2 de la LORTAD y 1.2. del Estatuto, incluye a la APD dentro de la clasificación de Administración Independiente, encuadrándola concretamente en lo que el profesor Parejo Alfonso, citado por la misma, califica de novedoso tipo de organizaciones "administrativas", las cuales surgen para y en sectores clave, caracterizados por un fuerte dinamismo.

Asimismo, De la Serna toma en consideración las ideas de los entes independientes de supervisión del profesor Betancor Rodríguez, las cuales pueden resumirse por una parte en que "Todas las Administraciones independientes participan de dos características comunes: ...que sus miembros ... no pueden ser removidos discrecionalmente ni recibir órdenes o instrucciones del Gobierno...por lo que gozan de un estatuto jurídico que garantiza su independencia...lo que permite que su gestión sea políticamente neutral" y por otra en que "... uno de los elementos que permite calificar un ente público de independiente es la no sujección de sus actos a instrucciones de ningún otro órgano...ausencia de un control jerárquico...sólo cabe un control de legalidad por parte de los órganos de la jurisdicción y por los limitados supuestos en los que se puede destituir al director".

Pues bien, sobre la base de dichas consideraciones, la profesora entiende que lo más relevante es la fijación de una relación cerrada de hipótesis de cese anticipado del Director de la APD, limitando la posibilidad de instrucción del expediente a los supuestos c), d) o e) del art. 15.2 del Estatuto, de todo lo cual deduce una estabilidad del Director de la Agencia que en palabras de la profesora

■[23] DE LA SERNA BILBAO, María Nieves "La Agencia de Protección de Datos Española: con especial referencia a su característica de independencia" Actualidad Informática Aranzadi, núm. 22, enero 1997, Ed. ARANZADI.

"... es el principal y más importante mecanismo de garantía de independencia". A lo cual añade la importancia del Consejo Consultivo, en cuanto el Director tiene que ser nombrado por el Gobierno de entre sus miembros, así como la independencia de carácter funcional de la Agencia, en cuanto a que las decisiones del Director cierran la vía administrativa, dejando abierta la contenciosa administrativa y por último, como corolario de la independencia predicada de la APD, la contemplada legalmente en materia presupuestaria.

A la vista de la resumida exposición de la defensa del carácter independiente de la APD que realiza la mencionada profesora, nos mantenemos firmes en nuestra posición de entender que la misma no es predicable en la regulación actual de la LORTAD y el Estatuto de la APD, por entender, aparte de lo ya expuesto, que si bien es cierto que el Estatuto establece unos supuestos concretos ya predeterminados por los que el Gobierno puede cesar al Director de la APD, no es menos cierto que dichos supuestos no sólo no aparecen bien delimitados, sino que además, esta falta de concreción, puede servir de base para entender que la discreccionalidad del gobierno se recoge de forma subrepticia en las letras a) y b) del art. 15.2 del Estatuto. Con lo cual, no queda demostrada la pretendida estabilidad de la autoridad y por consiguiente su independencia, por más que se pretenda abundar en otros aspectos como la importancia atribuida al Consejo Consultivo por ser nombrado el Director de entre sus miembros, lo que a juicio de la profesora implica una mayor independencia. Al respecto, no cabe olvidar que dicho Consejo está formado por miembros de entidades públicas y privadas. Asimismo, la pretendida independencia de naturaleza funcional, en cuanto a que las decisiones del Director de la Agencia ponen fin a la vía administrativa, sería ingenuo pensar la adopción de un acto por la Agencia en contra de la política gubernamental, si el Director no quiere verse inmerso en un expediente por incurrir en causa de cese, pues aunque han de ser oídos los miembros del Consejo, nada dice la Ley Orgánica o el Estatuto, sobre el carácter vinculante del informe que éste emitiera.

3.7. GRUPO DE PROTECCION

Organo, que de responder a la misión que la Directiva le atribuye, está destinado a ser el gran catalizador entre los Estados miembros de la C.E., tal como esboza el Considerando 65 de la Directiva, al considerar, que actuará con total independencia, a fin de asesorar a la Comisión y contribuir a la importante misión, de la aplicación uniforme de las normas nacionales adoptadas en aplicación de la Directiva.

La Directiva dedica dos artículos, el Art. 29, a fin de determinar la formación y funcionamiento de tal órgano y el Art. 30, en el que se determinan las funciones. En cuanto al primero, resaltar únicamente que la composición estará integrada por el representante de la autoridad o autoridades de control designada por cada Estado miembro.

Lo importante de su regulación, se centra en las funciones reconocidas en el Art. 30, principalmente por atribuir al Grupo, en su nº1.a), el velar por el cumplimiento de uno de los Principios básicos de la Directiva, como es, contribuir a la aplicación homogénea de la Directiva, mediante el estudio de toda cuestión relativa a la aplicación de las disposiciones nacionales destinadas a hacer efectiva el cumplimiento de la misma, con lo que, a su vez, se cumple con otro de los principios básicos como es el evitar diferencias entre los Estados miembros.

Otras funciones atribuidas, de menor relevancia, pero no por ello dejan de ser importantes, son las de emitir dictámenes sobre el nivel de protección existente y sobre los códigos de conducta elaborados, formular recomendaciones sobre cualquier asunto sobre protección de datos, funciones estas, que se tramitarán por el Comité y la Comisión, a la cual asesorará e informará, en caso de apreciar divergencias entre lo establecido en la Directiva y la practica de los Estados miembros. Estableciendo como obligación del Grupo, la elaboración de un informe anual sobre el nivel de protección existente.

La LORTAD, dentro de las funciones atribuidas a la APD, en su Art. 36.l), al atribuirle el desempeñar las funciones de cooperación internacional en materia de protección de datos personales y, por extensión, a lo establecido en el Art. 9,2 del Estatuto de la APD, si bien refiriéndose al Convenio 108, por el que se establece la obligación de prestar asistencia a las autoridades designadas, lo que por Real Decreto 156/96, de 2 de febrero, que modifica el Estatuto de la APD, a fin de designar a ésta como representante español en el Grupo de protección de personas a que se refiere la Directiva y atribuyendo al Director de la APD la potestad de designar a la persona encargada de personalizar dicha representación, adicionando al Art. 9 del Estatuto el Apartado 3 a fin de recoger dicha modificación.

3.8. MEDIDAS DE EJECUCION

Ya el último Capítulo de la Directiva, el VII, hace referencia al Comité como órgano encargado de asistir a la Comisión en su función de ejecución de las medidas que en cada caso hayan de adoptarse, se entiende, para cumplimiento de lo establecido en la Directiva. El Comité, formado por representantes de los Estados miembros y presidido por el representante de la Comisión, deberá pronunciarse sobre los proyectos de dichas medidas, mediante la emisión de un dictamen. Para el caso de que dichas medidas sean aplicadas en sentido contrario a lo establecido en el dictamen, se contempla la particularidad, en el Art. 31, único en este Capítulo, de que entren en juego tres órganos comunitarios, los dos ya citados, y el Consejo, que será el órgano encargado de dirimir la cuestión.

El papel que desempeña el Comité en el orden comunitario, viene a corresponderse con el atribuido en la LORTAD (art. 37) y el Estatuto (art. 18) al Consejo Consultivo, pero a diferencia de lo que ocurre con los dictámenes no tomados en consideración por la Comisión en el plano comunitario, los informes emitidos por el Consejo a propuesta del Director no vinculan a éste, ni dan lugar a arbitrio de un tercer órgano, de lo que se deducen las amplias facultades en todos los órdenes que la LORTAD atribuye al Director de la APD.

3.9 MARGEN DE MANIOBRA, GARANTIAS Y DEFICIENCIAS

3.9.0. Introducción

En congruencia con el conjunto de los Principios Básicos contemplados en los Considerandos 7 al 11 de la Directiva y en especial atendiendo a lo establecido en el nº 9, cuyo contenido hace referencia a "que los Estados miembros dispondrán de un margen de maniobra(...)dirigido a mejorar la protección que proporciona su legislación en la actualidad", resulta evidente la doble finalidad de dicho considerando, con el que se pretende, de una parte, dejar un margen a los Estados para que, dentro del marco determinado por la Directiva, estos dispongan de la suficiente autonomía a fin de adaptar dicha norma, en la medida que les sea posible, a sus peculiaridades internas. Por otra parte, procurando que dicha potestad se ejerza de forma que suponga una mejora de la legislación hasta el momento existente, con objeto de establecer un mayor grado de protección de las personas físicas frente al TDP. Para nivelar el ínter relación

entre las dos pretensiones señaladas, resulta imprescindible que, a su vez, la Directiva arbitre las garantías necesarias a fin de evitar el conflicto entre ambas y, en consecuencia, impedir que prevalezca una con el consiguiente menoscabo de la otra.

Un tercer aspecto debe tenerse en cuenta a fin de evitar que el equilibrio pretendido, entre el margen de maniobra y las garantías, pueda verse desestabilizado. Nos estamos refiriendo, a la necesidad de determinar las posibles deficiencias de que adolece la norma comunitaria, las cuales pueden plantearse dada la dificultad práctica de concretar determinados conceptos o ideas, lo que puede dar lugar a interpretaciones dispares que no sólo afecten al equilibrio al que nos referimos, sino también a la unificación de criterios entre los Estados miembros.

3.9.1 Margen de maniobra atribuido por la Directiva a los Estados miembros

Como ya se ha puesto de manifiesto, el margen de maniobra contemplado para la transposición de la Directiva al Derecho interno de los Estados miembros, es reconocido por el Considerando 9 de la Directiva, siendo desarrollado de forma amplia a lo largo de su articulado, en los términos que pasamos a enunciar:

En cuanto al ámbito de aplicación, se atribuye a los Estados miembros la responsabilidad de aplicar la Directiva, mediante la norma que al efecto establezcan, incluso mediante el establecimiento de normas específicas para determinados sectores (Consid°. 68), contemplando toda una serie de supuestos que puedan plantearse en cuanto al responsable del tratamiento de datos personales (Art. 4 DC).

En cuanto a los Principios básicos de protección de datos y Derechos, que en la Directiva aparecen contemplados bajo el epígrafe "Condiciones Generales para la licitud del tratamiento de datos personales", la norma comunitaria se limita a establecer el marco dentro del cual los Estados miembros precisarán las condiciones de licitud. (Art. 5 DC).

La Directiva, en cuanto a los datos sensibles que regula bajo el epígrafe "Tratamiento de categorías especiales de datos" (art. 8) establece la particularidad de prohibir el tratamiento de los mismos, aunque dicha prohibición puede quedar desvirtuada cuando se obtiene el consentimiento explícito del interesado, si bien a este respecto, se atribuye a los Estados miembros la potestad, de impedir el

levantamiento de tal prohibición, aunque se cuente con el consentimiento del interesado. Asimismo, en el punto 4 del mismo artículo, se contempla de forma amplia otra posibilidad de levantar la prohibición al tratamiento de datos sensibles, aún prescindiendo del consentimiento del interesado, al permitir a los Estados que amparados en "motivos de interés público importante", puedan establecer otras excepciones a las ya contempladas para el tratamiento de datos sensibles, siempre que dispongan las garantías necesarias y sean notificadas a la Comisión. Dichas excepciones puedan establecerse mediante la legislación interna del Estado o por decisión de la Autoridad de Control.

Se deja la vía abierta a los Estados miembros para limitar, mediante una disposición legal, los Derechos de Acceso, Rectificación, Cancelación, Bloqueo y Notificación del Art. 12, con fines de investigación científica o, en su caso, sean guardados en forma de archivos de carácter personal con fines estadísticos, sin establecer una limitación temporal concreta, ya que se limita a referirse a un periodo que no supere el tiempo necesario.

Dentro de la regulación del Derecho de Oposición y bajo el epígrafe "Decisiones individuales automatizadas" (art. 15.2) en el que se contempla el reconocimiento al interesado de no verse sometido a una decisión con efectos jurídicos basada en el tratamiento automatizado de datos destinados a evaluar su personalidad, derecho que será garantizado por los Estados miembros, salvo que el Estado lo autorice legalmente siempre que establezcan medidas que justifiquen el interés legítimo del interesado.

La Directiva, contempla la posibilidad de suavizar la obligación de notificar a la Autoridad de Control la intención de realizar un tratamiento de datos personales mediante su simplificación o incluso llegando a su omisión, atribuyendo tal posibilidad a los Estados miembros, dentro de unos supuestos.

También se contemplan excepciones para los supuestos "fuentes accesibles al público", la Directiva, dado su carácter, otorga a los Estados la posibilidad de dispensarlos, no sólo de la obligación de notificación del art. 18.1, sino también, de la obligación de publicidad a que se refiere el Art. 21.1

Dentro de la Sección dedicada a la notificación, en su art. 21, la Directiva alude a la Publicidad de los tratamientos, atribuyendo a los Estados miembros la obligación de velar por su cumplimiento, así como de cuidar por que la Autoridad de Control lleve un Registro en el que se inscriban las notificaciones que se vayan

realizando y en consecuencia facilitar la consulta por cualquier persona que tenga interés.

En cuanto a los recursos, la Directiva en el art. 22, hace referencia a dos clases de recursos, los contemplados en vía administrativa y los relativos a la vía judicial. La Directiva deja libertad a los Estados para aplicar lo relativo a los Recursos y en concreto para determinar el procedimiento sancionador.

La Directiva establece como requisito para hacer posible la transferencia de datos personales a países terceros, el que dicho país garantice un nivel de protección adecuado, atendiendo para su determinación a un conjunto de consideraciones y atribuyendo a la Comisión su comprobación (Art. 25 D.C.). Pero el principio del "nivel de protección adecuado" no es ineludible, ya que la Directiva admite la posibilidad de que los Estados miembros dispongan la transferencia a terceros países, aún sin contar con el requisito del nivel de protección adecuado, condicionándolo al hecho de que se den determinadas circunstancias.

En cuanto a la TDP entre los Estados miembros de la CE, se considera necesario, que la Comunidad intervenga a fin de superar la disparidad de criterios, mediante el establecimiento de un nivel de protección equiparable, que evite la obstaculización de la libre circulación entre los mismos, y ello, independientemente de que se contemple un margen de maniobra para los Estados miembros, siempre que se desarrolle en el contexto de la Directiva.

El Art. 28 de la Directiva, en el que se regula la Autoridad de Control, establece la posibilidad de que cada Estado pueda establecer varias autoridades de control.

Asimismo la Directiva en su art. 29, establece que la composición del Grupo de protección estará integrada por el representante de la autoridad o autoridades de control designado por cada Estado miembro.

También atribuye a estos el designar a su representante para integrar el Comité contemplado en el art. 31.1 de la Directiva.

3.9.2. Garantías establecidas en la Directiva

Las garantías que a nuestro entender tienen más consistencia y de las

cuales va a depender el equilibrio a que hacíamos referencia al iniciar este capítulo, se sustentan básicamente en los Organos contemplados por la Directiva, los cuales, grosso modo, por un lado tienen la finalidad de llevar a buen fin la protección de las personas físicas en materia de TDP, por otro, la de velar por una aplicación homogénea entre los Estados miembros evitando que surjan diferencias entre los mismos y, por último, la de asistir a la Comisión en su función de ejecución de las medidas que en cada caso hayan de adoptarse para cumplimiento de lo establecido en la Directiva. Nos estamos refiriendo, respectivamente a las actividades mencionadas, a la Autoridad de control (art.28), el Grupo de protección (art. 29) y al Comité (art.31).

También es una novedad introducida por la Directiva, la de atribuir al Responsable del Tratamiento o, en su caso, el Representante en que éste delegue, la responsabilidad que en cada supuesto pueda derivarse del tratamiento de datos personales, hasta el punto de establecer como condición indispensable para la aplicación de la Directiva, el hecho de que las actividades del responsable del tratamiento de datos personales se desenvuelvan dentro del ámbito de aplicación del Derecho Comunitario (Considerando 12), contemplando toda una serie de supuestos que puedan plantearse en cuanto al responsable del tratamiento de datos personales (Art. 4 D.C.),

Asimismo y en cuanto al responsable del tratamiento, la Directiva en su Art. 6 atribuye a los responsables del tratamiento la obligación de garantizar el cumplimiento de los principios generales reconocidos en toda norma de protección de datos.

Se atribuye al responsable del tratamiento o a su representante, la obligación de informar al interesado, salvo que ya hubiera sido informado, de los datos recabados a fin de ser tratados.

En cuanto al mantenimiento de la exactitud de los datos, parece deducirse del tenor literal de la Directiva, que dicha actividad no sólo pueda realizarse de oficio, sino que por el contrario, cualquier interesado puede instar su actualización.

Los registros de condenas penales, medidas de seguridad e infracciones, habrán de se ser llevados bajo el control de los poderes públicos, así como las sanciones administrativas o procesos civiles.

La Directiva inicia la regulación de los Derechos en la Sec. 5ª con El Derecho de Acceso, el que regula de forma más detallada que el Convenio y la LORTAD, y siendo a su vez menos restrictiva que éstas, en el sentido de que al contrario de lo contemplado en la LO, no establece limitaciones en cuanto a su ejercicio, aunque haga referencia a una "periodicidad razonable", pero sin que se concrete en un periodo de tiempo determinado.

Como particularidad introducida al regular el Derecho de Acceso, se contempla, lo que en la LORTAD aparece regulado de forma independiente como Derecho de Rectificación y Cancelación (Art. 15), añadiendo además la posibilidad del Bloqueo de los datos y contemplando la obligación de notificar el haber practicado tales actividades conforme a lo solicitado por el interesado

La Directiva comunitaria, además de contemplar el reforzamiento del tratamiento de los datos especialmente protegidos, introduce una novedad, al hacerlo extensivo a la transmisión de datos dentro de una red.

Dentro de la regulación establecida en la Directiva de la obligación de notificación, se contempla la posibilidad de establecer excepciones para las "fuentes accesibles al público", lo cual quiere decir que implícitamente está reconociendo la aplicación de la norma comunitaria a este tipo de datos.

En su art. 21 la Directiva alude a la Publicidad de los tratamientos, atribuyento a los Estados miembros la obligación de velar por su cumplimiento, así como de cuidar por que la autoridad de control lleve un Registro en el que se inscriban las notificaciones que se vayan realizando y en consecuencia facilitar la consulta por cualquier persona que tenga interés, sin limitar a plazo alguno.

En cuanto a los recursos, la Directiva en el art. 22, hace referencia a dos clases de recursos, los contemplados en vía administrativa y los relativos a la vía judicial. La Directiva deja libertad a los Estados para aplicar lo relativo a este tema y en concreto para determinar el procedimiento sancionador. Contempla la reparación del perjuicio sufrido por el interesado, atribuyendo tal responsabilidad al responsable del tratamiento, salvo que justifique que la causa del perjuicio es ajena a su actividad.

La Directiva Comunitaria establece como requisito para hacer posible la transferencia de datos personales a países terceros, el que dicho país garantice un nivel de protección adecuado, atendiendo para su determinación a un conjunto de

consideraciones y atribuyendo a la Comisión su valoración, en colaboración con los Estados miembros (Art. 25 D.C.).

Tanto el Art. 27, como el Considerando 61 de la Directiva, hacen referencia a los Códigos de Conducta, los que tienen por cometido la correcta aplicación de las disposiciones nacionales adoptadas por los Estados miembros en aplicación de la Directiva, así como la posibilidad de que los Códigos puedan ser sometidos a examen del Grupo de protección a que se refiere el art. 29 de dicha norma, pudiendo la Comisión efectuar una publicidad adecuada de los que hayan obtenido el directamente favorable de dicho Grupo, pero sin que establezca la obligación de su registro.

3.9.3. Deficiencias de que adolece la directiva

Con carácter general, a lo largo de la regulación establecida en la Directiva se abusa de la utilización de conceptos jurídicos indeterminados, así como de la falta de especificación de las garantías en los supuestos para los que éstas se contemplan, amén de otras deficiencias y carencias que iremos desglosando.

3.9.3.1. Utilización de Conceptos jurídicos indeterminados

En cuanto a lo que en la Doctrina Jurídica se conoce como conceptos jurídicos indeterminados, podemos hacer referencia a supuestos como el contemplado en el Art. 7, el cual evoca el principio general del consentimiento del interesado de forma "inequívoca". Sin embargo, en el modo de establecer excepciones a tal principio, acude al uso de conceptos jurídicos indeterminados, tales como "interés vital", "misión de interés público", "interés legítimo perseguido", conceptos estos que habrán de ser concretados en cada caso por la Autoridad de Control, sin que todo ello beneficie en modo alguno a los interesados, pues se les priva de la garantía de saber a priori, que limitaciones son las que se contemplan con la referencia a tales términos.

La Directiva, en el art. 8 al establecer la particularidad de prohibir el tratamiento de los datos sensibles, flexibiliza tanto tal prohibición, que acaba convirtiéndola en la excepción; así independientemente del margen permitido a los Estados miembros puede quedar sin contenido, cuando se plantean supuestos como los ya calificados de conceptos jurídicos indeterminados, tal como el "interés vital" o recurriendo a ambigüedades como "cuando haya que respetar las

obligaciones y derechos(...)del responsable del tratamiento en materia laboral".

En su momento calificamos de excesivo el margen permitido a los Estados miembros por la Directiva, al permitirles, que amparados en "motivos de interés público importantes", lo que no es mas que una remisión en blanco, puedan establecer otras excepciones a las ya contempladas para el tratamiento de datos sensibles.

En el Derecho de Acceso, la obligación de notificar el haber practicado tales actividades conforme a lo solicitado por el interesado, con una salvedad, que ello no resulte imposible o suponga un esfuerzo desproporcionado, con lo cual, queda en manos del responsable el practicar efectivamente la notificación, ya que siempre podrá escudarse en la dispensa mencionada, para eludir tal obligación.

En el Derecho de Acceso no establece limitaciones en cuanto a su ejercicio, aunque hace referencia a una "periodicidad razonable", pero sin que se concrete en un periodo de tiempo determinado.

En cuanto a la Seguridad del Tratamiento recogido en el Art. 17 de la Directiva, los legisladores comunitarios, hacen referencia a una "seguridad adecuada" a los riesgos del tratamiento y a la naturaleza de los datos.

La Directiva en su Sec. 9ª, bajo el epígrafe "Notificación" viene a establecer con carácter general la necesidad previa de notificar a la Autoridad de Control la intención de realizar un tratamiento de datos personales, También se contempla la posibilidad de suavizar tal obligación, mediante su simplificación o incluso llegando a su omisión, atribuyendo tal posibilidad a los Estados miembros, dentro de unos supuestos que, en principio, no aparecen bien delimitados, pues cuando se hace referencia a "categorías de tratamientos que no puedan afectar a los derechos y libertades de los interesados" se está dejando a los Estados vía abierta para su libre interpretación.

El principio del "nivel de protección adecuado" establecido en la TDP no es ineludible, en este sentido, la Directiva contempla la posibilidad de prescindir de las excepciones a que se refiere el art. 26.1, cuando el responsable del tratamiento establezca las garantías suficientes, con la única condición, de que se informe a la Comisión y a los demás Estados miembros (Art. 26.2. D.C.), los cuales pueden oponerse a la transferencia, siempre y cuando justifiquen debidamente los motivos

3.9.3.2. Falta de especificación de las garantías contempladas

La obligación de notificación por parte del responsable del fichero puede quedar vacía de contenido cuando añade "o resulte imposible o exija esfuerzos desproporcionados", ya que puede servir en cualquier caso de excusa para eludir la obligación de informar al interesado dada la dificultad de demostrar lo contrario. También se excepcionan, cuando el registro o la comunicación a tercero esté expresamente prescrito por la ley, y como suele ser lo habitual, con la obligación de establecer las garantías apropiadas, las cuales no especifica.

En cuanto al margen de maniobra permitido a los Estados miembros por la Directiva, en cuanto que al contemplar la posibilidad de que amparados en motivos de interés público importantes, puedan establecer otras excepciones a las ya contempladas para el tratamiento de datos sensibles, añadiendo, siempre que dispongan las garantías necesarias, las cuales no llega a especificar, y sean notificadas a la Comisión, pero sin determinar si ésta en su caso puede oponerse a las mismas.

Las excepciones contempladas en la Directiva al regular, dentro de la Sección 7ª el Derecho de Oposición, las "Decisiones individuales automatizadas" en las que se atribuye a los Estados miembros la garantía de su correcta aplicación, salvo que ello se haya contemplado en un contrato, con ciertas condiciones, o también, que el Estado lo autorice legalmente siempre que establezca medidas que justifiquen el interés legítimo del interesado.

3.9.3.3. Otros supuestos

Dentro de las excepciones a la prohibición inicialmente establecida del tratamiento de datos sensibles, puede resultar realmente peligroso lo relativo a las fundaciones y asociaciones de determinado carácter sin fin lucrativo, a las que conforme al Art. 18.4 de la DC, se les puede eximir de la obligación de notificar a la Autoridad de Control o simplificar la misma, lo que, como ya expusimos en su momento, a nuestro modo de ver, puede dar lugar a facilitar la actividad de las sectas que se amparen en alguna de la finalidades mencionadas en el Art. 8.2.d) DC.

En la regulación establecida en la Directiva al contemplar en el art. 13 lo relativo a las excepciones y limitaciones, ya dejamos de manifiesto en su

momento, que no compartíamos el margen permitido a los Estados miembros de limitar el alcance de las obligaciones y derechos, cuando dicha limitación se efectúe en los supuestos a que dicho artículo se refiere en los apartados d) al f), al privar al interesado de unos derechos y de unas garantías con relación al tratamiento de sus datos personales, los que pueden afectar, entre otros Derechos, a su propia Intimidad, frente a unos intereses que afectan a infracciones penales o deontológicas, intereses económicos o financieros "importantes" o a funciones de control, inspecciones o reglamentarias relacionadas con las anteriores. Intereses estos, que habría que examinar caso por caso, a fin de determinar si realmente han de prevalecer por encima del Derecho del interesado o no. También se establece igual limitación, a fin de garantizar la protección del interesado o de los derechos e intereses de otras personas, es decir, se limitan unos derechos, que pueden ser Fundamentales, para proteger otros, que en principio no aparecen definidos.

En el número 2 del Art. 13 D.C., se deja la vía abierta a los Estados miembros para limitar, mediante una disposición legal, los Derechos de Acceso, Rectificación, Cancelación, Bloqueo y Notificación del Art. 12, con fines de investigación científica o, en su caso, sean guardados en forma de archivos de carácter personal con fines estadísticos, sin establecer una limitación temporal concreta, ya que se limita a referirse a un periodo que no supere el tiempo necesario.

En cuanto al margen de efectividad del Derecho de Oposición, si bien la Directiva tiene el acierto de introducirlo como una novedad que redunda en beneficio del interesado; dado el margen a que queda reducido, hubiera sido preferible omitir su regulación, pues no es de recibo que se permita a los Estados miembros la potestad de dejarlo sin contenido, si la legislación interna de los mismos, se pronuncia en este sentido, siendo extraño que haya algún Estado que reconozca este Derecho dada las implicaciones que de él se derivan.

El cuanto al principio del "nivel de protección adecuado" respecto a la TDP la Directiva admite la posibilidad de que los Estados miembros dispongan la transferencia a terceros países, aún sin contar con dicho requisito, condicionándolo al hecho de que se den determinadas circunstancias, enumeradas como excepciones en el Art. 26.1 de la norma comunitaria.

En los Considerandos 3 al 9 de la Directiva se hace referencia a la TDP entre los Estados miembros, estableciendo que se debe garantizar la libre circulación entre los mismos. La Comunidad debe intervenir a fin de superar la

disparidad de criterios, independientemente de que se contemple un margen de maniobra para estos, siempre que se desarrolle en el contexto de la Directiva. Al respecto, el legislador comunitario, es consciente de que ello puede implicar el resurgimiento de disparidades en la aplicación de dicha norma.

La Directiva omite cualquier referencia a la importación de datos de terceros estados.

Si bien la Directiva predica la independencia de la Autoridad de control al igual que lo hace la LORTAD, esta voluntad queda desvirtuada desde el momento en que la Autoridad de control está formada por miembros elegidos por la Autoridad de control de cada Estado miembro, en el caso español, la APD representada a su vez en la persona del Director, quien a su vez es nombrado por el Gobierno, incluso puede ser cesado. Por todo lo cual, independientemente, al estar impregnada de interferencias políticas, queda en entredicho. Todo lo cual se puede hacer extensible a la independencia predicada igualmente del Grupo de protección, por iguales motivos que los mencionados para la Autoridad de control

4. ANALISIS DE LAS LEGISLACIONES SOBRE P.D. DE LOS ESTADOS MIEMBROS DE LA C.E. CON ANTERIORIDAD A LA DIRECTIVA 95/46/CE

4.0. INTRODUCCION

Como ya esbozamos en su momento[24], uno de los problemas más acuciantes en el panorama existente, previo a la aprobación de la Directiva 95/46/CE, entre los Estados miembros, era fundamentalmente la disparidad de criterios en materia de protección de datos, que incidía de forma negativa en varios aspectos, entre ellos, en la pretensión comunitaria de establecer un mercado único europeo sin fronteras, para lo cual se hacía necesario establecer un nivel equiparable de protección de los derechos y libertades de los ciudadanos comunitarios, especialmente atendiendo a la protección del Derecho a la intimidad. Esta falta de unanimidad de criterios, no sólo venía determinado por las distintas regulaciones establecidas por las leyes de protección de datos (LPD), sino también por la carencia de las mismas en determinados países, como era el

[24] Vid. Pág. 3, 1. Introducción.

caso de Italia y Grecia, lo cual impedía entre otros objetivos comunitarios, la posibilidad de garantizar el flujo transfronterizo de datos entre los propios Estados miembros, motivando regulaciones restrictivas al efecto, como era el caso noruego en que se prohibía toda exportación de datos relacionados con informaciones crediticias, o el caso sueco, que impedía la exportación de cualquier tipo de datos personales a países que no fueran parte del Convenio 108, salvo que existiera consentimiento expreso del afectado.

Partiendo de la importancia que el Convenio 108 tuvo en su momento, contribuyendo a acelerar la aprobación de leyes sobre PDP y a revisar las ya existentes, siendo su objetivo el de lograr un mínimo nivel equivalente de protección procurando, por un lado, que los particulares de los Estados miembros tuvieran un mínimo de protección y, por otro, permitir la libre circulación de los datos, el llamado "núcleo irreductible"; dando como resultado, el que la totalidad de los Estados miembros aprobaran el Convenio 108, a pesar de que no todos lo ratificaron. Lo cierto es que dicho Convenio, con el paso de los años y el imparable avance de las "nuevas tecnologías" resultaba insuficiente por caduco y falto de precisión en su regulación y lo más grave de todo, en palabras de Lazpita Gurtubay [25]:

" ... es la posibilidad que ofrece a los países ratificantes de excluir categorías enteras de archivos automatizados, lo que significa que dichos datos no están protegidos por las leyes que los han excluido, haciendo necesario conocer el criterio adoptado por cada una de las leyes nacionales para valorar la protección ofrecida en cada situación concreta, resultando particularmente difícil en un contexto internacional".

Lo cual impedía que pudiera ser tomado como paradigma, en materia de protección de datos, a fin de unificar criterios entre los Estados miembros, de ahí la necesidad cada vez más acuciante de establecer una norma que viniera a superar todas estas deficiencias en el marco de la Comunidad Europea.

■[25] LAZPITA GURTUBAY, María "Análisis Comparado de las Legislaciones sobre Protección de Datos de los Estados Miembros de la Comunidad Europea" Informática y Derecho 6-7, La Protección de Datos Personales, pág. 413. UNED, Centro Regional de Extremadura, Mérida 1994.

Visto desde otro ángulo, la falta de regulación unitaria entre los Estados miembros, igualmente hacía peligrar la efectiva de los acuerdos elaborados entre algunos de los Estados miembros, en este sentido cabe mencionar el Acuerdo de Schengen de 1985[26], con el que se pretendía suprimir los controles de las fronteras comunes para concentrarlos en las fronteras exteriores, a fin de crear un "espacio interior común" para lo que se hacía necesario un modo uniforme de controlar el cruce en las fronteras exteriores, creando a tal fin el Sistema Informático de Schengen (S.I.S.). que supone el soporte para la transmisión automatizada de los datos necesarios para la consecución de los objetivos propuestos.

Es precisamente en la protección de datos personales, donde surge el principal escollo, pues son las legislaciones nacionales las que deben asegurar en este sentido los derechos y libertades fundamentales, especialmente el derecho a la intimidad, tal y como se recogía en el art. 8 del Convenio 108, que como decíamos constituía la norma internacional tomada como paradigma en materia de PDP Pero dada la diferencia de criterios entre los Estados firmantes a la hora de establecer el nivel de protección de los derechos mencionados, en palabras de Sánchez Bravo[27] "Esta disparidad supone un serio obstáculo a la realización de esa finalidad protectora perseguida. Es por ello que se impone que el nivel de protección sea equivalente en todos los Estados miembros..."

4.1. EVOLUCION DE LA PRIMERA A LA SEGUNDA GENERACION

Como señala Lazpita Gurtubay[28]:

■[26] Acuerdo de Schengen de 14 de junio de 1985, firmado por Bélgica, Francia, Luxemburgo, Países Bajos y la antigua República Federal Alemana en la ciudad que lleva su nombre. Acuerdo completado posteriormente por el Convenio de Aplicación del Acuerdo de Schengen, firmado el 19 de junio de 1990.

■[27] SANCHEZ BRAVO, Alvaro "La Protección de los Datos Personales en la Europa de Schengen" Informática y Derecho núm. 12 al 15, Segundo Congreso Internacional, Actas (Volumen II) pág. 1424, UNED, Centro Regional de Extremadura, Mérida, 1996.

■[28] LAZPITA GURTUBAY, María "Análisis Comparado de las Legislaciones sobre..." ob. cit. pág. 404.

" Desde una perspectiva exclusivamente europea, todas las leyes de protección de datos tienen en común los aspectos siguientes: el reconocimiento del carácter excepcional (Unique Nature) del procesamiento de datos personales; la inequívoca manifestación de los propósitos de los requerimientos para procesar informaciones personales; la continua revisión actualizadora de las normas y la previsión de una autoridad independiente de control"

Partiendo de estas características comunes de las leyes sobre PDP y previamente a efectuar un análisis más pormenorizado de las mismas, consideramos conveniente perfilar la evolución que estas normas han experimentado desde sus inicios. En este sentido, mencionaremos como primera norma en la materia la del Länden de Hesse[29] de 1970, en Alemania Federal, siendo a partir de la misma cuando los Estados conscientes del peligro que la informática podía revestir para los derechos de sus ciudadanos, comienzan a aprobar leyes sobre protección de datos.

Esta primera oleada de leyes de PDP constituyeron lo que se dió en llamar leyes de la "primera generación", siendo la sueca de 1973 la pionera, estableciendo una regulación en la que se contemplaba a la vez tanto los datos relativos al sector público, como al privado, caracterizada por basarse en un sistema de registro masivo con el que se pretendía en esencia como su propio nombre indica la constitución de un registro central de todos los bancos de datos del país, atribuyendo a la Autoridad de Protección de Datos la potestad de autorizar a los responsables de los bancos de datos existentes el tratamiento de los llamados "datos sensibles", si bien reconociendo un conjunto de derechos y garantías a los ciudadanos, tales como los derechos de información, acceso, rectificación. Dada la influencia de esta ley en el entorno europeo, siguieron otras leyes en Francia, Dinamarca, Noruega y Austria de 1978 y la de Luxemburgo de 1979. Estas leyes se caracterizaban por ser rígidos instrumentos basados en una ley general con un órgano de control, las cuales se crean como reacción al nacimiento de la informática.

■[29] La primera norma europea tutelar de datos fue promulgada en Hesse en 1970, su breve articulado preveía la regulación del acceso a la información de los bancos de datos públicos y la supervisión de su funcionamiento a un ombudsman especializado, el Comisario para la protección de datos.

La Ley alemana de 1977, si bien pertenece a esta primera generación, establece una serie de innovaciones con respecto a las de su tiempo, que la colocan en una posición a caballo entre las de la primera y segunda generación. Así, a diferencia de las que siguen el modelo sueco, la alemana se basaba en el sistema de registro de auto regulación, dejando prácticamente inexistente el registro central. La característica principal de esta ley, es la de permitir el procesamiento de datos personales, no porque se realice bajo la vigilancia de una autoridad central como ocurría en las de la primera generación, sino porque el Derecho así lo contemple o porque se cuente con el consentimiento del particular. Establece, al igual que las anteriores, un conjunto de garantías, pero ampliándolas a supuestos como el de información de la existencia de ficheros con datos que le conciernen, la obligación de la cancelación de datos inexactos, así como los que ya no tengan valor para los fines para los que se recogieron, así como el introducir la necesidad de contemplar medidas de seguridad para la protección de los datos y por último, contemplando la figura del Controlador de Datos, como persona responsable del control de los bancos de datos.

Con el Convenio 108, se inicia la "Segunda Generación" que trae consigo la aprobación de nuevas leyes y la revisión de las correspondientes a la primera generación. Se caracterizan por procurar una simplificación, abandonando los mecanismos previos de control y procurando la autorregulación mediante la posibilidad de imponer sanciones administrativas a fin de hacer efectiva la protección de datos. Esencialmente se procura un equilibrio entre la protección de los derechos de los ciudadanos, especialmente el derecho a la intimidad, con el desarrollo de las nuevas tecnologías en el ámbito de la información, estableciendo a tal fin la figura de una Autoridad de Control.

4.2. NORMATIVA DE LOS ESTADOS MIEMBROS SOBRE PDP

En este apartado haremos un breve estudio del conjunto de las leyes del ámbito europeo comunitario, con especial hincapié en aquellas que han destacado, bien sea por suponer el inicio de una época, como es el caso de la sueca, por sus peculiaridades, casos francés y británico o por su influencia en otras normas, caso alemán.

4.2.1. Suecia.

Ley sobre Datos, nº. 289, de 11 de mayo de 1973, (DATALAG-) reformada por las leyes 334/79 y 442/82, así como otras reformas posteriores de

27 de mayo de 1992, 22 de diciembre de 1993, 1 de diciembre de 1994 y 8 de junio de 1995.

En cuanto a su ámbito de aplicación, va dirigida a cualquier persona física de cualquier nacionalidad siempre que se encuentre residiendo en el país. Su objeto es tanto los archivos públicos como los privados. Respecto a los bancos de datos, contempla la obligación de inscripción ante la autoridad de aplicación, quien expedirá una licencia al efecto, salvo en el supuesto de que por ley se establezca otra cosa o refieran a datos sensibles y médicos. También se regula la obligación de hacer público qué datos se recogen y procesan, debiendo ser conformes a la finalidad del banco de datos y mantenerse seguros, los cuales, una vez cumplida la finalidad para la que fueron recogidos deben ser eliminados.

En cuanto a los derechos del particular a quien afecta la recogida de datos, cabe señalar que una vez al año puede conocer si sus datos aparecen registrados y cuáles son éstos. Derecho de corrección y que se notifique a terceros la misma, así como el Derecho de integración, a fin de que la información sea correcta.

Existe un régimen especial para determinada categoría de datos, a los que califica de sensibles, como los que hagan referencia a condenas penales, reincidencia, salud, sexo y ayudas sociales. Cumpla dentro de este régimen igualmente los datos muy sensibles que se refieran a la raza, opinión política, credo y convicciones. Por último y sin que el motivo de su inclusión dentro de este régimen sea muy claro, se refiere a los datos sobre personas que no estén relacionadas con el titular del banco de datos, tal vez obedeciendo a motivos de seguridad.

También se establece una clase de registro muy particular, el denominado SPAR (Registro Permanente de las Personas y los Domicilios) al cual se puede acudir para obtener datos básicos, pudiendo el particular hacer constar su negativa a recibir publicidad por vía postal.

Por lo que respecta a la transferencia internacional de datos, por regla general se requiere la autorización de la autoridad de aplicación, salvo para el caso que el país de destino sea un Estado miembro del Convenio 108 del Consejo de Europa.

La autoridad de aplicación, la forma un órgano colegiado el

"Inspectoriado de Datos", constituido por once miembros.

El sistema sancionador es bastante severo, al contemplar penas privativas de libertad y multas, con posibilidad de ser agravadas en determinados supuestos. Todo ello con imposición de la responsabilidad civil que pudiera derivarse de la falta y la sanción complementaria de confiscación de los archivos infractores.

Por lo expuesto, se aprecian influencias de las normas de la primera generación, como en lo relativo al ámbito de aplicación, a los principios relativos a la calidad de los datos o al carácter de especial otorgado a los datos sobre personas que no estén relacionados con el titular del banco de datos, si bien la Reforma introducida en el año 1982, con posterioridad a la aprobación del Convenio 108 denotan un intento por acoplarse a las directrices establecidas por ése, apreciándose la misma en la regulación de la transferencia de datos y en consecuencia participando de las normas de la segunda generación.

4.2.2. Francia

Ley sobre "Informática, Ficheros y Libertades" núm. 78-17 de 6 de enero de 1978. Constituye el sistema más flexible de los vigentes en Europa previo a la aprobación de la Directiva 95/46/CE. A diferencia de la ley sueca, son sujetos de protección todas la personas físicas de cualquier nacionalidad, residan o no en Francia.

De su art. 1 se deduce, que su ámbito de aplicación es más amplio que el de otras normas, supeditando en todo caso la informática a las personas físicas cuando establece en su art. 1 que " La informática deberá estar al servicio de cada ciudadano...". Su ámbito de aplicación abarca, siguiendo la línea de amplitud señalada, a todo archivo automático o manual, público o privado. En cuanto a los datos objeto de especial protección, reserva el control absoluto de los datos relativos a condenas penales al sector público; considerando como datos sensibles los relativos a la raza, opiniones políticas, credo o afiliación a sindicatos, para los que establece como requisito imprescindible de posibilidad de tratamiento el consentimiento por escrito del afectado, exceptuando los archivos de iglesias, sindicatos o asociaciones, así como los archivos afectos a la libertad de prensa. Los datos sólo se conservarán por el tiempo declarado o autorizado, lo que significa que ya de antemano se debe establecer el tiempo que durará el tratamiento.

Por lo que a las garantías se refiere, establece la obligación de seguridad y la de proceder de oficio en la corrección de los datos inexactos.

En cuanto a los derechos de los interesados, se establecen algunas particularidades en relación con la ley sueca, las cuales ponen de manifiesto la ya comentada supeditación del tratamiento a los intereses de las personas físicas, así se contempla el derecho a ser informado de forma que le sea entendible de los datos archivados y que le conciernen, también se establece la posibilidad de cobrar una pequeña cuota al efecto. De peculiar se puede calificar la posibilidad que se le concede de discutir la información cuyo tratamiento redunde en contra de sus intereses, así cómo la de oponerse a que se procese información que le concierne, siempre que esta información no se halle en ficheros de titularidad pública.

En cuanto a los principios, se recoge el de tratamiento leal, en el sentido que al interesado se le debe de informar del carácter obligatorio u optativo de la declaración de los datos, los efectos que supondría la negativa, el destinatario de la información y como ejercer los derechos de acceso y réplica.

Se establece una regulación distinta para los ficheros públicos y privados, siendo necesario para el funcionamiento de los primeros, una resolución específica que los contemple, previo el directamente de la autoridad de control, quien expedirá una licencia. Por lo que respecta a los privados, deben comunicar a la autoridad de control, la existencia del archivo y sus características, previamente al desarrollo de su actividad.

Por lo que se refiere a la transferencia internacional de datos, sólo se refiere a los archivos privados, en cuanto contempla la posibilidad de ser sometidos a la autorización de la autoridad de control o ser reglamentada tal actividad por dicha autoridad. Se entiende que en cuanto a los públicos, la propia resolución que establece su funcionamiento, establecerá a su vez la actividad desarrollada en este aspecto.

De gran importancia es el papel que se atribuye a la autoridad de control, recayendo en un órgano colegiado "La Comisión Nacional de la Informática y las Libertades" (CNIL) compuesto por diecisiete miembros, doce designados por órganos públicos y cinco por personalidades de reconocida competencia. Tiene el carácter de autoridad administrativa independiente con amplias facultades reglamentarias, de control y sancionadoras. Actúa bajo la actividad de tres

subcomisiones especializadas en determinadas parcelas.

Se contemplan sanciones de carácter penal que pueden acarrear la privación de libertad y multa. Se establecen medidas cautelares a fin de evitar la desaparición u ocultación de datos.

4.2.3. Reino Unido

Data Protección Act 1984, de 12 de julio. Fue de las leyes en las que influyó decisivamente la aprobación del Convenio 108, ya que habiendo tomado conciencia de la necesidad de poner límites a la informática en los tiempos en que se aprobaron las leyes correspondientes a la primera generación, sin embargo tuvo que transcurrir un dilatado periodo de tiempo para establecer una regulación de protección de datos, debido a la actitud reacia del gobierno británico a poner límites al procesamiento de datos.

Sujetos objeto de protección, al igual que la ley francesa, se hace extensiva a todas las personas físicas de cualquier nacionalidad, residente o no en el país. En cuanto al ámbito de aplicación se refiere a los ficheros automatizados públicos y privados, reservándose la posibilidad de contemplar los manuales, siguiendo las pautas que al respecto establece el Convenio 108. También se aprecia la influencia de éste en cuanto a la regulación establecida de los Principios relativos a la calidad de los datos, siendo una réplica del art. 5 del Convenio.

Los derechos atribuidos al afectado, además de los típicos de información y acceso, corrección y borrado para el caso de que los datos sean inexactos, se establece la particularidad de excluir del registro una serie de datos, entre ellos los relativos a las nóminas, listas de jubilados, datos contables etc.

Aunque se contempla la posibilidad de establecer garantías para las categorías especiales de datos, éstas no se han establecido, por lo que no gozan de protección especial.

La autoridad de control encargada de garantizar el cumplimiento de la ley con poderes de inspección, recae en la persona del "Registrar", el cual es responsable ante el Parlamento y cuya obligación es la de llevar el registro y control de los bancos de datos personales públicos, privados y de servicios a terceros, emitir directrices de comportamiento y recibir las quejas. Tiene la posibilidad de interferir el flujo transfronterizo de datos. Las resoluciones del

Registrar son apelables ante el "Data Protección Tribunal"

En cuanto a las sanciones, aunque el mantener o procesar datos de forma contraria a la establecida legalmente, no se contemplan penas privativas de libertad, si se recogen penas pecuniarias sin sujeción a límite. Los perjudicados pueden exigir indemnización de daños y perjuicios.

4.2.4. Alemania

Ley Federal sobre la Protección de Datos (BDSG) de 27 de enero de 1977, reformada el 20 de diciembre de 1990, ampliando en gran medida su ámbito de aplicación al sector público, donde se establece la obligación de publicar los datos que se recogen y procesan y a quién y cómo los procesan, tal vez obedeciendo a las consecuencias derivadas de la Sentencia de 15 de diciembre de 1983[30] sobre la Ley del Censo Electoral. Incluye en su ámbito de aplicación todo archivo automatizado o manual, público o privado (en estos se establecen ciertas limitaciones), salvo los archivos manuales no destinados a comunicarse a terceros y archivos cuya finalidad sean actividades de información o entretenimiento; siendo sujetos de protección, cualquier persona física de cualquier nacionalidad, residente o no en un Estado miembro.

Como particularidad, se establece la regla general de prohibición de procesar datos personales, salvo que por ley se establezca otra cosa o se cuente con el consentimiento expreso y por escrito del interesado.

Los derechos del sujeto se concretan en el de información, corrección, bloqueo y cancelación.

Otra particularidad es la obligación que se establece para quienes presten servicio de información a terceros, de omitir, comunicar la información relativa a datos de más de cinco años de antigüedad, con lo que parece deducirse, que no se

■[30] Tribunal Constitucional Federal Alemán Sentencia de 15 de diciembre de 1983, sobre la Ley del Censo de 1983. Sentencia de gran influencia en la que se reconoce el "Derecho de la autodeterminación informática", estableciendo grandes limitaciones al tratamiento de datos personales, especialmente limitando las amplias potestades de que gozaban los poderes públicos en este ámbito, como así lo demostraba la regulación establecida al respecto por la Ley recurrida.

establece limitación al tiempo de conservación de los datos o que no se atiende al límite atendiendo a los fines para los que fueron creados.

También resulta peculiar la regulación relativa a los datos de carácter especial, en el sentido de que no se establece una relación de datos sensibles, sino que se presta atención a las operaciones comerciales en las que se establece una liberación de la transmisión de datos a terceros respecto a una serie de datos, generalmente de utilidad en dicho sector.

Para la transmisión de datos entre Estados se remite a las condiciones exigidas por el Convenio 108, art. 12.

La autoridad de control recae en un funcionario nombrado por el presidente, actuando bajo la denominación de "Delegado Federal para la Protección de Datos Personales".

En cuanto al régimen de sanciones se contemplan penas privativas de libertad y multas.

4.2.5. Otros Estados del ámbito europeo comunitario

- Entre las leyes de la primera generación quedan por mencionar las siguientes:

* Dinamarca.- Su ley de protección de datos data de 1978, caracterizándose por la distinción entre ficheros públicos y privados, estableciendo una normativa diferente para cada uno de ellos. Dicha ley sufrió dos reformas, la de 1987 por la que se amplia el derecho de acceso a los sujetos de datos y la de 1991 por la que se simplifica el control de los ficheros públicos.

* Luxemburgo.- Con una ley de protección de datos de 1979, limitando su regulación a los datos personales automatizados.

* Austria.- Ley de 18 de octubre de 1978 "Bundesgesetz über den Schutz personenbezogener Daten (Datenschutzgesetz - DSG)", reformada por BG BGBI 1981/314 y BG BGBI 1986/370.

- Entre las de la segunda generación:

* En Irlanda la "Data Proteccion Act" de 1988, dada la influencia del Convenio 108 su regulación se adapta en gran medida a las directrices marcadas por el mismo. Es muy similar al modelo Británico. La autoridad de control se denomina "Irish Data Protection Commisioner" cuya misión es la de velar por el cumplimiento de la ley, siendo el encargado de permitir la transferencia internacional de datos.

* La "Ley sobre los Ficheros de datos personales" de los Países Bajos de 1989. Al igual que la española, aunque con menos retraso, tiene por objeto cumplir el mandato constitucional por el que se contemplaba la protección del Derecho a la Intimidad de las personas frente a la informática y por otra con la ratificación efectuada del Convenio 108. El órgano encargado del cumplimiento de la ley es la Cámara de Registro.

* En Portugal la legislación de protección de datos esta constituída por el art. 35 de la Constitución portuguesa, la Ley 10/1991 de 29 de abril "Ley de Protección de Datos Personales frente a la Informática" y Ley 28/94 de 29 de agosto por la que se "Aprueban medidas de Reforma de la Protección de Datos Personales". Por lo tanto al igual que los Países Bajos y España, recoge en su Constitución la necesidad de proteger a las personas frente a los avances de la informática, si bien con una regulación más exhaustiva que la española, pues no se limita exclusivamente a hacer una remisión de desarrollo legal sino que establecía un breve sistema de tutela. El órgano encargado de velar por el cumplimiento de la ley es la Comisión Nacional para la Protección de Datos Personales Automatizados.

* La ley 1987/471 "Personal Data File Act", de 30 de abril de Finlandia, reformada por Decretos 1994/387, de 27 de mayo y 1994/431, de 3 de junio.

* La "Ley relativa a la protección de la vida privada, en lo que respecta al tratamiento de datos personales" de 8 de diciembre de 1992 de Bélgica. Como órgano de protección se establece "La Comisión Consultiva para la Protección de la Vida Privada" y por otra parte el "Registro Nacional de Personas Físicas". Su entrada en vigor se ha efectuado de forma progresiva, acudiendo a numerosos decretos-ley para su desarrollo.

* En España La Ley Orgánica 5/1992 de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal, de 29 de abril (L.O.R.T.A.D.) En circunstancias similares al país vecino, la Constitución Española de 1978

aprovechó la sensibilización del momento para establecer en el art. 18.4 la remisión a una norma con rango legal para la limitación de la informática, aprobando y ratificando en el año de 1994 el Convenio 108 del Consejo de Europa, así como la firma del protocolo en 1990 del Convenio de Schengen de 1985 .

- Leyes posteriores a la Directiva 95/46/CE.

* La Ley de 31 de diciembre de 1996, nº 675 "Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali" [31]de Italia, la cual si bien es posterior a la aprobación de la Directiva 95/46/CE, para nada hace referencia a la misma, sin que se ajuste a las directrices marcadas por la norma comunitaria, con lo que entendemos que el legislador italiano lo que se ha planteado con la reciente aprobación de esta ley es cubrir la laguna existente en su ordenamiento jurídico y al mismo tiempo, aprovechar dicha necesidad para cumplir con algunos de los compromisos internacionales asumidos y más perentorios, dilatando la transposición de la Directiva al periodo que le resta del plazo de tres años establecido por la misma al efecto.

4.3. TRANSPOSICION DE LA DIRECTIVA A LOS ESTADOS MIEMBROS:

Situación actual

La actividad desarrollada por los Estados miembros de la C.E. a fin de transponer la Directiva a sus legislaciones internas, hasta el momento está resultando un tanto decepcionante, sin que en principio se aprecie una actividad mínima a tal fin.

Una excepción la constituye el caso belga, donde a partir de la aprobación de la Directiva, han aprovechado las ventajas que esta aporta para reformar su antigua ley de 1982, la cual había quedado totalmente desfasada, dada la utilización de conceptos ambiguos, con un ámbito de aplicación poco definido qué con las nuevas tecnologías podía hacer extensible la aplicación de la ley belga a todo el mundo (art. 3), derechos de los ciudadanos limitado al igual que su ejercicio y en general su excesivo formalismo.

■[31] Vid g. 1, Capítulo 1. Introducción.

En contraposición a la actividad desarrollada por los belgas, tenemos el caso de Italia donde, como ya hemos tenido ocasión de comentar, se acaba de publicar su primera ley de protección de datos sin que se haya aprovechado el hecho de que la Directiva era de fecha anterior, para haber adaptado la nueva ley a la norma comunitaria, por el contrario, la regulación que se establece parece no estar muy acorde con sus directrices.

Por lo que a Portugal se refiere, el legislador es consciente de la necesidad de transponer la Directiva, por considerar que su legislación actual es mucho más restrictiva. A este fin, se hará necesario la reforma el art. 35 de la Constitución Lusa, pues en la misma se establece la imposibilidad de identificar a sus ciudadanos por un número de identificación personal, hecho que es admitido por la Directiva y aunque no imponga su obligación, en ningún caso lo prohibe.

En Finlandia, por el Ministro de Justicia se ha creado una Comisión "Personal Data Commision" en fecha 4 de octubre de 1995, a fin de realizar el proyecto encaminado a adaptar la actual Ley 1987/471, de 30 de abril en materia de protección de datos a la Directiva 95/46/CE.

5. LA LORTAD EN EL PANORAMA EUROPEO

5.0. INTRODUCCION

Hay que remontarse a los tiempos, en que la Informática comenzaba a despegar como una nueva tecnología, con unas prestaciones hasta entonces desconocidas y un desarrollo sin límites imaginables, para que algunos Estados, percatados del peligro que ello podía suponer para los derechos y libertades de sus ciudadanos y, en concreto, para su intimidad, comenzaran a limitar su uso, mediante la aprobación de leyes de protección de datos, siendo la primera en la materia, la Sueca del 1973. En nuestro país, ya con cierto retraso, los legisladores conscientes de la ausencia de regulación en la materia, aprovechan la redacción de la Constitución Española de 1978, para recoger expresamente la necesidad de limitar la Informática, remitiéndose a una ley, que en su día hiciera realidad tal inquietud. Mandato que se dilata en el tiempo de forma insospechada, hasta que por fin, se aprueba la Ley Orgánica 5/92, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal.

Con la aprobación de dicha Ley, se viene a cubrir una dilatada etapa de vacío normativo en materia de protección de datos en nuestro país, y ello, a pesar

de haber sido el segundo país europeo, después de Portugal, en recoger constitucionalmente la necesidad de limitar la Informática, además de haber sido uno de los cinco primeros países europeos en ratificar, el 27 de enero de 1984, el Convenio del Consejo de Europa de 1981, primer texto internacional en materia de protección de datos de carácter personal, el cual, ante la carencia legislativa y en virtud de lo establecido en el Art. 10 de la Constitución, ha sido esgrimido como fuente de valor interpretativo por la Sentencia del T.C. 254/1993, de 20 de julio[32] :

Respecto a la cuál debe ser el contenido mínimo provisional, en relación con el derecho reconocido en el art. 18.4 CE, aún en ausencia de desarrollo legislativo, el primer elemento de tal contenido es negativo: el uso de la informática encuentra un límite en el respeto al honor y a la intimidad de las personas, siendo aquí donde pueden venir en auxilio interpretativo los tratados y convenios internacionales sobre esta materia.

El Legislador configura la LORTAD de forma estanca con relación a todo un cuerpo normativo preexistente que, hasta ese momento, había cumplido el importante cometido de suplir todas aquellas lagunas que pudieran plantearse en materia de protección de datos según apunta Heredero Higueras[33]. En este sentido, cabe destacar en especial, la Ley 62/1978, de 26 de diciembre de Protección Jurisdiccional de los Derechos Fundamentales de las Personas, la Ley Orgánica 1/1982, de 5 de mayo de Protección Civil del Derecho al Honor, a la Intimidad Personal y Familiar y a la Propia Imagen, la Orden de 30 de julio de 1982 sobre Limitación de Acceso a la Información contenida en las Bases de Datos Fiscales, Ley Orgánica 3/1986, de 14 de abril, de Medidas Especiales en materia de Salud Pública y por último, la Ley 12/1989, de 9 de mayo, de la Función Estadística Pública, con la que la LORTAD guarda un nexo de unión al establecer el Art. 36 m) de la Ley de la F.E.P., la atribución a la Agencia de Protección de Datos (APD), el control de la aplicación de las disposiciones de protección de datos contenidos en ella.

■[32] (TC IªS 254/1993 de 20 de julio.- Ponente: Sr. García-Mon y González -Regueral.) LA LEY, 1994-1, 152 (2282-TC)

■[33] HEREDERO HIGUERAS, M: "Ley Orgánica 5/1992, de 29 de octubre, de regulación del Tratamiento Automatizado de Datos de Carácter Personal" Boletín Informativo del Ministerio de Justicia, núm. 1669, Madrid 1993.

En palabras de Pérez Luño[34], la LORTAD llega tarde y mal, lo primero, por la demora en su aprobación y, lo segundo, porque no aprovecha la experiencia previa del Derecho Comparado en la materia. Por ello, la mayoría de autores, entre ellos, Carrascosa López[35], coinciden en hablar de una serie de deficiencias que arrastra la LORTAD, entre ellas, la ya mencionada en palabras de otros autores referida a las numerosas excepciones, asimismo la posibilidad de que los datos sensibles sean recogidos y tratados por las Fuerzas y Cuerpos de Seguridad del Estado prescindiendo del consentimiento del afectado, la dependencia gubernativa del Director de la APD, fruto de lo cual, quedan por resolver cuatro Recursos de Inconstitucionalidad, el del Defensor del Pueblo, los de la Generalidad y el Parlamento de Cataluña y del Grupo Parlamentario Popular.

En este sentido, es oportuno traer a colación las dudas planteadas por el profesor Valentín Carrascosa[36], al preguntarse, si realmente la Lortad nace en virtud del mandato constitucional y la obligación contraída con la ratificación del Convenio de Estrasburgo para proteger efectivamente a las personas o, por el contrario, se trata de cumplir a toda prisa con la imposición del Convenio de Schengen[37], cuyo objetivo principal, es más bien, la autoprotección de lo Estados, lo que vendría a explicar la protección especial establecida para los Ficheros de titularidad pública. Siguiendo con las incógnitas planteadas por este Autor, en el sentido de si la LORTAD realmente lo que busca es cumplir con una obligación, pero con un escaso compromiso de fondo.

Esta tendencia proteccionista de la LORTAD hacia los Ficheros de

■34 PEREZ LUÑO, Antonio-Enrique "La LORTAD: Entre las luces y las sombras", en Informática y Derecho, Núm. 6-7, pág.83 UNED Mérida 1994.

■35 CARRASCOSA LOPEZ, Valentín "La LORTAD: Una necesidad en el panorama Legislativo Español", en Informática y Derecho núm. 6-7, pág.15, UNED, Mérida 1994.

■36 CARRASCOSA LOPEZ, Valentín "La LORTAD: Una necesidad en él..." ibid., Pág. 23.

■37 - Convenio de Aplicación del Acuerdo de Schengen, firmado el 19 de junio de 1990.
- Acuerdo de Schengen, fimado por los Estados del Benelux, R.F.A. y la R. Francesa el 14 de junio de 1985 en Schengen,.

titularidad pública, frente al verdadero espíritu que debe inspirar toda ley de protección de datos, como es la de velar por la protección de los Derechos y Libertades de las personas físicas frente al tratamiento de los datos de carácter personal, es lo que ha dado lugar, en gran medida, a la interposición de los Recursos de Inconstitucionalidad antes mencionados contra la Ley Orgánica, por considerar en términos generales que atenta contra los Derechos y Principios reconocidos previamente por la propia LORTAD.

Como no sería justo referirse exclusivamente a las carencias de la LORTAD, en su haber, hay que señalar siguiendo a Pérez Luño, el haber definido los Principios Básicos que informarán la actuación de los bancos de datos automatizados que procesan informaciones personales (Arts. 4 a 11) o el reconocimiento y tutela jurídica de la Libertad Informática (Arts. 12 a 17) estableciendo al efecto un mecanismo de protección, el Habeas Data o facultad de acceso, como cauce o acción procesal para salvaguardar la libertad informática.

Volviendo a las deficiencias que arrastra la LORTAD, hay que advertir que las mismas no son exclusivas de nuestra Ley de protección de datos, ya que, en un aspecto u otro, las legislaciones del resto de los Estados de la C.E., debido en parte a la dilatada exclusividad del Convenio 108 como única norma de Derecho Internacional a tener en cuenta en esta materia, la que resultaba caduca e insuficiente, por limitarse a establecer unas pautas generales y permitir a los Estados miembros unas posibilidades tan amplias de establecer excepciones, que provoca el que las legislaciones internas difieran mucho unas de otras, llegando a afectar a temas de tanta transcendencia como es el "flujo transfronterizo de datos", donde la falta de unanimidad de criterios entre los Estados y el avance diario de las nuevas tecnologías, particularmente de las telecomunicaciones, hacía peligrar el control sobre los datos personales, pues no todos los Estados reconocían un mínimo de garantías.

Ante esa situación y centrándonos en el marco de la Comunidad Europea, los Estados y estudiosos en la materia, consideraban necesario la urgente elaboración de una norma de ámbito Comunitario que viniera a unificar criterios y a ampliar las pautas marcadas por el Convenio 108. Así se aprueba por el Parlamento Europeo y el Consejo, la tan esperada Directiva 95/46/CE, la que atendiendo a las necesidades señaladas, viene a reconocer en su Considerando 11, que la Directiva precisa y amplía los principios de protección de los derechos y libertades de las personas recogidos en el Convenio 108.

5.1. LA LORTAD COMO NORMA DE LA SEGUNDA GENERACION Y LA INFLUENCIA DEL CONVENIO 108

Como ya hemos indicado, la LORTAD se sitúa entre las Leyes de protección de datos de la Segunda Generación, si bien, al final de la misma, cuando la influencia del Convenio 108 sobre la materia se hacía ya insuficiente, por lo que ya se comenzaba a contemplar la necesidad de aprobar una norma comunitaria que diera respuesta a la realidad de nuestro tiempo, iniciándose un proyecto de directiva en 1990 que no se culminaría hasta la aprobación de la Directiva 95/46/CE.

En palabras de Heredero Higueras[38] la Ley Orgánica en general sigue las pautas marcadas por el Convenio 108, con un sistema de protección cautelar o preventivo basado en un conjunto de Derechos y Principios para hacerlos valer. Aunque en realidad esto sólo es predicable de su Preámbulo, pues como advierte De Julios Campuzano[39], parece como si el Preámbulo y el Articulado de la Ley hubieran sido diseñados por legisladores distintos, ya que si bien el Preámbulo está repleto de buenas intenciones, lo cierto es, que éstas se desvanecen en la parte dispositiva de la Ley, al contemplar un entramado tal de excepciones, que dejan vacío de contenido el conjunto de Derechos y Principios. Reflexión recogida por la profesora Mª. Eugenia Gayo[40], al señalar con relación a las excepciones, que "hacen de las garantías establecidas en la LORTAD para la protección de los ciudadanos, claramente insuficientes, llegando incluso a tener que buscar un sistema de defensa y garantías frente a la propia Ley".

Sin embargo, no son el gran número de excepciones lo más preocupante, sino la ubicación de las mismas, pues éstas se hallan dentro de la regulación que al efecto establece la LORTAD para los Ficheros de Titularidad Pública, como queriendo revestirlos de un blindaje que los haga inmunes a las garantías

■38 HEREDERO HIGUERAS, M: "Ley Orgánica 5/1992..."Op. Cit.

■39 DE JULIOS CAMPUZANO, Alfonso "Letra y Espíritu de la LORTAD: ¿Un problema de coherencia? En Informática y Derecho, núm. 6-7, pág.88, UNED Mérida 1994.

■40 GAYO SANTA CECILIA, Mª Eugenia "Garantías del ciudadano ante la LORTAD: posibles vías de defensa y protección de sus derechos fundamentales", en Informática y Derecho, nº4, pág. 206, UNED-Mérida, 1993.

establecidas con anterioridad para las personas. Preocupación esta, que no es compartida por el Legislador al regular los Ficheros de Titularidad Privada, pues no hace extensible a éstos, las excepciones contempladas en los de carácter público, ni contempla otras excepciones distintas, salvo las peculiaridades que pueda introducir respecto a las distintas clases de ficheros pertenecientes al ámbito privado.

Esta influencia derivada del Convenio 108 también se hace notar cuando la Ley Orgánica, al determinar su objeto, introduce expresamente en su Exposición de Motivos el término de "privacidad", lo que ha dado lugar a interpretaciones de diverso cariz, siendo lo más coherente a nuestro modo de entender, lo señalado por López-Muñiz[41], para el que habría que diferenciar, entre lo que el Preámbulo dice y lo que realmente establece el articulado de la Ley. En este sentido señala que "la referencia a la privacidad de la Exposición de Motivos es superflua e innecesaria" negándose a admitir que la privacidad sea como un aspecto informático de la intimidad.

Pero la confusión introducida por la Exposición de Motivos aún va más allá, al definir la privacidad como una faceta de la persona más amplia que la propia intimidad, por lo que parece dar a entender, que el verdadero objeto de la Ley es la privacidad. Sin embargo, la realidad es muy otra, ya que la referencia a este concepto se limita al Preámbulo, sin que el texto articulado de la Ley haga mención alguna al respecto, refiriéndose en todo momento a la Intimidad, la cual es definida por Georgina Battle[42] como "el derecho que compete a toda persona de tener una esfera reservada en la cual desenvolver su vida sin que la indiscreción ajena tenga acceso a ella".

El art.1 de la LORTAD viene a corroborar lo dicho anteriormente, al determinar su objeto, remitiéndose al mandato constitucional de desarrollo del Art. 18.4 de la CE, con lo que entendemos puede englobar todo un amplio conjunto de Derechos de la persona, que se determinará en función de lo que cada cual quiera entender por lo establecido al final de dicho artículo "... y el

■41 LÓPEZ-MUÑIZ GOÑI, Miguel "La Ley de Tratamiento Automatizado..." ob. cit. Pág. 99.

■42 BATTLE, Georgina "El Derecho a la Intimidad Privada y su Protección". Ed. Alfil. Alcoy. 1972

pleno ejercicio de sus Derechos". A nuestro modo de ver, se trata de una "remisión en blanco" por la que, independientemente de que se preste mayor atención al Derecho a la Intimidad, se deja vía abierta a cualquier tipo de Derechos y Libertades, en particular, a los calificados por el Profesor Sánchez Agesta[43] de derechos individuales de libertad (libertad negativa), sin que tengan por qué estar reñidos los términos intimidad y privacidad, pues para este autor, los derechos de la intimidad personal se identifican por proteger "una esfera inderogable de libertad personal en la que se desenvuelve la racionalidad y la libertad de la vida privada de los individuos", añadiendo que "la vida privada íntima es como la atmósfera misma de la personalidad".

En cuanto a su ámbito de aplicación, la influencia se advierte al considerar el amplio margen que establece el Convenio 108 a fin de permitir a los Estados miembros excluir categorías completas de ficheros ((art. 3.2.a)), así la LORTAD excluye un gran número de ellos (Art. 2.2. y 3)

Las definiciones contempladas en la LORTAD son prácticamente una réplica de las del Convenio, introduciendo la novedad del afectado y del procedimiento de disociación.

En cuanto a los Principios de protección de datos, el artículo 4 de la LORTAD es una reproducción del artículo 5 del Convenio, si bien, contemplado con mayor amplitud e introduciendo como novedad el Derecho de Información y el Consentimiento del afectado, aunque ambos principios quedan prácticamente vacíos de contenido al regular los ficheros de titularidad pública en los que se establece un gran número de excepciones que afectan tanto a principios como a derechos. La regulación establecida para los "datos sensibles", en cuanto a la enumeración de los mismos viene a ser prácticamente idéntica, sin embargo, en este apartado la LORTAD introduce una importante novedad en cuanto a la regulación establecida por el Convenio, en cuanto a la necesidad del consentimiento expreso y por escrito de algunos datos (art. 7.2 y 3). Por lo que respecta a la Seguridad de los datos, la regulación de la LORTAD especifica algo más lo que haya de entenderse por las "medidas de seguridad apropiadas" a que se refiere el Convenio, si bien, se remite a un desarrollo reglamentario, que

■[43] SANCHEZ AGESTA, Luís. "Sistema Político de la Constitución Española de 1978" Segunda Edición, págs.109 y SS. Ed. Editora Nacional, 1981.

efectuado por Real Decreto 1332/1994 no aporta nada nuevo.

En cuanto a los Derechos, la LORTAD no añade nada nuevo a lo establecido en el Convenio, salvo que hace una regulación más pormenorizada. Se establece igualmente la posibilidad de recurso limitándolo a la vía administrativa y a la jurisdicción contenciosa, pudiendo efectuarse la reclamación ante la APD, con posibilidad de obtener una indemnización.

Al igual que la generalidad de las leyes de la segunda generación y por permitirlo en tal sentido el Convenio, como ya hemos señalado, la LORTAD establece una distinción entre Ficheros de titularidad pública y los de titularidad privada. Aprovechando el legislador esta posibilidad, para dotar a los ficheros de titularidad pública de un blindaje especial, mediante la contemplación de un gran número de excepciones y limitaciones de los principios y derechos de los afectados, lo que ha dado lugar a la interposición de cuatro recursos de inconstitucionalidad.

Con relación al Flujo Transfronterizo de Datos, vienen a coincidir en cuanto a la exigencia de un "nivel de protección equivalente o equiparable", en este sentido la LORTAD establece unas excepciones diferentes a las del Convenio.

Tal como recomienda el Convenio, se contempla la creación de una autoridad de control a fin de facilitar la ayuda mutua entre los Estados miembros y velar por el cumplimiento de las garantías establecidas en la ley. Dicha cualidad en recae sobre la Agencia de Protección de Datos (APD) representada por el Director de la misma, al que se le otorgan amplias facultades, pero sin que por ello dejen de surgir dudas sobre su independencia.

5.2. INCIDENCIA DE LA DIRECTIVA 95/46/CE EN LA LORTAD

Como hemos tenido ocasión de comprobar, no son pocos los supuestos en que la Directiva comunitaria incide en la regulación establecida por la LORTAD. La mayoría de los cuales, han quedado perfilados en la exposición hecha hasta el momento, por lo que, en el presente capítulo procederemos a relacionarlas atendiendo, por una parte, a los cambios necesarios para adecuar la LORTAD a lo establecido en la Directiva y, por otra, determinando hasta qué punto dichos cambios van a significar un reforzamiento de la protección de las personas físicas respecto al tratamiento de datos personales y a su libre

circulación. Visto lo cual, haremos un breve análisis de las implicaciones de los cambios relacionados y, en su caso, lo que el reforzamiento de la protección supone con relación a los Recursos de Inconstitucionalidad planteados contra determinados artículos de la LORTAD.

5.2.1. Cambios derivados de la futura transposición

En este apartado distinguiremos entre los cambios que, a nuestro entender, se hacen necesarios en la LORTAD como consecuencia de la transposición de la Directiva, en cuanto afecten a los aspectos generales de la misma y los que afecten a los Principios y Derechos contemplados para garantizar la protección de las personas físicas.

5.2.1.1. Cambios que afectan a aspectos generales de la LORTAD.

En cuanto a su ámbito de aplicación, la Directiva introduce una importante innovación, al hacer referencia tanto al tratamiento automatizado o no de DP contenidos o destinados a ser incluidos en un Fichero, con lo que está admitiendo la aplicación de sus disposiciones a los DP contenidos en ficheros manuales. Por su parte, la LORTAD sólo hace referencia al T.A. de DP y a toda modalidad de uso posterior, incluso no automatizado, pero en tal caso deben estar registrados en soporte físico susceptible T.A. (Art.2).

La Directiva no sólo contempla dentro de su ámbito de aplicación la inclusión del Sonido y la Imagen como DP, sino que además los amplía a todos los aspectos del sector audiovisual, en concreto, el Considerando 14 se refiere a cualquier manipulación sobre datos relativos a las personas físicas constituidos por sonidos e imagen, salvo las exclusiones a que se refieren los Considerandos 16 y 17, las cuales ya quedaron expuestos en su momento. La LORTAD no contempla dichos datos, aunque en su desarrollo reglamentario, el Art. 1.4 del Reglamento 1332/94, incluye como datos de carácter personal toda información, fotográfica, acústica o de cualquier otro tipo, pero, aún con todo, sigue teniendo un carácter más restrictivo que la Directiva, puesto que no los hace extensivos a todo el sector audiovisual.

Dentro del ámbito de aplicación de la Directiva, se excluyen toda una serie de materias, en cuanto el tratamiento de datos personales afecte a actividades no comprendidas en el ámbito de aplicación del Derecho Comunitario, refiriéndose a las previstas en los Tít. V y VI del Tratado de la Unión Europea y,

en concreto, a las que afecten a la seguridad pública, la defensa y la seguridad del Estado, así como las actividades del Estado en materia penal (Art. 3 DC y Considerando 13), también el tratamiento de datos para la salvaguarda del bienestar económico, cuando dicho tratamiento esté relacionado con la seguridad del Estado (Considerando 13), la protección de las personas jurídicas respecto del tratamiento de datos que les conciernen (Considerando 24).

La LORTAD va más allá que la Directiva, ampliando el ámbito de exclusión a las actividades a que se refieren los Arts. 2.2 y 3, las que al no aparecer contempladas dentro de las materias excluídas por la Directiva, salvo las relativas a las actividades de las personas físicas desarrolladas en el ámbito doméstico o familiar (Art. 2.2.b LORTAD), hacen necesaria su reforma en tal sentido.

La Directiva establece como condición indispensable para su aplicación, el hecho de que las actividades del responsable del tratamiento de DP se desenvuelvan dentro del ámbito de aplicación del Derecho Comunitario (Considerando 12), sin que la LORTAD haga referencia alguna al respecto.

La Directiva no contempla la distinción establecida por la Lortad entre Ficheros de titularidad pública y Ficheros de titularidad privada, pero tampoco se deduce de su articulado, que se oponga a ello, siempre y cuando dicha distinción no menoscabe los derechos de las personas físicas, según se deduce el propio espíritu de la norma comunitaria. En este sentido, la diferente regulación entre los ficheros mencionados, sí supone una diferencia de trato, que redunda en perjuicio de los afectados, al contemplarse en los de titularidad pública gran cantidad de excepciones que afectan tanto a los Derechos como a los Principios para hacerlos valer.

La Directiva en su Art. 6 atribuye a los responsables del tratamiento la obligación de garantizar el cumplimiento de los principios generales reconocidos en toda norma de protección de datos, es decir, tratamiento licito y leal, recogida de datos con fines determinados, explícitos y legítimos y que con relación a estos fines los datos sean adecuados, pertinentes y no excesivos, así como exactos y conservados por un periodo no superior al necesario. La LORTAD, en cuanto a este particular, en su art. 9, hace referencia al responsable del fichero, al que atribuye el deber de adoptar las medidas necesarias de seguridad y el deber de secreto. Si bien, podrían equipararse ambas figuras, la atribución de responsabilidad al responsable es mucho más amplia en la Directiva.

De la regulación establecida en al Directiva, parece deducirse, que la exactitud de los datos puede instarla cualquier interesado, mientras que en la LORTAD tal posibilidad sólo es posible de oficio, como expresamente establece su Art. 4.4. Sin embargo, la LORTAD viene a reconocer tal posibilidad a los afectados, si bien dentro de la regulación que al efecto establece, al contemplar los derechos de los interesados, pudiendo instar la rectificación (Art.15 LORTAD).

Para la Directiva no se considera incompatible el tratamiento posterior con los fines determinados, siempre que se utilicen con fines históricos, estadísticos o científicos y se establezcan las garantías adecuadas. En este sentido, la Lortad únicamente se refiere a los DP utilizados con fines históricos.

La Directiva contempla la posibilidad de establecer excepciones y exenciones en cuanto al TDP con fines periodísticos, artísticos o literarios, a fin de conciliar el derecho a la intimidad con las normas que rigen la libertad de expresión (Art.9 DC). La LORTAD no se pronuncia al respecto.

Los Registros de condenas penales, medidas de seguridad e infracciones, habrán de ser llevados bajo el control de los poderes públicos, así como las sanciones administrativas o procesos civiles. En la LORTAD los datos relativos a dichas materias aparecen excluidas del ámbito de aplicación de la misma.

La Sec.4ª del Cap. II, se establece la distinción, entre los datos recabados del propio interesado y cuando no lo han sido. La LORTAD no contempla dicha diferencia.

La Directiva comunitaria, además de contemplar el reforzamiento del tratamiento de los datos especialmente protegidos, introduce una novedad, al hacerlo extensivo a la transmisión de datos dentro de una red. La Lortad no establece regulación alguna al respecto.

La Directiva contempla dentro de su ámbito de aplicación, los supuestos de "las fuentes accesibles al público", además, dado su carácter, otorga a los Estados la posibilidad de dispensarlos, no sólo de la obligación de notificación del art. 18.1, sino también, de la obligación de publicidad a que se refiere el Art. 21.1. La LORTAD, haciendo referencia expresa a estas fuentes en su Art. 11.2.b), los excluye de su ámbito de aplicación (Art.2.2 a) y c)).

La Directiva, al establecer la obligación que atribuye al responsable del fichero de efectuar la notificación recogida en el Art. 18.1, no hace distinción entre ficheros de titularidad pública y los de titularidad privada. Por su parte, la LORTAD contempla la obligación de notificación, en principio, sólo para los Ficheros de titularidad privada, si bien, la regulación posterior del Reglamento, hace extensible dicha obligación a los de titularidad pública, aunque sin determinar que dicha obligación tenga que ser a priori, cosa que se predica de los de titularidad privada. Por otra parte, el procedimiento de notificación a que se refiere la Directiva en su Art. 19.2, es a su vez contemplado por el Reglamento (Art. 17) si bien haciendo la distinción entre Ficheros de titularidad pública y privada.

La Directiva, en cuanto a la Transferencia de DP a países terceros (Cap. IV), se atiene al principio de que los mismos garanticen un "nivel de protección adecuado", determinando en el Art. 25.2. las circunstancias a las que se debe atender a fin de perfilar el carácter adecuado de dicho nivel. La LORTAD en este sentido no recoge pronunciamiento alguno. Por otra parte, las excepciones que establecen una y otra norma respecto al nivel de protección, son distintas (Art.26.1. D.C. y Art. 33 LO).

En cuanto a la regulación de los Códigos tipo, la Lortad circunscribe su aplicación exclusivamente para los Ficheros de titularidad privada, estableciendo la obligatoriedad de su inscripción en el Registro General de Protección de Datos (Art. 31). La regulación establecida por la Directiva en este tema, bajo la denominación de Códigos de Conducta (Art. 27), es más flexible en cuanto no establece la obligación del registro, ni limita su regulación a determinados tipos de ficheros.

La independencia de la Autoridad de Control es contemplada tanto por la Directiva (Art. 28.1), como por la LORTAD (Arts. 34.2 y 35.2), sin embargo, como ya expusimos en su momento y con relación a la regulación que la Lortad establece al efecto, tal independencia queda en entredicho. En este sentido y por lo que respecta a la independencia que la Directiva predica del llamado Grupo de Control (Art. 29.1.) Considerando que el representante español es la APD y que corresponde al Director de la misma la designación de dicho representante (R.D. 156/96), motiva el que también respecto a este órgano y, al menos, en cuanto al miembro designado por nuestro país, haya que dudar igualmente de su independencia.

5.2.1.2. Cambios que afectan a los Principios y Derechos

La LORTAD, ante la exclusividad del Convenio 108 como una fuente Derecho internacional en materia de PDP y a pesar del desfase que arrastraba en el momento de aprobación de la LO, sigue las pautas marcadas por el Convenio 108. La Directiva, viene a reconocer en su Considerando 11, que la misma precisa y amplía los principios de protección de los derechos y libertades de las personas recogidos en el Convenio 108.

La Directiva en su Art. 6.2, atribuye a los responsables del tratamiento la obligación de garantizar el cumplimiento de los principios generales reconocidos en toda norma de protección de datos, es decir, tratamiento licito y leal, recogida de datos con fines determinados, explícitos y legítimos y que con relación a estos fines los datos sean adecuados, pertinentes y no excesivos, así como exactos y conservados por un periodo no superior al necesario. La LORTAD no señala, con carácter general, quién sea la persona u órgano que deba responder ante dicha vulneración.

En cuanto al mantenimiento de la exactitud de los datos, en la Directiva no sólo se considera de que se establezca de oficio, como expresamente establece la LORTAD en su Art. 4.4, sino que por el contrario, cualquier interesado puede instar su actualización. La LORTAD reconoce tal posibilidad a los afectados, si bien dentro de la regulación que al efecto establece al contemplar los derechos de los interesados (Art.15 LORTAD).

Para la Directiva no se considera incompatible el tratamiento posterior con los fines determinados, siempre que se utilicen con fines históricos, estadísticos o científicos y se establezcan las garantías adecuadas. En este sentido, la LORTAD únicamente se refiere a los utilizados con fines históricos.

La Directiva en el art. 8 reconoce como "datos sensibles", el origen racial, étnico, las opiniones políticas, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, así como los datos relativos a la salud o la sexualidad. Esta relación amplia los supuestos de datos sensibles contemplados en la Lortad, aunque no recoja los datos relativos a la religión y creencias a que se refiere esta última en su art. 7, sobre la base de lo establecido en el art. 16 C.E. La Directiva, por otro lado, establece la particularidad de "prohibir" el tratamiento de los mismos, mientras la LORTAD expresa en su art. 7 que "...nadie podrá ser obligado".

La Directiva incluye dentro de su ámbito de aplicación los registros de condenas penales, medidas de seguridad e infracciones, los que habrán de ser llevados bajo el control de los poderes públicos, así como las sanciones administrativas o procesos civiles (art. 8.5). En la LORTAD los datos relativos a infracciones penales quedan excluidas del ámbito de aplicación de la misma (art. 2.3.c).

Contempla la Directiva lo que constituye una novedad en una norma sobre protección de datos, en cuanto a la posibilidad de establecer excepciones y exenciones en cuanto al TDP con fines periodísticos, artísticos o literarios, a fin de conciliar el derecho a la intimidad con las normas que rigen la libertad de expresión (Art.9 DC).

La Directiva en cuanto al Derecho de Acceso, establece una regulación más detallada y menos restrictiva que la recogida en la LORTAD, pues no establece limitación en cuanto a su ejercicio, aunque haga referencia a una "periodicidad razonable", pero sin que se concrete en un periodo de tiempo determinado. Como particularidades, la Directiva contempla dentro del Derecho de Acceso, lo que en la LORTAD aparece regulado de forma independiente como Derechos de Rectificación y Cancelación (Art. 15), añadiendo además la posibilidad del Bloqueo de los datos y contemplando la obligación de notificar haber practicado tales actividades conforme a lo solicitado por el interesado, con una salvedad, que ello no resulte imposible o suponga un esfuerzo desproporcionado.

El Derecho de Oposición del interesado es una novedad introducida por la Directiva (art. 14) aunque acaba por limitarlo a unos cuantos supuestos, a la vez que otorga a los Estados miembros la potestad de dejarlo sin contenido, si en la legislación interna de los mismos, se decide establecer otra cosa. Dentro de la limitada posibilidad de hacer efectivo este Derecho, la Directiva establece la imposibilidad de tratar los datos sobre los que se haya mantenido una oposición justificada.

Si el Derecho de Oposición constituye una novedad, también lo es la regulación más amplia y facilitando la actividad del interesado, que dentro de la regulación que de dicho derecho hace en el párrafo b) del Art. 14, respecto de los datos recabados y que le conciernan destinados a la prospección. Actividad desarrollada por el responsable del tratamiento o por un tercero al que le son

cedidos los datos con dicha finalidad y la cual es contemplada por la Directiva con cierta cautela, obligando a los Estados miembros a establecer las garantías necesarias para garantizar a los interesados su conocimiento.

En cuanto a las Decisiones individuales automatizadas recogidas también dentro de la regulación del Derecho de Oposición en el art. 14, se contempla el reconocimiento al interesado de no verse sometido a una decisión con efectos jurídicos basada en el tratamiento automatizado de datos destinados a evaluar su personalidad, derecho que será garantizado por los Estados miembros, salvo que ello se haya contemplado en un contrato, con ciertas condiciones, o también, que el Estado lo autorice legalmente siempre que establezca medidas que justifiquen el interés legítimo del interesado. La LORTAD al respecto, reconoce tal Derecho en el art. 12 sin que por el contrario establezca excepciones al respecto, por lo que en este sentido es más restrictiva.

La Directiva en su Sec. 9ª, bajo el epígrafe "Notificación" el art. 18 viene a establecer con carácter general la obligación previa de notificar a la Autoridad de Control la intención de realizar un tratamiento de datos personales, atribuyendo nuevamente al responsable del tratamiento o, en su caso, al representante , la responsabilidad de cumplir con tal obligación. Se contempla la posibilidad de suavizar tal obligación, mediante su simplificación o incluso llegando a su omisión, atribuyendo tal posibilidad a los Estados miembros.

Por su parte, la LORTAD contempla la obligación de notificación, en principio, sólo para los Ficheros de titularidad privada, si bien, posteriormente el Reglamento hace extensible dicha obligación a los de titularidad pública, aunque sin determinar que dicha obligación tenga que ser a priori, cosa que se predica de los de titularidad privada. Resulta más amplia la regulación establecida por el Reglamento, si bien éste omite lo relativo a la descripción de las categorías de interesados y de los datos a que se refiere el tratamiento, recogido por la Directiva. El procedimiento de notificación a que se refiere la Directiva en su Art. 19.2, es a su vez contemplado por el Reglamento (Art. 17), sin bien, distinguiendo entre Ficheros de titularidad pública y privada.

5.2.2. Posible refuerzo de la protección de las personas físicas frente al tratamiento de datos personales

Como ya hemos tenido oportunidad de apreciar en la relación efectuada en los dos epígrafes anteriores relativos a las implicaciones de la Directiva en la

LORTAD, son numerosos los cambios que afectan a la LO, lo cual no debe ser motivo de sorpresa, pues tal circunstancia ya es apuntada en el Considerando 11 de la Directiva, al señalar, que los principios de protección de la norma comunitaria precisan y amplían los del Convenio 108, el cual, a su vez, es tomado como modelo por nuestra ley de P.D. al objeto de configurar el esquema de regulación de la materia que constituye su objeto.

Si bien, como decíamos, las modificaciones y novedades introducidas por la Directiva son numerosas, es preciso determinar, si las mismas, en atención a los Principios básicos que procura establecer la norma comunitaria, consistentes en: evitar diferencias entre los Estados miembros (Considerando. 7), sin que ello implique una disminución de la protección (Considerando. 10), lograr un tratamiento equivalente (Considerando 8), proporcionar un margen de maniobra a los Estados miembros que vaya dirigido a mejorar la protección que rige la legislación actual (Considerando 9) y, por último, tener en consideración, que el principio de respeto a la intimidad precisa y amplía el del Convenio 108 (Considerando 11); se corresponden efectivamente con la regulación normativa contemplada en su articulado y, por lo tanto, suponen un auténtico reforzamiento de los Derechos y Principios de protección de las personas físicas o, por el contrario, si realmente lo que se logra con la Directiva es un nuevo marco de regulación en materia de protección de datos, necesario dentro del ámbito de la Comunidad Europea y, por lo tanto, sin que en la práctica se establezcan las suficientes garantías, dada la confrontación que surge entre la protección pretendida y el margen reconocido a los estados miembros para establecer sus propias peculiaridades.

Por lo que hemos tenido oportunidad de analizar hasta el momento, en principio, nos pronunciamos por un teórico reforzamiento de la protección de las personas físicas frente al tratamiento de datos personales, pues en la regulación establecida por la Directiva se pueden observar deficiencias, garantías, margen de maniobra de los Estados miembros, lo que traerá consigo una serie de cambios en las legislaciones internas de los Estados miembros, que hace imprevisible cual sea su resultado final, aunque se puede aventurar, que se establecen mecanismos suficientes para llevar esta tarea a buen puerto.

5.2.3. Recursos de Inconstitucionalidad

Partiendo del planteamiento realizado por Martín-Casallo[44], la Directiva de por sí, viene a dejar vacío de contenido alguno de los artículos afectados por los Recursos de Inconstitucionalidad planteados contra la LORTAD, en concreto, el art. 19, por cuanto, si bien la Directiva no recoge expresamente una regulación que diferencie entre ficheros públicos y privados (en este sentido la única diferenciación apreciada, a juicio del autor, es la que hace referencia a la regulación de los Ficheros, en cuanto los datos sean recabados directamente del interesado y los obtenidos de forma distinta), lo cierto es, que tampoco se opone a dicha distinción, sin embargo, lo que si se deduce de su espíritu, es que dicha diferenciación no debe repercutir en una minoración de los Derechos reconocidos al interesado, motivo por el cual, se impone la derogación total de dicho artículo y en consecuencia, también del Art. 11.2.e) del mismo texto legal.

Siguiendo la línea argumental del Director de la APD, entendemos, que la Directiva no sólo da lugar a derogar el Art. 19 y por ende el Art. 11.2.e) de la LORTAD, sino que además, a nuestro modo de ver, puede hacerse extensible a todos los artículos contemplados en la regulación establecida en la Lortad para los Ficheros de titularidad pública (Capítulos. I del Título IV) que contengan excepciones a los Derechos y Principios de los afectados, excepciones que, sin embargo, no son contempladas en los Ficheros de titularidad privada. Por lo tanto, dada la diferente regulación de dichos ficheros y la ubicación de las excepciones, hechos estos, que suponen un detrimento de los Derechos de los afectados y de los Principios para hacerlos valer, así como una clasificación de ficheros basada en un tratamiento desigual, implica que la regulación de la LORTAD entre en conflicto con lo establecido en la Directiva, en cuanto que la diferente regulación de ficheros no puede suponer un menoscabo de los derechos de los afectados. Con ello no queremos decir que la Directiva no contemple excepciones a los Derechos de los interesados, ni que las excepciones contempladas en la Lortad sean todas inconstitucionales, sino que, en atención a lo expuesto, algunas pueden serlo, dada su ubicación en la LORTAD.

■[44] MARTIN CASALLO-LOPEZ, Juan José "Implicaciones sobre la Directiva ..." ob. cit. págs. 5 y 6.

Así las cosas y de conformidad con lo establecido en el Art. 93 en relación con el 18.4 de la Constitución y, teniendo en cuenta, que la Directiva es una norma posterior a la LORTAD, por lo que dado su rango de Norma Comunitaria y lo establecido en su Art. 32.1, se impone la necesidad de reformar la LORTAD en este sentido. En consecuencia, además de dejar vacío de contenido los Recursos de Inconstitucionalidad planteados contra el Art. 19, por extensión, habría que predicar lo mismo de los Arts. 20.3, 22.1 y 22.2 de la LORTAD, dada la necesaria derogación tácita que impone la Directiva, así como del Art. 21.1 y 2.I, independientemente de que éste no esté afectado directamente por alguno de los cuatro Recursos de Inconstitucionalidad planteados.

6. PLAZOS E IMPLICACIONES DE LA NO TRANSPOSICION DE LA DIRECTIVA

6.0. INTRODUCCION

La actividad desarrollada por los Estados miembros a fin de transponer la Directiva a sus Ordenamientos internos, como ya hemos dicho, está resultando muy escasa hasta la fecha, siendo Bélgica de los pocos países de los Estados de la CE que realmente han iniciado una actividad encaminada a la transposición de la Directiva a su Derecho interno, motivo por el que ha sido objeto de estudio por algunos autores, siendo interesante resaltar el comentario del prof. Dr. J. Dumortier y Ana M. Alonso[45], en un trabajo conjunto de análisis de dicha transposición:

"Merece la pena tener en cuenta el ejemplo belga, que muestra la intención del legislador de aprovechar la oportunidad de la transposición de la directiva para reformar en profundidad y mejorar en la medida de lo posible la actual ley de protección de datos".

En dicho comentario se aprecia la importancia que por estos autores se

■[45] Dr. J. DUMORTIER y ALONSO BLAS, Ana María "La Transposición de la Directiva de protección de datos en Bélgica" Actualidad Informática, pág. 11, Aranzadi, núm. 20, julio de 1996.

da a la necesidad de actuar sin dilaciones en el mismo sentido que los legisladores belgas, de ahí la motivación que intentan insuflar al resto de Estados miembros para que no demoren en exceso tal obligación.

Si el caso belga es un ejemplo a seguir, independientemente de lo acertado de la actuación de sus legisladores, en cuanto a la interpretación que de la Directiva hagan, a fin de amoldar su ley de PD a la norma comunitaria; llama poderosamente la atención el caso de Italia, en el que careciendo de una ley en la materia, no haya aprovechado la reciente Ley de 31 de diciembre de 1996, nº 675[46], a fin de transponer la Directiva a su Derecho interno, pues con una primera lectura de la misma, ya es suficiente para apreciar que su finalidad es la de cubrir la laguna existente en la materia durante tantos años en su Ordenamiento Jurídico, ya que a lo largo de su articulado no hace referencia alguna a la Directiva 95/46/CE. Incluso su título "Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali" no parece ceñirse a las directrices marcadas por la Directiva, la que había sido publicada un año antes a la ley objeto de comentario, ya que en dicho título se hace referencia a la tutela de la persona y de "otros sujetos", expresión esta última que parece sugerir la referencia a otras personas, que no pueden ser otras que las jurídicas, cuando es bien sabido, que la norma comunitaria exclusivamente contempla como objeto de regulación a las personas físicas.

6.1. PLAZOS PARA LA TRANSPOSICION DE LA DIRECTIVA

En las Disposiciones Finales de la Directiva y en concreto en el art. 32 de la misma, se establecen los plazos de que disponen los Estados miembros a fin de transponer la Directiva a sus legislaciones internas, estableciendo a este respecto un plazo general y dos para supuestos concretos. En tal sentido el apartado 1 de dicho artículo establece con carácter general el plazo de tres años a partir de su adopción, para la aprobación de la norma que al efecto establezcan. Ampliando dicho plazo para el supuesto de los tratamientos que ya se hayan iniciado a la entrada en vigor de la Directiva a tres años desde la adopción de la norma interna aprobada en aplicación de la Directiva. Por último estable el plazo de doce años para el tratamiento de datos que ya se encuentre incluidos en ficheros manuales.

■[46] Vid pág. 3, en el apartado 1. Introducción. Martín-Casallo, LOPEZ "Implicaciones de la Directiva sobre..."Op. cit. pág. 6.

En el punto 4 se recoge la obligación de los Estados miembros de comunicar a la Comisión el texto de las disposiciones de Derecho interno en el ámbito regulado por la Directiva y el art. 33 la obligación de la Comisión de informar en el plazo de tres años desde la adopción de la Directiva sobre la aplicación de la misma.

6.2. IMPLICACIONES DE LA NO TRANSPOSICION

La cuestión básica que se nos plantea, es determinar si la Directiva como norma comunitaria tiene eficacia directa en el Derecho español o por el contrario necesita de alguna apostilla para hacerla valer.

En principio para aclarar la cuestión planteada, tomaremos como referencia la Sentencia de 24 de abril de 1990 del Tribunal Supremo, en la que se trata de especificar las implicaciones que para España tiene el hecho de someterse a la potestad normativa de las Instituciones comunitarias, como consecuencia de su adhesión al Tratado de la CEE.

En dicha Sentencia, entre otros temas, se hace referencia a la primacía del Derecho Comunitario sobre el Derecho interno, como consecuencia de la cesión de soberanía que se produce, desde el momento en que España ratifica dicho Tratado, lo que resulta incuestionable en virtud de lo establecido en el art. 93 de la Constitución Española.

Tema más complicado de abordar, es el de determinar si tanto el efecto directo como la aplicabilidad directa son predicables de las Directivas. En este sentido, conviene en principio, distinguir entre uno y otro concepto, pues aunque en la práctica, como reconoce la propia Sentencia se tiende a confundirlos, entendemos de gran importancia su distinción por conllevar efectos distintos. Así siguiente la Affaire 9/70, Arrêt Du de 6 de octubre de 1970, mientras que la aplicabilidad directa hace referencia a la no necesidad de un acto de Derecho interno para conferir valor a una norma comunitaria, lo cual sólo es predicable de los Reglamentos y no de las Directivas, las cuales en todo caso necesitan de una norma del Estado miembro para su incorporación al Derecho interno; por su parte el efecto directo hace referencia a la posibilidad de hacer valer una norma de Derecho comunitario a pesar de la inexistencia de una norma de Derecho interno de ejecución.

En cuanto a la aplicabilidad directa, como acabamos de decir, sólo es predicable de los Reglamentos. La cuestión es determinar si el efecto directo es igualmente predicable exclusivamente de los Reglamentos, cualquiera que este sea, o también se puede hacer extensible a las Directivas. Siguiendo la Sentencia del TS, hay que entender que el efecto directo sólo es predicable de los Reglamentos y no de todos, sino de aquellos a los que denomina "self executing" o jurídicamente perfectos, es decir, que no necesitan ser complementados para definir su alcance. En cuanto a las Directivas, en ningún caso cabe atribuirle efecto directo, lo que supone que en ningún momento puedan ser esgrimidas por los interesados para hacer valer los derechos que deriven de dichas normas, mientras no exista una norma de ejecución directa.

No obstante lo dicho, la realidad es muy distinta, pues no faltan interpretaciones extensivas por parte del TJCE al atribuir efecto directo en ciertos supuestos a las Directivas, entendiendo el TS en Stc. de 23-noviembre-1990, que dichas interpretaciones son permitidas sólo cuando el Estado miembro en cuestión no hubiera introducido en su ordenamiento jurídico la regulación a la que estaba obligado.

Por lo expuesto, si transcurrido el plazo general de tres años o el determinado para los otros supuestos concretos, sin que se haya incorporado la Directiva al Derecho interno de cada Estado miembro, en virtud de la doctrina sentada por el TJCE y, en el caso concreto español, en consideración con la interpretación en tal sentido hecha en la Stc. de 23-noviembre-1990, cabe la posibilidad de compeler al Estado miembro a su incorporación, bien por instarlo en tal sentido cualquier particular al que interese hacer valer su derecho mediante la aplicación de la regulación establecida en la Directiva o también, porque el juez lo aprecie de oficio.

7. CONCLUSIONES

Del estudio realizado resulta evidente que la Directiva 95/46/CE establece una regulación que viene a cubrir en términos generales la necesidad de disponer en el ámbito europeo comunitario de una norma que responda a los problemas creados por la confluencia de distintos factores, entre los que cabe destacar, la insuficiencia del Convenio 108 como único instrumento de Derecho Internacional en materia de protección de datos, las diferencias surgidas entre los Estados miembros, especialmente en lo relativo a la transferencia internacional de datos, los distintos niveles de protección de unos

estados con respecto a otros con relación a los derechos y libertades de las personas físicas, especialmente su intimidad, la falta de normativa de algunos de ellos. Todo lo cual, viene agravado por el espectacular desarrollo de las nuevas tecnologías, que han determinado el que se hable de una nueva época con expresiones como "Sociedad de la Información" o "Sociedad de las autopistas de la Información".

No obstante la concienzuda regulación establecida por los legisladores comunitarios, hay que tener en cuenta que en materia de protección de datos confluyen una serie de intereses, tales como la necesidad de no obstaculizar el desarrollo de las técnicas de telecomunicaciones e información, dadas las ventajas que estas aportan a la sociedad actual, por otra parte, se encuentran los intereses de los Estados miembros, interesados en no ceder en exceso su soberanía y, por último, los intereses de las personas físicas como principales afectados en la materia, puesto que son sus datos los que implican la necesidad de una regulación. Intereses todos ellos, a los que la Directiva intenta dar respuesta procurando un equilibrio entre los mismos, prohibiendo y permitiendo en cada supuesto objeto de regulación.

Efectivamente la Directiva tiene en cuenta todos esos intereses en juego los que contempla al establecer sus Principios en los Considerandos 7 a 11. La cuestión es determinar si el equilibrio pretendido será efectivo en la práctica. Es evidente que mientras no se transponga a los Estados miembros y se vean los efectos que tal regulación produce, no nos podremos pronunciar con certeza sobre la efectividad de la Directiva. Sin embargo, a lo largo de este estudio se han señalado lo que por nuestra parte hemos calificado de ciertas deficiencias, que ya han sido caballo de batalla en las legislaciones anteriores sobre protección de datos. Nos referimos a supuestos como el de la contemplación de unos Derechos y Principios, para los que seguidamente se establecen unas limitaciones, por medio de acudir a excepciones, garantías no definidas o a conceptos jurídicos indeterminados, sembrando la incertidumbre de si en la práctica, dichos Derechos y Principios, no quedarán vacíos de contenido. Por otra parte, el amplio margen de maniobra atribuido a los Estados miembros, no deja de ser un riesgo de cara a procurar una regulación homogénea entre los mismos.

A los inconvenientes anteriormente señalados, la Directiva viene a dar respuesta con la personalización de la responsabilidad que pueda surgir del tratamiento en el Responsable del mismo o en su representante. También y

fundamentalmente con la creación de una serie de órganos como son la Autoridad de control, el Grupo de protección y el Consejo, los que en conjunto y en las parcelas de actuación que se les asigna, velarán porque la normativa comunitaria se cumpla en todos sus extremos. No obstante, independientemente de la importancia que realmente tienen estos órganos en el conjunto de la Directiva, nos surge la duda de si la independencia que de ellos se predica realmente es efectiva, porque de no ser así, estando destinados a ser los principales garantes del cumplimiento de la Directiva, a nuestro entender, este aspecto sería el primer fracaso. En este sentido, cabe decir que para la integración del Grupo de protección, por parte de nuestro país se ha designado a la Agencia de Protección de Datos y en concreto a su representante, el Director, para designar la persona que nos represente, siendo que la independencia del Director está en entredicho dada su dependencia del Gobierno, en cuanto a su nombramiento, cese y relaciones con el mismo. Motivo por el que ya surgen dudas fundadas de la efectividad de tales órganos.

En otro orden de cosas, dichos Organos deben velar porque se definan y concreten en la práctica unas medidas de seguridad, al menos las imprescindibles, a fin de lograr una seguridad efectiva. Asimismo, para que las obligaciones atribuidas al Responsable del tratamiento, a las que tanto se hace referencia en la Directiva, no sean una mera ficción, es necesario estructurar las medidas que hagan posible un seguimiento pormenorizado de las actividades que éstos desarrollen.

Entendemos que es importante potenciar los Códigos de Conducta, por ser la forma mas flexible de asegurar un compromiso por parte del que constituye el mayor sector que puede realmente trastocar la protección pretendida, es decir las asociaciones profesionales y demás organizaciones. Hasta la fecha, su efectividad ha sido bastante pobre, por no decir nula, si entendemos a la experiencia en nuestro país y ello a pesar de la obligación de registro y dictamen favorable de la APD, la cual no es contemplada en la Directiva.

Por lo que a la LORTAD se refiere, decir, que la Directiva implica una reforma de la LORTAD en una serie de aspectos que ya hemos tenido oportunidad de relacionar, incidiendo asimismo en los recursos de inconstitucionalidad planteados contra la misma, de tal manera que muchos de los artículos impugnados quedan vacíos de contenido dada la contradicción que suponen con relación a la regulación establecida por la Directiva, no tanto

por las limitaciones que contemplan, las cuales, sí es cierto que en algunos aspectos chocan frontalmente con lo establecido en la norma comunitaria, sino, desde nuestro punto de vista, principalmente por la ubicación de las mismas, al suponer un menoscabo de los derechos de los interesados. En cuanto al ámbito de aplicación, la Lortad debe extenderse a los supuestos a que se refiere la Directiva y que ya apuntamos en su momento
Asimismo, consideramos que el legislador español debe aprovechar la oportunidad que le brinda la Directiva 95/46/CE y emprender una reforma con detenimiento de todos aquellos aspectos que de alguna manera dejan alguna sombra de dudas, como puede ser, además de los indicados anteriormente, el caso de la independencia del Director de la Agencia de Protección de Datos, así como el excesivo proteccionismo que brinda a los Ficheros de titularidad pública con el consiguiente menoscabo de los mecanismos de protección establecidos en defensa de las personas físicas.

Terminar diciendo, que en principio, lo importante es que se ha salvado una grave deficiencia, mediante la creación de una norma, que tiene unas pretensiones dignas de ser tenidas en cuenta, aunque su efectividad en el futuro esté por determinar, dada la confluencia de factores, algunos de ellos en continuo cambio, pero que el esfuerzo por lograr el equilibrio necesario entre ellos ha quedado plasmado en la Directiva 95/46/CE.

8. FUENTES Y BIBLIOGRAFIA

8.1. FUENTES

-ACUERDO DE SCHENGEN, firmado por los Estados del Benelux, R.F.A. y la R. Francesa el 14 de junio de 1985 en Schengen.

-AGENCIA DE PROTECCION DE DATOS "Análisis y valoración de diversos problemas de la protección de datos a escala Nacional Problemas relativos a las Medidas de Seguridad " vid. Pág. 189 y SS. de la Memoria de 1995.

-AGENCIA DE PROTECCION DE DATOS "La seguridad en el tratamiento de datos personales" vid. pág. 62 y ss. de la Memoria de 1994.

-AGENCIA DE PROTECCION DE DATOS "Análisis de las tendencias Legislativas, Jurisprudenciales y Doctrinales de los distintos Países en materia de Protección de Datos -España-" vid Págs. 175 y 181 y SS de las Memorias de 1995 y 1996.

-AGENCIA DE PROTECCION DE DATOS, "Códigos tipo" págs. 89 ,141 y 179 de las Memorias de 1994, 1995 y 1996 (respectivamente)

-BOLETIN DE JURISPRUDENCIA CONSTITUCIONAL (BJC), IV, Jurisprudencia Constitucional Extranjera, Tribunal Constitucional Alemán, Sentencia de 15 de diciembre de 1983. Ley del Censo. Derecho a la Personalidad y a la Dignidad Humana.

-CONSTITUCION ESPAÑOLA de 1978, B.O.E.

-CONVENIO 108 DEL CONSEJO DE EUROPA, de 28 de enero de 1981, para la protección de las personas con respecto al tratamiento de datos de carácter personal.

-CONVENIO DE APLICACIÓN DEL ACUERDO DE SCHENGEN, firmado el 19 de junio de 1990.

-DIRECTIVA 95/46/CE, del Parlamento Europeo y del Consejo de Europa, 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. Boletín Informativo del Ministerio de Justicia núm. 1765.

-GACETA OFICIAL DE LA REPUBLICA ITALIANA de 8 de enero de 1997, se publica la "Ley de 31 de diciembre de 1996, nº 675 "Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali". Así como la Ley de 31 diciembre 1996, n. 676 por la que "Delega al Governo in meteria di tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali".

-LEY ORGANICA 5/92, de 29 de octubre de Regulación del Tratamiento Automatizado de los Datos del Carácter Personal. Suplemento al Boletín de Información del Ministerio de Justicia al núm. 1688. Noviembre 1993.

-REAL DECRETO 428/1993, de 26 de marzo, por el que se aprueba el Estatuto de la Agencia de Protección de Datos.

-REGLAMENTO 1332/94, de 20 de junio, por el que se desarrollan determinados aspectos de la Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal.

-TRIBUNAL CONSTITUCIONAL IªS, 254/1993 de 20 de julio.- Ponente: Sr. García-Mon y González -Regueral.) LA LEY, 1994-1, 152 (2282-TC 8.2. BIBLIOGRAFIA

-BATTLE, Georgina "El Derecho a la Intimidad Privada y su Protección". Ed. Alfil. Alcoy. 1972

-CARRASCOSA LOPEZ, Valentín "La LORTAD: Una necesidad en el panorama Legislativo Español", en Informática y Derecho núm. 6-7 UNED, Mérida 1994.

-DE JULIOS CAMPUZANO, Alfonso "Letra y Espíritu de la LORTAD: ¿Un problema de coherencia? en Informática y Derecho, núm. 6-7 UNED Mérida 1994.

-DRESNER, Stewart H. "Panorama de la Legislación Europea sobre Trotección de Datos Personales" Informática y Derecho 6-7, La Protección de los Datos Personales, UNED, Mérida 1994.

-DUMORTIER J. y ALONSO BLAS, Ana María "La Transposición de la Directiva de Protección de Datos en Bélgica" págs. 8 a 11 de Actualidad Informática Aranzadi , núm. 20, Ed. ARANZADI, Madrid julio de 1996

-GAYO SANTA CECILIA, Mª Eugenia "Garantías del ciudadano ante la LORTAD: posibles vías de defensa y protección de sus derechos fundamentales", en Informática y Derecho, nº4, UNED-Mérida, 1993.

-HEREDERO HIGUERAS, M: "Ley Orgánica 5/1992, de 29 de octubre, de regulación del Tratamiento Automatizado de Datos de Carácter Personal" Boletín Informativo del Ministerio de Justicia, núm. 1669, Madrid 1993

-LAZPITA GURTUBAY, María "Análisis Comparado de las Legislaciones sobre Protección de Datos de los Estados Miembros de la Comunidad Europea" Informática y Derecho 6-7, La Protección de Datos Personales, pág. 413 UNED, Centro Regional de Extremadura, Mérida 1994

-LOPEZ-MUÑIZ GOÑI, Miguel. "La Ley de Tratamiento Automatizado de los Datos de Carácter Personal" en Informática y Derecho, núm. 6-7 UNED Mérida 1994.

-MARCHENA GOMEZ, Manuel "Intimidad Informática: La Protección Jurisdiccional del Habeas Data" Boletín Informativo del Ministerio de Justicia, núm. 1768, Madrid 1996.

-MARTIN-CASALLO LOPEZ, Juan José. "Discurso Apertura" de la Conferencia sobre Seguridad, Privacidad y Protección de Datos. Agencia de Protección de Datos, celebrada en Madrid del 30 nov. al 1 dic. de 1996.

-MARTIN CASALLO-LOPEZ, Juan José. "Implicaciones sobre la Directiva de protección de datos en la normativa española "Actualidad Informática Aranzadi, nº 20 julio de 1996.

-MATHEWS, Steve "Protección de Datos ¿Proceden Nuevos Estándares de Seguridad?" Conferencia sobre Seguridad, Privacidad y Protección de Datos, Agencia de Protección de Datos, celebrada en Madrid del 30 nov. al 1 dic. de 1996.

-MENSBRUGGHE, Patricia van der "Flujos transfronterizos de datos en la Directiva 95/46 de las Comunidades Europeas" Actualidad Informática Aranzadi , nº 20 pág. 14, Ed. ARANZADI, Madrid julio de 1996.

-MILLE, Antonio "Informaciones de caráter personal Derecho Comparado y prospectiva" Informática y Derecho 12 a 15, II Congreso Internacional de Informática y Derecho, Actas (Vol. II), UNED, Mérida 1996.

- PEREZ LUÑO, Antonio Enrique "La LORTAD: Entre las luces y las sombras", en Informática y Derecho, núm. 6-7 UNED, Mérida 1994.

-SANCHEZ AGESTA, LUIS "Sistema Político de la Constitución Española de 1978" Segunda Edición, págs.109 y ss Ed. Editora Nacional, 1981.

- SANCHEZ BRAVO, Alvaro "La Protección de los Datos Personales en la Europa de Schengen" Informática y Derecho núms. 12 al 15, Segundo Congreso Internacional, Actas (Volumen II) pág. 1424, UNED, Centro Regional de Extremadura Mérida 1996.

-DE LA SERNA BILBAO, María Nieves "La Agencia de Protección de Datos Española: con especial referencia a su característica de independencia" Actualidad Informática Aranzadi, núm. 22, enero 1997, Ed. ARANZADI.

-VELAZQUEZ BAUTISTA, Rafael "Protección Jurídica de Datos Personales Automatizados", Ed. COLEX, Madrid 1993.

Tras los pasos de la Seguridad perdida. Delitos Informáticos

GUILLERMO CONSENTINO
JOSE ALBERTO GARCIA
DANIEL OMAR TEJERO
NESTOR FABIAN TEJERO

Universidad de San Juan Bosco de la Patagonia (ARGENTINA)

PROLOGO

Cuando en nuestras relaciones cotidianas observamos con agobiante malestar que la inseguridad se ha instalado en todos los niveles de nuestra sociedad y el hecho de que un mundo nuevo emerge a través de la informática, nos da la idea que en algunos aspectos lograremos, al menos como un anhelo, el restablecimiento de esa tan vapuleada seguridad.

¿En virtud de qué manifestamos o se nos representa espontáneamente ello?. Creemos que la generación y utilización social de nuevos conocimientos, artes y técnicas ha implicado, conforme indica la experiencia histórica, transformaciones culturales en las actividades productivas y, consecuentemente, en las formas de relación y organización social.

Los problemas que las innovaciones tecnológicas introducen en la sociedad, conforman una temática que, considerada desde una perspectiva político-criminal, entendida como modelo de orientación para el derecho penal futuro y marco de interpretación de la dogmática del orden jurídico-penal vigente, permiten señalar la existencia de dos aspectos básicos, constituídos por:

- Los efectos de la concentración económica;

- La necesidad de que los elementos típicos (descriptivos y normativos) se expresen a los efectos de respetar los principios de legalidad y tipicidad, en tipos

que -en tanto descripción de la conducta prohibida por la norma- permitan realizar la adecuación típica de las acciones prohibidas con precisión.

Concentración económica: la tendencia a la concentración económica, expresada por medio del accionar de empresas multinacionales, pone de relieve la contradicción de intereses entre países con distintos niveles de desarrollo. La evolución del comercio mundial evidencia una creciente especialización intra-tecnológico-industrial entre los países desarrollados y en desarrollo, en lo que respecta al comercio de manufacturas, servicios y tecnologías.

En este plano se comprueba la presencia de una criminalidad, no reprimida penalmente, que, asentada en el abuso del poder económico y político, trasciende con su actuación los límites geográficos de los Estados, afectando los intereses y derechos económicos de los países en desarrollo.

Sobre esta situación el profesor Tiedemann ha señalado que "las investigaciones criminológicas más recientes, especialmente en los países angloamericanos y escandinavos, han demostrado, en base a estudios sobre la génesis normativa, que la no tipificación de ciertas conductas puede deberse a la influencia ejercida sobre los órganos legislativos por poderosos grupos de personas interesadas. En dichas situaciones, quien tiene ese poder se encuentra jurídicamente (por encima del alcance de la ley) -para utilizar una expresión acuñada en el VI Congreso de las Naciones Unidas sobre Prevención del delito y tratamiento del delincuente (Caracas, 1980)- en relación con el abuso del poder, especialmente por parte de las empresas multinacionales o transnacionales".

Cuestiones de tipicidad: la técnica ha constituído también, en forma tradicional, un instrumento y objeto de acciones que afectan intereses que la comunidad procura tutelar. En este sentido, la experiencia indica que la utilización de nuevas modalidades delictivas suelen anticiparse a las previsiones penales, que aparecen así como desactualizadas, imposibilitadas de operar como mecanismo de prevención general -impidiendo que la pena opere como inhibidor de ciertos comportamientos frente a la sociedad- o de represión penal de conductas.

Sin embargo, como indica el profesor Zaffaroni, el nivel de riesgo social derivado de situaciones como la contaminación ambiental, el despliegue nuclear, el volumen financiero de la transferencia electrónica de fondos y la centralización de datos personales, por mencionar algunos aspectos del problema, obliga a acentuar los trabajos interdisciplinarios a los efectos de poder establecer un

sistema de prevención eficiente, que avance sobre el desfase normativo y el recurrente criterio de pretender resolver cualquier tipo de conflicto social mediante formulaciones típico-penales abiertas, que independientemente de atentar contra la seguridad jurídica, sólo contribuyen a evidenciar, más allá de la existencia de una referencia legal, la ineficacia del sistema de justicia penal en estos supuestos.

Efectuado este escueto análisis, sobre lo que creemos la implantación del problema de la inseguridad en que actualmente vivimos, podemos afirmar a modo de hipótesis que la instauración de la Informática en los distintos niveles de nuestra sociedad nos llevará a reencontrarnos con la seguridad social, económica, política, educacional, judicial, etc.

Es nuestro agradecimiento a esta cátedra que nos permite investigar un tema tan profundo y lleno de controversias, lo que nos llevó a efectuar esta investigación y ofrecer nuestro humilde aporte, plasmado en esta monografía.

EVOLUCION Y REPERCUSIONES SOCIALES DE LA INFORMATICA

La informática, o sea la "ciencia del tratamiento lógico y automático de la información mediante ordenador", tuvo, como es sabido, en los últimos años, sobre todo tras la aparición de la telemática y los microordenadores, un desarrollo enorme y desempeña hoy un papel extremadamente importante en el campo social y económico, tanto a nivel individual como colectivo.

En verdad, faltan datos precisos y unívocos acerca del número de ordenadores que funcionan actualmente en todo el mundo, si bien la proliferación de sistemas cada vez más sofisticados y complejos es tanta, que existe el temor de que se forme una verdadera "telaraña informática" en torno al individuo y a la sociedad misma.

A los efectos de una primera orientación, las áreas afectadas por la informatización pueden dividirse en: sector del registro civil, fiscal, de la previsión social, judicial y policial, de la educación y la instrucción, de la defensa nacional, comercial y bancario, de los transportes y seguros, y de las organizaciones profesionales.

ACTUALIDAD DE LOS BIENES INCORPORALES

Materia objeto de examen: en lo que concierne a las cosas materiales, muebles o inmuebles, es respecto de ellas que se ha desenvuelto principalmente la doctrina y la jurisprudencia. Y, comprendidos en la concepción amplia del vocablo "propiedad" los bienes inmateriales, la propiedad intelectual e industrial.

Es decir, no es que los bienes inmateriales o incorporales no hayan sido considerados en la esfera de los derechos patrimoniales, pero es también cierto que ha sido en las últimas décadas que su importancia acreció, exigiendo su examen más detenido.

Ello así, porque el avance de la ciencia y de la técnica ha producido distintas manifestaciones y logros, a los que según algunas orientaciones son aplicables las reglamentaciones de las mencionadas propiedades, intelectual o industrial, o bien son necesarias nuevas reglamentaciones jurídicas que permitan acompañar el progreso experimentado.

Preexistencia y continuidad de la calificación de los bienes incorporales o inmateriales: según la sucinta relación antecedente, es apreciable que los bienes inmateriales o incorporales no estaban excluidos en el cuadro de los derechos patrimoniales.

Ya tales bienes estaban definidos en el derecho romano, puestos de relieve en la obra de Ginossar, en la cual desarrolla su concepción sobre una nueva clasificación de los derechos patrimoniales.

En lo pertinente, adecuado a nuestro tema, resumiendo su idea, creemos que los romanos, guiados por su admirable instinto jurídico, consideraron que la propiedad difiere de los demás derechos, pues ella absorbe el bien sobre el cual recae, por lo que resulta lógico colocar en un mismo pie entre las cosas que forman el activo de un patrimonio de una parte, las cosas corporales (tierras, esclavos, ropas, oro, plata, etc.); y de otra parte, las cosas incorporales, es decir, los derechos, especialmente las obligaciones, y los derechos de obligación de crédito.

Aubry y Rau sustentaron que "el término propiedad ha sido extendido a las cosas incorporales y comprendido en él a la propiedad literaria, artística e industrial".

En este orden de consideraciones, en la obra de Planiol-Ripert se advierte una denominación significativa de los derechos sobre las cosas incorporales, pues se los designa como propiedades incorporales.

Si recordamos la proposición de Ginossar respecto de una nueva clasificación de los derechos patrimoniales y tenemos presente el concepto de Savatier de que "todo derecho, aún sobre una cosa concreta es incorporal, no existiendo sino bienes incorporales", estimamos que ellos encierran principios jurídicos que permiten zafar la caracterización del derecho de propiedad tal como se lo limita a las cosas corporales o materiales.

Derecho comparado: En los códigos y en las legislaciones latinoamericanas y europeas, los derechos de autor o de inventor están caracterizados como derechos de propiedad o como derechos de autor o de inventor.

Valdés Otero expone -en relación con la ley del Uruguay- su criterio favorable a la denominación de "derechos de autor", incorporada por el legislador a la ley respectiva.

"Creemos -sostiene- ajustada la denominación de derechos de autor que ha recibido nuestra ley, pues, a diferencia de los derechos intelectuales, que también se encuentra ampliamente difundida en el derecho comparado, no compromete una definición en el problema de la naturaleza jurídica. En la doctrina brasileña se sostiene que el derecho de autor es una propiedad inmaterial.

Rojina Villegas, en la doctrina mejicana, estima que "queda definida la naturaleza de este derecho de autor o propiedad intelectual, resolviendo como primer punto, que se trata de un derecho real, y no personal. Es decir, que se trata de un derecho patrimonial de naturaleza real.

Estima Puig Brutau que el calificativo de propiedades intelectuales e industriales constituye un recurso del razonamiento jurídico para encajar determinados intereses en el sector jurídico donde podían hallar protección, cual es el de los derechos de propiedad; asimismo, que en la reelaboración doctrinal, "el calificativo -expresa- queda a veces sustituido por el de propiedad sobre bienes inmateriales. La perduración del concepto de propiedad garantiza la continuidad de unos efectos, y el nuevo calificativo señala el hecho indudable de que la equiparación es sumamente artificiosa".

Proyección de las formulaciones precedentes: los derechos del autor y del inventor quedan, pues, encuadrados en el concepto de "propiedad", sobre la base de su extensión a los bienes, cosas corporales o materiales, independientemente de la necesidad de determinación de la naturaleza jurídica de los bienes inmateriales.

Estimamos que prevalece la noción de derecho independientemente de la corporeidad o incorporeidad del resultado de la creación o de la actividad inventiva. En cuanto a la conservación de la expresión "propiedad intelectual", estimamos que se subordina a los preceptos constitucionales según que ellos determinen o no ese concepto.

Pero ello no empece a sustentar la expresión de derechos intelectuales o industriales, cuyo objeto puede ser todo cuanto puede resultar de la creación del hombre (patentes de invención, marcas, modelos de utilidad, know-how, software y productos obtenidos por esos procedimientos) reconocidos como derecho subjetivo por el ordenamiento normativo.

RELACIONES ENTRE LA TECNOLOGIA Y EL DERECHO

Las innovaciones y las invenciones técnicas han sugerido la creación de nuevos derechos, y, a menudo, de derechos específicos. En ciertos casos, se impuso al Legislador la necesidad de una nueva reglamentación; así ocurrió con la invención del automóvil, que impuso una cantidad de normas de policía y de circulación, codificadas hoy en día en un "código de la circulación".

Hasta ahora, sin embargo, las relaciones entre la informática y las reglas del derecho son ambiguas.

Sea como fuere, desde hace ya un tiempo se viene hablando, en varios países -sobre todo en Alemania, España, Estados Unidos, Francia y Noruega-, de un "derecho de la informática", definido recientemente como "conjunto de las normas, de las instituciones y de los principios aplicables a los hechos, actos y actividades relacionadas con el tratamiento de la información y con la informática". Se trataría, de un "derecho especial en marcha hacia la autonomía".

Según algunos autores, el derecho de la informática derivaría su unidad de la originalidad técnica caracterizada por el fenómeno informático, por el cual, en muchos casos, las soluciones jurídicas tradicionales resultan inadecuadas.

En opinión de otros, el derecho de la informática será esencialmente un punto de cruce entre diversos derechos, pues la técnica de los ordenadores repercute en numerosas ramas del derecho: del derecho civil al derecho comercial y al derecho de autor; del derecho constitucional y administrativo al derecho penal.

EL DERECHO PENAL DE LA INFORMATICA

Si se acepta esta interpretación en lo concerniente a la multidisciplinariedad del derecho de la informática, podría hablarse entonces de un "derecho civil de la informática" que debería regir especialmente las cuestiones que surgieren del uso y de la producción de programas y contratos informáticos; de un "derecho público de la informática", que reglamentaría sus rasgos constitucionalistas y administrativos; y de un "derecho penal de la informática", cuyas funciones serían las de prever y reprimir específicamente las violaciones típicas del propio sector.

En sentido general el derecho penal de la informática sería esa subespecie del derecho de la informática que respecta a los actos ilícitos de índole penal como quiera vinculados con el empleo del ordenador. En sentido estricto, el derecho penal de la informática podría ser definido como aquel grupo de normas jurídicas por las cuales el Estado, prohibe, con la amenaza de una pena, ciertos comportamientos humanos específicos en el campo de la informática.

La creación de un derecho penal de la informática presenta, empero, dificultades de no poca cuenta, y sea desde el punto de vista científico-dogmático o desde el del derecho positivo. En efecto, han de proceder a formular normas específicas, modificar eventualmente el sistema de sanciones, coordinar las distintas normas entre sí; todo ello teniendo en cuenta principios fundamentales vigentes en los sistemas jurídicos de los países occidentales, que generalmente prohiben el recurso a la analogía en materia penal y están basados en el principio de legalidad estricta.

AFECTACIONES AL SOFTWARE. PROPIEDAD INTELECTUAL

Se ha definido al software como "el conjunto de datos e instituciones destinadas a producir información, que permiten controlar el funcionamiento del hardware y lo habilitan para cumplir determinados resultados", comprendiéndose

dentro de ese concepto, los programas de computación, su descripción y la documentación complementaria.

La detección de distintas conductas que implican usar sin autorización, modificar, borrar o copiar datos, informaciones o programas, plantea la necesidad de establecer, en atención al carácter inmaterial del objeto, cuál es el marco de protección jurídico-penal del software.

Al respecto existen dos posturas según entiendan que el soporte lógico (software) de los sistemas automáticos de procesamiento de datos se halla protegido por las normas que tutelan los derechos del autor (copyright), o bien se entienda que este marco legal resulta limitado e inadecuado a estos efectos.

Una corriente opina que el resguardo está brindado por las normas del derecho autoral, sosteniendo la viabilidad de proteger los "derechos de propiedad intelectual" sobre los programas de computación, ya que éstos constituirían una "creación personal intelectual".

Desde otra perspectiva se ha sostenido que el destinatario de las "obras" protegidas por el derecho de autor es el hombre, mientras que los programas de computación -fundados en un algoritmo- son un conjunto de instrucciones, que no revelan la personalidad del programador, destinadas a una computadora, y no a la percepción humana.

PROTECCION JURIDICA DEL "SOFTWARE" Y DE LOS MICROORGANISMOS

En nuestra legislación no están reglamentados los bienes incorporales mencionados supra, el "software" y los "microorganismos".

En el derecho comparado prevalece la orientación según la cual a los programas del computador le son aplicables las leyes de propiedad intelectual. En cuanto a los microorganismos, en la doctrina, jurisprudencia y convenios internacionales, son considerados patentables.

Desde el punto de vista legislativo no es de buena técnica establecer definiciones en las normas en que se perceptúen los derechos, así como hallar puntos de partida inconmovibles o definir la naturaleza jurídica a partir de todo lo cual sea dable su clasificación y sistematización.

En estos casos, se está en presencia de un hecho nuevo en el campo de la creación y de la técnica, con bases en proyecciones que la ley de propiedad intelectual no previó ni pudo prever.

Objetivamente considerada, la concepción del programa en la medida que su significado y aporte representen un interés es susceptible de protección jurídica, admitido que todo derecho, en el criterio de Jhering, "...establece la expresión de un interés reconocido por el legislador que requiere y merece protección...". Los derechos se transforman, por lo tanto -prosigue-, en la medida que cambian los intereses de la vida...".

La ley 11723 (Ley de Propiedad Intelectual) no sólo reconoce derechos a las obras extranjeras, sino que nuestro país se ha adherido a los convenios internacionales de protección del derecho de autor (Convención Universal sobre derecho autor y Convención de Berna), que contienen preceptos concordantes que permiten asegurar en todos los países la protección del derecho de autor.

En su consecuencia se operaría la protección del "software", sin demoras en la extensión de los convenios internacionales y sin disposiciones restrictivas, pues como acontece en nuestro país, no existe ley que los reglamente.

En consecuencia de lo expresado es fundamental la sanción de una ley especial, que necesariamente debería establecer: el objeto protegido debe contemplar los programas descritos en forma inteligible, de manera tal que pueda facilitar el uso y aplicación del software, el "originario" y el "derivado", así como la adaptación, reproducción o innovaciones de que pueda ser objeto.

La protección debería, asimismo, extenderse a los "algoritmos" y a la "combinación de algoritmos" aún conocidos.

Con las precisiones correspondientes y normas que integren los principios formulados, es dable evitar no sólo la monopolización de los registros, sino también obtener la consecuencia esencial, cual es el logro de un desarrollo propio en la materia, pues si el objeto de la protección es amplio, mayor será la posibilidad de registro de innovaciones, perfeccionamientos y de combinaciones de "algoritmos", aún conocidos.

En este punto cabe reglar los casos de software no registrados, como así también la responsabilidad civil y penal por la violación del derecho acordado.

Para ello es necesario reglamentar principalmente que la obligación de otorgar licencia, no se frustre por recursos dilatorios y excusas del titular, mediante las cuales pretenda justificar la falta de comercialización, reproducción o uso del software. O pretensión de justificación mediante la importación. En el punto debería contemplarse la hipótesis de nulidad del registro.

En cuanto a la patentabilidad de los microorganismos, el régimen que reglamenta el reconocimiento internacional del depósito de microorganismos a los fines del procedimiento en materia de patentes, se rige por el Tratado de Budapest de 1977.

El Tratado establece como principal característica, que un Estado contratante que permita o exija el depósito de microorganismos, a los fines del procedimiento en materia de patentes, debe reconocer, para ese procedimiento, el depósito de un microorganismo efectuado ante una autoridad internacional de depósito, lo mismo si esa autoridad está establecida en su territorio o fuera de él. En otras palabras, basta un sólo depósito hecho a una autoridad internacional de depósito única a los fines del procedimiento en materia de patentes ante las oficinas de patentes de todos los Estados contratantes y ante una oficina regional de patentes, si ésta declara que reconoce los efectos del tratado.

HACIA LA DELINCUENCIA INFORMATICA

Esta proyección de la tecnología informática expresada por la cantidad de ordenadores en funcionamiento, en las más diversas tareas socialmente útiles, ha generado, asimismo, un conjunto de conductas, relacionadas con la operatoria de los sistemas automáticos de procesamiento de datos, que son aptas para originar perjuicios de distinto orden, como las lesiones a la intimidad, la seguridad, (político-industrial), o al patrimonio.

La acumulación, archivo, y centralización de datos, en bancos automatizados, con sus posibilidades de asociación, combinación, devolución y divulgación, genera una situación que ante el acceso, modificación, destrucción o difusión no autorizados de estos datos (referidos, por ejemplo a profesión religiosa, actividad política, situación económica, salud, empleo), puede significar perjuicios en la esfera privada de los individuos. La protección de la intimidad y

de los datos personales ha originado un gran movimiento, a nivel internacional, como asimismo dentro de distintos países, expresados en los proyectos elaborados en el seno de la Comisión Económica Europea, el Consejo de Europa y la O.S.E.D.E., a los efectos de establecer instrumentos que permitan tutelar al individuo, ante los riesgos derivados del uso no autorizado de la información contenida en los bancos automatizado de datos. Se procura establecer previsiones respecto a la difusión de datos personales, el acceso a ellos por personas no autorizadas, con posibilidades de control y rectificación de datos por parte de los interesados.

Las posibilidades de vulnerabilidad de los sistemas informáticos han quedado evidenciadas en casos como el registrado en el año mil novecientos ochenta y ocho, cuando un grupo de "hackers" de Alemania Occidental, ingresó y operó por medio de las líneas telefónicas internacionales en las computadoras de la Nasa, lo cual demandó ulteriormente meses de trabajo a los efectos de proceder a cambiar los passwords y limpiar las trampas (trap doors) que los intrusos habrían colocado para poder tener acceso al sistema.

En el plano de los intereses económicos, las entidades bancarias, compañías de seguros y empresas productoras de bienes y servicios en general, pueden resultar damnificadas, con importantes perjuicios patrimoniales. En este aspecto, también se puede referir un caso, detectado en junio de mil novecientos ochenta y ocho, cuando operadores no autorizados, mediante una intervención en el programa, giraron la suma de cincuenta y cuatro millones de dólares de un banco suizo a otra entidad financiera para su cobro.

La información objetiva disponible permite establecer proyectivamente que el incremento de la informatización en las operaciones financieras determinará que los delitos contra el patrimonio adquieran una progresión desconocida hasta el presente, y que el mayor volumen de afectaciones económicas se concentre en el futuro en este tipo de operatoria.

En este área las tareas de investigación de campo, a partir del análisis de casos sometidos a investigación judicial, se ve dificultada por la tendencia a no denunciar este tipo de hechos, por parte de los damnificados. Se considera que esta actitud reticente se debe a que las empresas perjudicadas procuran evitar poner en evidencia que sus sistemas informáticos son vulnerables, por el efecto desfavorable que el conocimiento de esta circunstancia podría tener sobre sus clientes.

Las conductas perjudiciales cometidas en relación con los sistemas informáticos pueden ser realizadas, básicamente, con dos modalidades: como manipulaciones o usos del programa, utilizando equipos automáticos de procesamiento de datos (por ej: confección de balances falsos, administración fraudulenta), donde el sistema informático es el medio de la acción, o bien acciones que tienen el sistema como objeto (por ej: hurto del soporte físico, daño en las instalaciones, robo del hardware), supuestos que no constituyen una criminalidad diferenciada y se adecuan a los tipos penales clásicos, vigentes en el ordenamiento positivo.

Desde esa perspectiva los supuestos específicos de delincuencia informática, conforme a la experiencia internacional, estarían básicamente constituidos por los siguientes casos:

- uso no autorizado del ordenador o sus equipos, ya sea excediendo el límite de la autorización para operar, ya sea introduciéndose en el sistema;

- introducción, alteración, modificación, utilización, copia o destrucción, no autorizados, de datos, sin remoción de soporte magnético;

- violación del secreto informático;

- intervenciones en el programa a los efectos de posibilitar transferencias electrónicas de fondos con afectaciones al derecho de propiedad.

LEGISLACION ARGENTINA A ESTE RESPECTO

La legislación argentina sobre propiedad intelectual expresada en la ley ll723, en los arts. 7l y 72, establece distintas formas de defraudación de los derechos de propiedad intelectual, y sobre la obra, remitiendo, a los efectos punitivos, a las penalidades previstas para el delito de Estafa (art. l72 del Código Penal Argentino), que prescribe para este ilícito pena de prisión de uno a seis años.

Para que proceda entonces la adecuación de la acción defraudadora a la descripción del tipo, debe verificarse la concurrencia de un comportamiento doloso y los elementos del tipo objetivo de estafa (engaño, error, disposición patrimonial, perjuicio).

De la descripción contenida en el art. 72 de la ley ll723, surge que el objeto de protección está constituido por la "obra" lo que nos lleva a señalar dos cuestiones:

a) se efectúa una remisión a otras disposiciones de la ley ll723, a los efectos de poder establecer qué se entiende por "obra", lo cual nos coloca ante un tipo de disposición que la dogmática penal califica como "ley penal en blanco", denominándose de esta manera a las leyes que "sólo contienen la conminación punitiva y que respecto del tipo se remiten a otras normas", y

b) se plantea el tema de precisar si el software puede ser considerado como una "obra", en el sentido que la entiende la ley de propiedad intelectual. Sobre esta cuestión ampliamente debatida, existirían limitaciones en cuanto poder considerar el elemento básico del software: el algoritmo (procedimiento de cálculo constituido por secuencias de operaciones numéricas-lógicas), como asimismo, al "código objeto" o "programa objeto" (transformación del "programa-fuente" en un programa sólo legible por la máquina y constituido por símbolos binarios), sobre el cual se efectúan generalmente las copias no autorizadas de software, como una "obra" -creación del intelecto humano-.

Por su parte, la referencia efectuada en el art. 7l al expresar que "será reprimido... el que de cualquier manera y en cualquier forma defraudare los derechos de propiedad intelectual que reconoce esta ley", reúne no sólo la referida característica de "ley penal en blanco" -cuando expresa: a "los derechos de

propiedad intelectual que reconoce esta ley"- sino que al señalar, además, "al que de cualquier manera y en cualquier forma defraudare", incurre en una descripción inespecífica, propias de los llamados "tipos abiertos", o sea, aquellos en los cuales existe un grado amplio de abstracción caracterizándose "por la circunstancia de que los elementos fundamentadores de la ilicitud del hecho no están totalmente enunciados en la ley". Esto obliga al juzgador a recurrir a pautas o reglas que están fuera del tipo penal para procurar resolver el conflicto sometido a su decisión.

De esta manera, ningún hecho, más allá del reproche social que pueda merecer, o el perjuicio que causare a la comunidad, puede ser merecedor de una pena del derecho penal, sino existe una ley previa que lo haya declarado punible. Este es un costo que la sociedad debe asumir en mérito a contar con un sistema jurídico seguro que conlleve a una interpretación precisa y estricta de la ley penal, a los efectos de evitar extenciones subjetivas que determinen la persecución de conductas no previstas en el tipo penal.

Consecuencia directa del principio de legalidad, adoptado por el art. 18 de la Constitución Nacional Argentina, es la prohibición de la analogía, entendida como la aplicación de la ley a un caso similar al legislado, pero no comprendido en su texto, en el ámbito del derecho penal, en perjuicio del imputado.

La sistemática de esta ley de propiedad intelectual, en los aspectos considerados, genera un marco técnico-legal incierto. Por lo cual entendemos, en atención a posibilitar criterios seguros en la aplicación de la ley penal, evitar interpretaciones analógicas y resguardar el principio constitucional de legalidad que corresponde proceder a legislar, en esta materia, en forma específica y subsidiaria, respecto de las normas del derecho privado, por parte del ordenamiento penal.

ENTRE EL HURTO Y LA ESTAFA. ÉSTA ES LA CUESTION

Resultaría importante destacar al respecto el trabajo realizado por Sandro F. Abraldes, publicado en la revista "La Ley", con la finalidad de demostrar que en todos los supuestos en que se obtenga un desplazamiento patrimonial indebido a través de un medio mecanizado o informatizado, constituye lisa y llanamente el delito de Estafa.

Comienza realizando una distinción entre los delitos de Estafa y Hurto, determinando que en el primero de los casos se está en presencia del engaño y la perfidia. En la Estafa se da a la mentira la apariencia de verdad. Su fin es la defraudación por el abuso de confianza.

Dice que conforme lo determina Creus, en la defraudación, la acción de la víctima se origina en su voluntad viciada por un error suscitado en ella, como también puede ocurrir que ese error induzca a la víctima a omitir conductas, cuyas omisiones facilitan la actividad ilícita del sujeto activo.

Otra diferencia está dada por el objeto de la acción, desde que objeto del hurto sólo puede ser la propiedad en su sentido de tenencia de cosas muebles, y en la usurpación de inmuebles, ese objeto sólo puede ser, su tenencia o posesión o la cuasi-posesión de los derechos reales, la estafa puede recaer sobre cualquiera de los contenidos posibles de la propiedad, como la tenencia o la posesión de una cosa mueble o su dominio, las ventajas económicas correspondientes a una explotación comercial o la indemnización pertinente a su frustración, el beneficio jubilatorio, la garantía susceptible de valor pecuniario que significa un embargo, el valor de un crédito, etc.

El autor coincide con Mancini en que el objeto específico de la tutela penal es el interés público en la inviolabilidad del patrimonio, que el Estado pretende proteger contra las acciones fraudulentas tendentes a arrancar prestaciones útiles con provecho propio o ajeno. Con la incriminación de la estafa la ley penal considera genérica y objetivamente el patrimonio y lo tutela con un fin objetivo y colectivo, dejando a la ley civil la protección de los distintos derechos subjetivos.

En el tema en cuestión resulta claro que la protección penal que brinda el delito de estafa es, a la par que distinta, mucho más amplia que la de hurto. Esta amplitud otorga al Juez una herramienta más idónea a la hora de individualizar la pena, con lo que la holgada gama de casos que ofrece la realidad, será siempre mejor cubierta por el delito de estafa que por el de hurto. La expectativa social de penalización y la esencia retributiva de la pena son aspectos que la estafa contempla de mejor manera en estos supuestos.

En la doctrina nacional, la corriente mayoritaria que encuentra su mayor exponente en Soler afirma que "sin error no hay estafa", así como no la hay sin ardid aún cuando mediante alguna maniobra se logre un beneficio indebido. El

que mediante una moneda falsa logra sacar de un aparato automático el artículo que contiene no comete estafa sino hurto ya que si bien existe maniobra no existe ninguna mente errada. No así cuando han existido maniobras sobre medidores de luz o de gas, para determinar un error en la factura sobre la base de falsas cifras.

El autor también opina que en un caso en que el sujeto trató de obtener dinero ajeno mediante la utilización de una tarjeta magnética también ajena y sin autorización, ignorando el número de clave que correspondía, ese comportamiento se entendió como constitutivo de hurto en grado de tentativa.

También Creus se enrola en esta alternativa, para quien la maniobra de fraude tiene que determinar el error de la persona, si por ejemplo, aquella tiende a equivocar los controles de una máquina expendedora para que acuse más de lo debido, no hay estafa sino hurto, pero ello no ocurre cuando la alteración de la máquina es el medio al que se acude para engañar a la persona que la emplea para controlar la medida de la prestación que debe realizar.

Donna en disidencia sostiene que no existe estafa en este caso sino hurto, por que el error que lleva la lectura del medidor no es determinante de la entrega del gas o de la electricidad, sino que es representativo de su valor a posteriori.

Rojas Pellerano sostiene que el ardid o engaño empleado mediante aparatos mecánicos constituye estafa. El hurto es la excepción. Fundamenta su posición en la "objetividad jurídica" pues la falsedad o engaño ofende la relación a formarse y en vía de ejecución (sea un contrato civil, comercial o administrativo).

Esta tendencia extrema de considerar configurada una estafa en todas las posibilidades aludidas encuentra algunos escasos precedentes en nuestra jurisprudencia, siendo uno de ellos el adoptado por la Cámara de Apelaciones de la Capital Federal, que consideró que la introducción de un disco de metal en lugar de una moneda en el molinete del tranvía subterráneo para eludir el pago constituye el delito de estafa si advertida la maniobra el actor fue detenido en el acto.

En la doctrina Italiana Tolomei sostiene que en las maniobras realizadas sobre aparatos automáticos distribuidores de mercancías existe estafa. Estos aparatos proporcionan un bien contra el pago de un precio por lo tanto el que simula el pago del precio engaña al propietario del aparato. Entiende que la

función de estos aparatos equivale a la que cumple un mozo que entrega comida a precio fijo, y así como comete estafa quien entrega al mozo una moneda falsa, también existe estafa cuando el fraude se realiza sobre un distribuidor automático.

En la doctrina Española existe un criterio dominante que niega la aplicabilidad del delito de estafa sosteniendo que a las máquinas no se las puede engañar y que en estos casos la sustracción se lleva a cabo de una manera subrepticia aunque astuta sin previa entrega ni voluntad humana directamente operante por parte del engañado no presente, por lo que concluyen remitiéndose a la figura de hurto.

En la corriente opuesta, la posición de Bajo Fernandez, no duda en calificar como estafa la conducta de quien obtiene dinero del cajero automático de un banco utilizando una tarjeta robada o hallada u otro objeto que la sustituya.

Análogo temperamento propicia Bustos Ramirez, ya que, a pesar de la amplitud de la defraudación y de la estafa en su pretensión de abarcar medios intelectuales de ataque al patrimonio, se ha producido un desfasamiento con la realidad, en razón del gran avance tecnológico producido. Así las cosas, el surgimiento de la computarización y maquinización de las actividades económicas ha traído como consecuencia la utilización de nuevos medios que no se pueden incluir dentro de las defraudaciones o estafas en virtud del principio de legalidad, como por ejemplo, el sujeto que se logra conectar con el ordenador de un banco y que a través de la alteración de su programa consigue que le sean borradas sus deudas, ha realizado una actividad que no se puede incluir en la estafa ni en ningún otro delito contra el patrimonio.

El fallo plenario "Ruzzolino, J. L." del año 1961, se reunió para resolver en qué disposición legal encuadrar la conducta de quien mediante la utilización maliciosa del conducto por el que se recuperan las monedas de un teléfono público, retira en su provecho las que quedaron depositadas por no haberse obtenido la prestación del servicio. El voto de la mayoría sostuvo que trasladado el concepto de estafa al ejemplo del plenario se advierte enseguida la ausencia de esa relación causal entre engaño, error y disposición.

La postura contraria sostuvo que ninguna dificultad existiría si en razón de hallarse el aparato efectivamente descompuesto, por tal motivo no recupera la moneda y después un tercero valiéndose de cualquier treta, que no importe forzar la cosa de donde ha quedado retenida, la sustrae para sí, pues tal apoderamiento

importa el delito de hurto simple... pero no ocurre lo mismo si la maniobra ha sido antes preparada a los fines de hacer creer al usuario que aquella posibilidad de rescate deriva de algún defecto propio de la máquina induciéndose de esa manera a su abandono equivalente en los hechos a una práctica entrega. Por lo que tal conducta resultaría una típica acción estafadora por un medio mecánico tan eficaz e idóneo al efecto como cualquier otro ardid o engaño de índole personal.

El autor del artículo continúa refiriéndose respecto de la inaplicabilidad del tipo penal de hurto por cuanto el mismo exige que exista la acción de "apoderarse" en el sentido de aprehensión física, material de la cosa por lo que aparecen grandes dificultades a la hora de proyectar las manipulaciones fraudulentas, mediante medios mecánicos, automatizados o informatizados, en la mencionada conducta típica, debiendo también tenerse en cuenta la dificultad de asignarle el carácter de cosa mueble al dinero contable, escritural o documental.

Hace también referencia a la dificultad de calificar como estafa los delitos cometidos a través de medios informatizados en los que opere una persona humana, en virtud de la ya comentada inexistencia de una mente errada.

No obstante ello este autor se inclina por encuadrar estas conductas en el artículo 172 del código penal y ejemplifica diciendo que si un consumidor accede a una máquina para obtener un bien, entabla una relación con la persona física o jurídica, que valiéndose del referido medio, entrega el bien. Sería desatinado reconocerle a un simple aparato el dominio de un acto de disposición patrimonial.

Regresando al caso de quien con una tarjeta extrae antijurídicamente fondos de un cajero automático, Nuñez diría que el mecanismo ya no expresa la voluntad de aquel que condicionó el acto de disposición a la forma legítima de su funcionamiento. ¿por qué no sostener que el cajero sigue expresando aquella voluntad preordenada pero sobre la base de un engaño, tal como no dudaría en afirmar Tolomei, cuando seguramente, equipararía este supuesto al del mozo que se le da una moneda falsa?. Es evidente que según esta línea que el acto ejecutivo es realizado a consecuencia del engaño de que es objeto el elemento intelectivo pre-establecido. Así puede aseverarse que el sujeto tiene el dominio mediato de la disposición patrimonial que lo perjudica.

Desde el principio fue intención del trabajo de este autor situar dogmáticamente a estos comportamientos en el art. 172 del Código Penal, Para ello ha demostrado lo siguiente:

- respecto al engaño, es imprescindible aceptar que el falseamiento de la realidad que él implica, no comporta necesariamente una relación directa y personal entre dos seres humanos, lo que debe ser desechado por vía de interpretación solamente comprensible en otro contexto histórico.

- Sobre el error, debe negarse su condición de elemento autónomo del tipo objetivo, circunscribiendo su función a la delimitación restrictiva del engaño típico, por lo que siguiendo una interpretación de esta índole quedan suprimidos algunos de los obstáculos que alguna doctrina invoca para calificar de estafa a las defraudaciones mediante medios mecanizados.

Ha probado, desde varias posiciones, que en lo concerniente al acto de disposición, debe aceptarse que se pueden realizar disposiciones materiales con el auxilio de una máquina, y que la colaboración en el traspaso patrimonial lesivo que este elemento implica, puede atribuirse a la persona física, pues el dominio de la disposición, sin duda, le corresponde.

Aún siendo evidente que la figura de estafa no fue concebida para esta nueva manifestación de la criminalidad defraudatoria, su aplicación en este ámbito cabe, sin contradecir las exigencias del principio de legalidad.

Esta nueva gama de delitos que estudiamos, no solamente han provocado inconvenientes y preocupaciones a la legislación penal argentina, sino también a países de notable desarrollo de Europa, tales como:

ALEMANIA

Donde el derecho penal ha tropezado con dificultades considerables, ya que en la década del ochenta, más precisamente del año mil novecientos ochenta y dos, se acepta la incorporación a la legislación penal de dos nuevos tipos penales, como el de "estafa por ordenador" y de "falsificación de datos almacenados", habiendo quedado resueltas las lagunas legales más importantes del Código Penal Alemán en relación con la lucha contra las manipulaciones del ordenador, permaneciendo abierta la cuestión de si, a causa del rápido desarrollo técnico

luego de esta aprobación podría considerarse que esté ya nuevamente anticuado, debido al constante crecimiento del sistema informático.

Los delitos informáticos más característicos en Alemania, y que han pasado a un primer plano resultan ser las manipulaciones de ordenadores, el espionaje informático, el hurto de software, el sabotaje de ordenadores, el hurto de tiempo, así como la comisión de delitos económicos en general por medio de ordenadores.

Manipulaciones del ordenador: consiste en modificaciones de datos, practicadas especialmente por empleados de las empresas perjudicadas con el fin de obtener un enriquecimiento personal. Se considera al ordenador como una instalación de procesos de datos, es decir, como una instalación en la que se introducen los datos que se tienen que procesar (el denominado input) y la forma de proceso deseada (a través del programa y los recursos de consola complementarios) obteniéndose automáticamente el resultado del proceso (el denominado output), se ponen de relieve los diversos métodos de manipulación del proceso de datos: el autor puede en un principio introducir datos falsos en el ordenador (manipulaciones del input), puede alterar el orden del proceso (manipulaciones del programa y de la consola), o bien puede posteriormente falsear el resultado, inicialmente correcto, obtenido del ordenador (manipulaciones del output).

Espionaje informático y hurto de software: el espionaje informático constituye en el ámbito de la criminalidad por ordenador la segunda forma más frecuente de delito. Para el autor es especialmente lucrativa, y para la empresa afectada es especialmente peligrosa, porque en los centros de cálculo de la mayoría de empresa con frecuencia se almacenan en muy poco espacio, importantes y numerosos secretos de las mismas.

La elevada capacidad de almacenamiento de datos que permiten los sistemas informáticos y la posibilidad de copiarlos rápida y discretamente con la ayuda del ordenador, conducen al hecho de que el espionaje informático abre nuevas dimensiones al espionaje económico.

En los últimos tiempos un punto central del espionaje informático y del hurto de software se observa ante todo en el ámbito de la concesión de licencias de programas, por ello en este ámbito se tendría que prestar atención al hecho de que los programas se transmitan solo en código objeto (no modificable), y que

contengan notas de bloqueo adecuadas (en especial las denominadas fechas de expiración y, si fuera posible, también bloqueos de copias).

Sabotaje informático: el modus operandi que se utiliza con más frecuencia en el ámbito de sabotaje informático consiste hoy en día sobre todo en la práctica de incendios y atentados con bombas, así como la introducción de los denominados "programas-crash", que borran grandes cantidades de datos en un cortísimo espacio de tiempo.

En el caso de sabotaje que se han descubierto en el ámbito internacional, se han tratado sobre todo de terroristas que actuaban por motivos ideológicos. Estos ven con frecuencia en el ordenador el símbolo del control y de la opresión estatal.

Por esta razón sería conveniente que todas las empresas duplicaran regularmente los datos más importantes y los almacenaran en algún lugar externo al edificio, y que dispusieran de un plan de catástrofes, en especial en relación con los casos de sabotaje.

Hurto de tiempo: se conoce aquellos supuestos tan frecuentes hoy en día en el ámbito del proceso de datos, en los que empleados del proceso de datos, utilizan los ordenadores de la empresa y parcialmente también sus programas, para fines privados y actividades complementarias.

Delitos económicos en general: las posibilidades de manipulación del ordenador son aprovechadas no sólo por empleados que perjudican a la propia empresa, sino también por la gerencia de empresas que trabajan fraudulentamente para perjudicar a la competencia o a organismos estatales. En los casos descubiertos hasta el momento se trataba ante todo de manipulacines de cuentas, balances, lista de inventarios y declaraciones de impuestos elaborados por el ordenador.

CARACTERISTICAS DE LOS DELITOS INFORMATICOS. DESARROLLO FUTURO Y DIFICULTADES DE AVERIGUACION

Permanencia y automatismo del hecho: La característica más evidente que evidencia la criminalidad informática de la criminalidad contra la propiedad en general, está constituida por la especial permanencia en la comisión del hecho.

La posibilidad de repetición que sirve de base a este fenómeno se fundamenta en la rígida organización que normalmente caracteriza la forma del trabajo del proceso de datos, de forma que si el autor encuentra una laguna, en cualquier momento podrá aprovecharse de ella y en este caso a veces se puede advertir la irregularidad a través de un cambio planificado del lugar de trabajo (job-rotation).

Sumas de daños: La permanencia del hecho, a la que acabamos de hacer referencia, constituye una de las causas de los daños tan elevados que producen los delitos informáticos, que es otra de las características de esta forma de criminalidad.

Con ello se confirma la tendencia que cada vez son más elevadas las sumas de daños que son ocasionadas sobre todo porque en el ámbito de la criminalidad informática se trata de dinero contable, cuya cantidad máxima no tiene porqué limitarse, como en cambio sucede en el objeto de las clásicas defraudaciones, que se limitaría a la cantidad de dinero que se encuentre en la caja.

Dificultades de averiguación: Las dificultades de averiguación que caracterizan el ámbito de proceso de datos radican, no en el ordenador, sino en el elevado número de procesos individuales ejecutados. La falta de visualización de los datos almacenados electromagnéticamente también dificulta de forma muy considerable la averiguación de las manipulaciones.

Este problema de averiguación que aquí se plantea (y que ha sido descrito de forma expresiva por la criminología americana como Second-hand) sólo puede resolverse si se reduce mediante un adecuado control informático de los revisores, auditores y funcionarios encargados de la persecución, el tiempo de búsqueda de la información.

Medidas para el descubrimiento de delitos informá-ticos: A fin de reducir al mínimo los riesgos de la criminalidad informática es importante, además, que las medidas preventivas de la empresa no sólo se dirijan a evitar, sino a también a descubrir esta clase de delitos. Como ya hemos dicho, el descubrimiento de delitos informáticos puede revestir considerables dificultades cuando el autor está en situación de manipular los controles y los balances de la empresa. Con frecuencia también en el hurto de software es difícil descubrir qué programas y qué datos se copiaron y utilizaron en el centro de cálculo ajeno. Por ello, si la

instalación de procesos de datos administra direcciones de clientes, puede resultar indicado, por ejemplo, almacenar también las direcciones privadas de los responsables de la seguridad o de los dueños de la empresa, pero de forma errónea (por ejemplo con un nombre falso). Así, si esta persona recibe una oferta de la firma competidora con la misma clase de error en la dirección, por lo menos tendrá conocimiento de que se han copiado los datos de los clientes de la empresa.

A este respecto, el Código Penal Alemán, para los fraudes por medios mecanizados o automatizados, y defraudaciones de fluido eléctrico y otras análogas, dentro del Capítulo "Estafas y otras Defraudaciones" incluye el parágrafo 265 a. que dice: "el que obtiene de forma subrepticia, con la intención de no pagar el precio, la prestación de un aparato automático, o de una red de comunicaciones públicas, el trasporte por un medio público de transporte, o el acceso a una representación u otra institución, será penado con...".

Asimismo, el Código Penal Alemán reprime en su parágrafo 263 a. "quien con la intención de conseguir una ventaja patrimonial ilícita para sí mismo o para otro, cause un perjuicio patrimonial a un tercero, influyendo sobre el resultado de una elaboración de datos por medio de una realización incorrecta del programa, a través de la utilización de datos incorrectos o incompletos, mediante la utilización no autorizada de datos, o influyendo en la elaboración a través de una intervención ilícita".

EN LO QUE RESPECTA A ESPAÑA

Y conforme conclusiones del Congreso sobre Derecho Informático, organizado por la Facultad de Derecho de Zaragoza durante el año 1989, debemos destacar:

Definición y características del delito informático: delito informático es toda acción dolosa que provoca un perjuicio a personas o entidades, en cuya comisión intervienen dispositivos habitualmente utilizados en las actividades informáticas.

División de delitos informáticos: pueden dividirse en tres grandes bloques:

a) uso indebido o manipulación fraudulenta de elementos informáticos de cualquier tipo, que posibilitan un beneficio ilícito, tal cual es el fraude informático;

b) casos de vandalismos, terrorismos, etc. cuya finalidad es provocar un perjuicio, con motivo de venganza, extorsión, etc. atentan contra la integridad de los elementos informáticos tal como es acciones físicas;

c) delitos relacionados con la integridad de la propiedad intelectual de los elementos informáticos, especialmente del software, tal como es piratería del software.

Al no existir regulación legal se ha optado por calificar de delictiva toda acción que de forma voluntaria causa un perjuicio a alguien independientemente de que produzca o no un beneficio a su autor. Y de inocua la que no provoca daño a nadie ni beneficia al autor.

Fraudes informáticos: Se puede definir como toda conducta fraudulenta realizada a través o con la ayuda de un sistema informático por medio de la cual alguien trata de obtener un beneficio ilícito.

Elementos: el sujeto, autor o autores de la conducta fraudulenta; el medio, sistema informático sin el cual no se podría llevar a cabo la acción; el objeto, el bien que produce el beneficio ilícito.

Clasificación de los perjuicios: a) perjuicio económico directo: existe una apropiación de bienes, es uno de los pocos que puede ser perseguido y castigado según la legislación tradicional, el problema no es tanto descubrirlo, sino como probarlo; b) perjuicio económico indirecto: no se produce una apropiación de bienes tangibles o valorables, ejemplo: sustracción de información confidencial de carácter económico, comercial, etc. que dañan los intereses de la organización a medio o a largo plazo de forma difícilmente cuantificable; c) perjuicios intangibles, casos poco frecuentes, pueden consistir en la manipulación de programas con la finalidad de deteriorar el prestigio de la empresa para la que se trabaja.

CARACTERISTICAS DE LA ACTIVIDAD INFORMATICA QUE INCIDEN EN LA COMISION DE LOS FRAUDES

Concentración de la información, existe la tendencia a concentrar la información en grandes bases de datos sobre la que interaccionan multitud de usuarios, que acceden a cualquier tipo de información una vez penetradas las medidas de control de accesos.

Ausencias de registros visibles, no existe la posibilidad de descubrir un hecho fraudulento por simple inspección visual al estar la información gravada en forma de impulsos eléctricos.

Los programas y los datos pueden alterarse sin dejar rastros, la alteración del programa o datos grabados en soportes magnéticos puede hacerse sin dejar ni rastro, salvo que se hallan adoptado las medidas de control necesarias.

Fácil eliminación de pruebas, es muy fácil hacer desaparecer programas manipulados o ficheros de datos alterados, pulsando una tecla o emitiendo una instrucción de borrado.

Complejidad del entorno técnico, incluso los sistemas más sencillos presentan una gran complejidad en términos de capacitación técnica.

Dificultad para proteger los ficheros mecanizados, la protección de la información almacenada en soportes magnéticos es muy compleja.

Concentración de funciones, el concepto de segregación de funciones incompatibles suele ser inexistente en los centros de procesos de datos.

Carencia de controles internos en las aplicaciones, que son débiles ante los intentos de manipulación fraudulenta.

Controles ineficaces para el personal técnico, éstos pueden ser soslayados por técnicos informáticos de una cierta calificación.

Dispersión territorial de los puntos de entrada al sistema, para acercar la informática al lugar donde se encuentra el usuario o donde produce los datos de entrada.

Dependencia de redes públicas de transmisión de datos, no es posible establecer medidas de control sobre las redes públicas, sólo sobre los mensajes propios.

TIPOLOGIA DEL FRAUDE INFORMATICO

Sustracción de dinero o documentos que los sustituyan, emisión de cheques auténticos y ficticios por el ordenador, etc.

Sustracción de mercancías, a través de la manipulación de sistemas mecanizados de control de inventarios para hacer desaparecer mercancías, introduciendo movimientos de salida falsos o de no registrar movimientos de entrada.

Sustracción de valores negociables o documentos que sirvan de soporte para el intercambio de mercancías o dinero, casos de apropiación de acciones, valores, participación en fondos de inversión, etc.

Sustracción de servicios, mediante manipulación de los sistemas de medición, registros, facturación y seguimiento de cobros, también la utilización de los dispositivos informáticos en provecho de los empleados de la empresa.

Sustracción de software, lo que se sustrae y generalmente se vende es una copia, los informáticos suelen pensar que las aplicaciones desarrolladas por ellos, son en cierto modo suyas y que la empresa que les ha pagado tiene sólo un relativo derecho de propiedad sobre ellas.

Sustracción de información, en la actualidad es uno de los delitos menos desarrollados, pero que pueden alcanzar una mayor tasa de perjuicios para las empresas afectadas, pudiendo denominarse "espionaje industrial realizado por procedimientos informáticos".

COMO SE REALIZA EL FRAUDE INFORMATICO (según Donn Parker)

Introducción de datos falsos: es el método más sencillo y más utilizado, consiste en manipular las transacciones de entrada, con el fin de introducir

movimientos falsos, o eliminar las transacciones verdaderas que deberían haberse introducido. Un ejemplo puede ser la introducción desde un terminal inteligente conectado a un ordenador central de transacciones falsas, para producir la emisión de cheques fraudulentos.

El caballo de Troya: el método consiste en introducir dentro de un programa de uso habitual, una rutina o conjunto de instrucciones, por supuesto no autorizadas, para que dicho programa actúe en ciertos casos de forma distinta a como estaba previsto.

Para utilizar este método de fraude es preciso poseer una capacitación técnica suficiente, al menos saber programar y tener acceso al programa para poder manipularlo.

Es éste un método difícil de detectar, pero fácil de prevenir instituyendo unos estrictos procedimientos de catalogación y descatalogación de programas, de forma que sea imposible acceder a ningún programa para su modificación sin los correspondientes permisos, y una vez que éste haya sido modificado, comprobar que el programa funciona correctamente, modificado en lo que se pretendía y que el resto siga igual.

Como ejemplo típico expondremos un caso real sucedido en España. El autor al parecer un ex empleado del centro de proceso de datos de la entidad o de una entidad de crédito, introdujo una rutina dentro del programa del tratamiento de cuentas corrientes, por la que un día determinado, aproximadamente seis meses después de haber cesado el empleado en su trabajo, y a una hora determinada entre las 11,00 y 11,30 se autorizase el pago de un talón de una cuenta concreta sin consultar el saldo, posteriormente la misma rutina borraba parte del programa, con lo que se eliminaba el rastro de la comisión del delito. El fraude fue de unos diez millones de pesetas y no se pudo probar la autoría del mismo.

La técnica de Salami: es la modalidad de fraude más sencilla de realizar y la que menos probabilidades de ser descubierta tiene. El procedimiento consiste en introducir o modificar unas pocas instrucciones en los programas para reducir sistemáticamente en unos céntimos las cuentas corrientes, los saldos de proveedores, etc, transmitiéndolos a una cuenta corriente que se abre con nombre supuesto y que controla el defraudador. Resulta muy difícil descubrir este tipo de fraude, porque no se produce ninguna señal de alarma.

Super zaping: consiste en el uso no autorizado de un programa de utilidad para alterar, borrar, copiar, insertar, o utilizar en cualquier forma no permitida, los datos almacenados en el ordenador o en los soportes magnéticos. El nombre de esta técnica viene de un conocido programa de utilidad "superzap" que es como una llave que abre cualquier rincón del ordenador por protegido que pueda estar, es un programa de acceso universal. Cuando se descubre la alteración de los datos se piensa que ha sido un funcionamiento inadecuado del ordenador o una transacción errónea. En la práctica es imposible probarlo.

Puertas falsas: el método consiste en la producción de interrupciones que hacen los programadores para el chequeo del programa, con lo que se dejan puertas falsas para entrar en él. El problema que plantea este método es tener la certeza de que cuando los programas entran en proceso de producción normal todas las puertas falsas hayan desaparecido. Este método de fraude requiere una especial cualificación técnica por parte de los autores, lo que reduce considerablemente el espectro de personas sobre las que podría sospecharse.

Bombas lógicas: es el procedimiento de sabotaje más comúnmente empleados por los empleados informáticos descontentos que antes de abandonar sus puestos de trabajo dejan una bomba lógica o bomba de tiempo, para producir daños en un momento posterior a su marcha de la empresa. Estas bombas se usan como medio de sabotaje, venganza o placer de perjudicar. El método consiste en introducir en un programa un conjunto de rutinas no utilizadas generalmente ni autorizadas para que en una fecha o circunstancia predeterminada, se ejecuten desencadenando la destrucción de información almacenada en el ordenador, distorsionando el funcionamiento del sistema, provocando paralizaciones intermitentes, etc.

Ataques asincrónicos: este procedimiento es el más complejo desde el punto de vista técnico, no se tiene noticia de la comisión de ningún fraude con él, aunque con su complejidad bien podría ser de los cometidos y no detectados hasta ahora.

La técnica se basa en la forma de funcionar de los sistemas operativos y sus conexiones con los programas de la aplicación a los que sirve y soporta en su ejecución.

El sistema operativo es el conjunto de programas que gobiernan y controlan el funcionamiento del ordenador y de todos sus dispositivos periféricos,

la entrada de los datos que debe ser procesada por los programas, la ejecución de éstos y la salida de información elaborada en los procesos hacia los dispositivos de salida. Otra función fundamental del sistema operativo es optimizar la ocupación de memoria central reasignando áreas en función de las necesidades de cada uno de los programas que están en ejecución en cada momento. También es quien controla y maneja todos los errores que pueden producirse, tanto en el ordenador como en el programa que sea ejecutado, avisando al operador por medio de mensajes de cualquier situación anómala que se produzca.

Los sistemas operativos funcionan en forma asincrónica, estableciendo colas de espera que van desbloqueando en función de la disponibilidad de los datos o recursos que estaban esperando.

Recogida de información residual: se basa en aprovechar los descuidos de los usuarios o técnicos informáticos para obtener información que ha sido abandonada sin ninguna protección como residuo de un trabajo real efectuado con autorización.

Puede hacerse de dos formas distintas: l) Método físico: consiste en recoger el material que se desecha en las papeleras como listado de pruebas de programas, fotocopias de documentos reservados, etc.; 2) Método electrónico: se basa en aprovechar las finalizaciones de ejecuciones de trabajos reales en el ordenador para obtener la información residual que ha quedado en memoria que no se ha tenido la precaución de borrar.

Divulgación no autorizada de datos reservados: se trata de la sustracción de información confidencial o espionaje industrial, realizar la copia de un fichero mecanizado es tan rápido y simple que es una forma de delito prácticamente al alcance de cualquiera.

Pinchado de líneas: es una técnica bastante generalizada para obtener información de forma clandestina. Todo lo que se necesita es un pequeño grabador, un cassette, un módem para demodular las señales telefónicas analógicas y convertirlas en digitales y una pequeña impresora para listar la información que se ha captado.

El procedimiento más eficaz para proteger la información por línea de comunicación, es la criptografía, aunque es un procedimiento poco extendido por

la escasa amenaza que suponen hoy en día los pinchados ilegales y por el costo relativamente caro de los dispositivos criptográficos.

Simulation and modeling: los ordenadores son una herramienta potentísima para efectuar simulación de situaciones, que permiten estudiar las consecuencias previsibles, sobre el comportamiento de una empresa, inversiones, estadísticas, etc.

El ordenador ha servido también para planificar y simular la comisión de un delito antes de realizarlo, aunque en realidad escasean los delitos cometidos por este método.

Otra clasificación realizada por Miguel Ramallo Romero y María Cinta Castillo Jiménez, incluye a:

Los hackers: son esa legión de jóvenes fanáticos de la informática con un ordenador personal, un módem y una gran imaginación que son capaces de acceder a través de una red pública de transmisión de datos al sistema informático de una empresa, institución bancaria, etc., introduciéndose en él. Este fenómeno aún no ha proliferado en España, en otros países esta forma de delincuencia está generalizada.

Las técnicas utilizadas por los hackers se basan en la oportunidad y el esfuerzo, para combatir este tipo de intrusos se establecen los habituales controles de acceso a la información. Uno de los problemas más graves con el que se enfrenta el hackers es hacer frente a las facturas de la compañía telefónica por la utilización masiva de las líneas de comunicaciones. Estos genios, suelen para combatirlo, puntear unas líneas telefónicas para desviar los cargos hacia otros usuarios. Su principal objetivo es penetrar en un sistema informático, para ello: 1) deben encontrar el número de teléfono que les permita conectar con el ordenador, 2) descubrir el identificativo que le permita abrir la cesión de trabajo, 3) averiguar la clave de acceso que le autorice a entrar en las áreas o ficheros reservados.

Se pueden destacar tres tipos de medidas de protección contra los accesos no autorizados a través de líneas de comunicación, dos son lógicos (de software) y un tercero físico (de hardware).

a) la primera consiste en desconectar la comunicación al tercer intento de acceso utilizando una clave errónea, e informar a quien proceda de que ha habido un intento de penetración en el sistema;

b) la segunda es no facilitar por pantalla ninguna información hasta tanto no se halla verificado la identidad de la persona que se ha conectado;

c) por último, un procedimiento bastante eficaz para eliminar el riesgo de ser víctima de los hackers, o de cualquier tipo de acceso indebido, vía línea de comunicaciones, consiste en tener un sistema de "call back" o de devolución de llamadas.

La eficacia de este dispositivo se basa en que cuando un usuario conecta con el sistema y se identifica válidamente, queda registrada su identificación y a continuación antes de comenzar la cesión de trabajo, el sistema investiga y desencadena una llamada del ordenador central al número real del usuario identificado.

La piratería del software: según la Organización Mundial de la Propiedad Intelectual, se entiende por software, al programa, conjunto de instrucciones que cuando se hallan en un soporte y formato legible por el ordenador dotan a este de la capacidad de procesar información en orden a realizar una determinada función o tarea, o calcular un determinado resultado.

El material de soporte es cualquier otra documentación, aparte del programa y de su descripción, creado para servir de ayuda a la comprensión y utilización de los programas, por ejemplo el manual del usuario.

Los elementos que se incluyen en la definición son bastantes heterogéneos, incluyen elementos tangibles, como puede ser el disco donde está grabado el programa, que es un elemento tangible y el programa grabado en el que es un elemento intangible, por lo que al comprar un disco conteniendo una serie de programas, no sólo no somos propietarios de dichos programas, sino que legalmente ni siquiera tenemos derecho a copiarlos, lo que hemos adquirido ha sido una serie de derechos de uso sobre los elementos intangibles, contenidos en el producto tangible que les sirve de soporte.

CAUSAS QUE DAN ORIGEN A LA PIRATERIA DEL SOFTWARE

Las personas que desarrollan un determinado software son asalariados de una empresa que creen tener sobre el software creado una serie de derechos, sin considerar el salario recibido por ellos.

El segundo factor que interviene, es el hecho que al hacer una copia no se deteriora el original, lo que da la apariencia de ser una acción inofensiva, pero en realidad las empresas dedicadas a la creación de software se ven gravemente perjudicadas y por el contrario las que consiguen las copias de los programas se ven beneficiadas al encontrarse con un programa que no han tenido que encargar ni comprar.

El tercer factor que interviene en el gran desarrollo que tiene la piratería del software, es el precio desproporcionadamente alto que se ha aplicado, a gran parte de los programas que se comercializan.

Actualmente el Código Penal Español en su art. 255 expresa: "será castigado con la pena de... el que cometiere defraudación, utilizando energía eléctrica, gas, agua, telecomunicaciones u otro elemento, energía o fluido ajenos por alguno de los medios siguientes:

1) valiéndose de mecanismos instalados para realizar la defraudación;

2) alterando maliciosamente las indicaciones o aparatos contadores;

3) empleando cualesquiera otros medios clandestinos".

El art. 248 de este Código expresa en su inciso primero: "cometen estafa los que, con ánimo de lucro, utilizaren engaño bastante para producir un error en otro, induciéndolo a realizar un acto de disposición en perjuicio propio o ajeno" y en su inciso segundo: "también se consideran reos de estafa los que, con ánimo de lucro, y valiéndose de alguna manipulación informática o artificio semejante, consigan la transferencia no consentida de cualquier activo patrimonial en perjuicio de terceros".

LA VANGUARDIA NORTEAMERICANA

Es de destacar la infraestructura desarrollada en los Estados Unidos para permitir el funcionamiento de la firma digital, utilizada en la actualidad para otorgar seguridad a las transacciones comerciales electrónicas y a la transferencia electrónica de datos.

El comercio electrónico en general, de Internet, en especial, fue ideado para el intercambio de información. Sin embargo, en la actualidad se los utiliza en gran medida para transacciones que requieren el posterior transporte de la mercadería objeto de las transacciones. La compra electrónica será la comercializadora inevitable de la Internet, pero los que la defienden fervorosamente deberían tener en cuenta que los hábitos de los consumidores, son difíciles de romper, ya que generalmente les gusta elegir y tocar las mercancías.

Otro requisito para el asentamiento del comercio electrónico radica en sistemas de pagos eficientes y seguros, pudiendo clasificar estos sistemas distinguiendo entre tarjetas de crédito, cheques digitales y dinero electrónico.

Con respecto a los cheques digitales, este sistema funciona como si se tratare de cheques reales, salvo que el usuario utiliza una firma digital para firmar el cheque y luego transmitirlo en línea (no linee) encuitado.

El usuario necesita una chequera electrónica que actualmente consiste en una tarjeta de tamaño de una tarjeta de crédito que puede contener datos y se inserta en un solté en la mayoría de las computadoras portátiles que se vende en la actualidad. En el futuro la chequera se llevará en una tarjeta inteligente (smart card), que cuenta con un chip y distintos tipos de memoria, que le permitirá generar cheques, llevar su registro de cheques y guardar claves públicas y privadas.

En lo que respecta a la seguridad, en principio, se da por sentado que el medio utilizado es inseguro. Preocupa sobre manera de que puedan ser interceptados datos que circulan por la red de redes Internet, que básicamente constituye el medio de transmisión de datos por excelencia. A esto podemos agregarle otro ingrediente que complica severamente la situación en el sistema norteamericano: La ausencia de terceras partes confiables.

Hasta el momento, lo más efectivo para proteger la información que se transmite, ha sido recurrir al milenario sistema de cifrar la información que se envía.

Esto nos introduce en la ciencia de la Criptografía, que estudia la ocultación, disimulación o cifrado de la información.

La Criptografía tradicional se basa en el concepto de que tanto el que envía el mensaje como el que lo recibe, conocen y utilizan la misma clave secreta. Este método se conoce como Criptografía con clave secreta, el que ha tenido dificultades para brindar la seguridad necesaria en este aspecto.

Existe un acuerdo generalizado acerca de que el sistema que mayor seguridad brinda en la actualidad a las transacciones electrónicas e intercambio electrónico de datos es el de la Criptología de clave pública, basada en algoritmos asimétricos, inventada en 1976 en la Universidad de Standford Estados Unidos. En este sistema cada persona obtiene un par de claves, llamadas clave pública y clave privada. Cada usuario debe generar su propio par de claves, por intermedio de un Software confiable.

Por este medio se obtienen transacciones seguras y auténticas con la certeza de la integridad de los datos y la imposibilidad de repudio por parte del emisor. El sistema requiere una infraestructura grande y compleja, pero esencial: Sin ella los usuarios no podrán saber con quién están tratando en la red, a quién le están enviando dinero, quien firmó un documento o si la información fue interceptada y alterada mediante la transmisión. Por ello los usuarios demandarán una fuerte infraestructura de administración con manejo de claves basadas en autoridades certificantes que operen bajo estrictas normas predeterminadas.

Se han advertido entonces distintas posturas legislativas respecto de la validez del documento electrónico: a) Una postura amplia en que el legislador establece la validez del documento electrónico, sin hacer referencia a su soporte material ni al tipo de lenguaje a utilizar. Tampoco se analiza o se ajustan otras normas que hacen referencia al documento tradicional (proyecto del Estado de California y Florida);

b) Una postura restringida en que el legislador se preocupa no sólo de establecer la validez jurídica del documento electrónico, sino también de

reglamentar su uso, a la vez que determina detalladamente la infraestructura técnica y operacional que se utilizará para la inserción del mismo en la práctica comercial (Utah y Georgia);

c) Una postura detallista en que el legislador revisa todo el cuerpo legal para derogar, modificar o agregar normas que hagan compatibles el sistema con el documento electrónico (proyecto del gobierno de Alemania); y por último,

d) Algunas combinaciones, donde se encuentra un sistema de intervención junto con algunas características de las posturas antes referidas (proyecto de ley de Italia y Chile).

Existen en los Estados Unidos restricciones impuestas por el gobierno al desarrollo y difusión de las tecnologías criptográficas. La National Security Agency (N.S.A.) fue creada por orden del presidente Truman en 1952, siendo su función primordial la intervención en el área de comunicaciones, interceptando y descifrando las comunicaciones secretas de otros gobiernos.

Se sostiene en los Estados Unidos que el Gobierno y la Industria deben trabajar conjuntamente a los efectos de crear una infraestructura que brinde seguridad y permita el desarrollo de productos que incorporen elementos de criptografía, sin menoscabar la seguridad Nacional y Pública.

La industria participará en la definición de algoritmos y protocolos standar, y desarrollará productos de claves de encriptado adecuados para la protección de los sectores públicos y privados. El Gobierno colaborará estableciendo estándares para la infraestructura de administración de claves y proveerá un mercado para productos de seguridad.

Resulta claro para las comunidades legales y técnicas de los Estados Unidos que el comercio electrónico requerirá mayor autenticación y certificación de los documentos electrónicos para asegurar la aceptación de los actos. Esto es particularmente cierto para aplicaciones comerciales en el ámbito internacional, donde de las diferencias en el derecho y la práctica, y las dificultades en establecer relaciones entre partes, aumentan la necesidad de mecanismos que brinden seguridad a las transacciones. El futuro del comercio electrónico internacional descansa en la importancia que los contratantes otorguen a la seguridad de la transmisión y contenido de la comunicación, y en la creencia de que esas

comunicaciones tendrán garantizado un adecuado reconocimiento que asegure su aceptación en cualquier jurisdicción, ya sea local o extranjera.

El proyecto Cybernotario propone rectificar la ausencia de seguridad en las transacciones originadas en los Estados Unidos, así como las que se realicen electrónicamente a través de la creación de una oficina "cuasi pública" conocida como cybernotario, cuyo rol será el de combinar experiencia legal y técnica en una sola especialización, y cuyos miembros ejercerán dos funciones distintas pero complementarias.

La primera de esas funciones permitirá que los actos pasados por ante el cybernotario tengan pleno reconocimiento y efectos fuera de los Estados Unidos. La segunda y más importante función surgirá de su capacidad de certificación y autenticación electrónicas de todos los elementos de una transacción comercial electrónica, indispensables para su aceptación por el derecho de los Estados Unidos y de los demás países. Mediante la utilización de la firma digital, el cybernotario, podrá certificar la identidad del emisor de un mensaje, lo que implica la imposibilidad de repudiar el mensaje, dan un alto nivel de seguridad en cuanto al contenido del mismo, fechar la notarización (fecha y hora de su intervención), y su protocolización con fines de archivo.

COLOFON

A lo largo de todo este trabajo hemos hecho referencia a la falta de tipificación específica, en nuestro país, de ciertas conductas ilícitas, sumamente perjudiciales para el patrimonio en su totalidad.

Hemos deslizado también la opinión del profesor Tiedemann, para quien, uno de los motivos por los cuales no existen normas específicas que sancionen este tipo de delitos, se debe a los intereses de poderosos grupos que influyen sobre los órganos legislativos, opinión con la que respetuosamente no coincidimos por estimar que los baches normativos a que éste refiere no se deben a las mencionadas presiones, sino, a la falta de capacitación en el tema informático que trae aparejado la desregulación de conductas cometidas por medio de maquinarias informatizadas, cuya evolución -en la mayoría de los casos- supera nuestro marco normativo legal vigente.

Asimismo se suma a ello la falta de especialización en el tema en análisis de quienes deben dar respuestas a la necesidad de tutelar los bienes jurídicos que

se afectan por esta nueva forma de delinquir, no obstante tener como modelo países, que si bien no ofrecen las mayores garantías, han establecido un notorio mejoramiento en este sentido implementando normas típicas que describen con claridad y suficiencia las figuras delictivas originadas por la informatización en la mayoría de sus relaciones internas e internacionales.

También abona esta deuda legislativa los diferentes problemas económicos y sociales por el que atraviesa nuestro país. En el primero de los casos el elevado costo que insume la instalación de diversas maquinarias, instituciones y especialistas hace que deba tomarse una decisión política de riesgo para las autoridades de turno. En virtud del segundo planteo efectuado en este párrafo, o sea el social, el incremento monetario que significaría un adelanto en la materia recrudecería la crisis social, pues se deberían distraer al menos por un largo período, las necesidades básicas de nuestra sociedad.

Por ello creemos firmemente que, aún cuando la aparición de delitos informáticos circula a una velocidad mayor que la de los legisladores en el campo preventivo y punitivo, es menester, al menos en nuestro país, comenzar creando tipos penales que describan conductas que ya son harto conocidas, como lo vienen haciendo países como Alemania, España y Estados Unidos, tal cual se refleja en los artículos incluidos en sus Códigos Penales, cuya transcripción hemos realizado en el presente trabajo.

Creemos en el dinamismo del derecho, por ello vemos una despreocupación acentuada en nuestros legisladores, que conforme lo investigado, toleran la petrificación de normas que ni siquiera integran nuestro digesto penal, sino que se encuentran contenidas por ejemplo en la ley de propiedad intelectual.

Asimismo y ante el letargo legislativo, nuestra jurisprudencia mayoritaria ha tenido que echar mano a la analogía, que si bien es permitida "in bonam parte", no la creemos conveniente; como también vemos desfavorable que nuestros doctrinarios se debatan en argumentos defensivos y estériles al tratar de encuadrar conductas atípicas realizadas a través de maquinarias informatizadas, únicamente dentro de dos tipos penales como lo son el Hurto y la Estafa.

Además de la analogía a la que hicimos referencia precedentemente, a la cual creemos que no será necesario acudir de existir normas que contengan específicamente las conductas disvaliosas en torno a este tema. No deberemos

caer tampoco, como lo ha hecho la ley de propiedad intelectual, en las llamadas leyes penales en blanco.

No debemos olvidar, al crear estas normas, el principio de legalidad acuñado en nuestra Carta Magna, que nos exige la investigación profunda, amplia y total de todos y cada uno de los hechos de carácter delictivo que lleguen a conocimiento de las Instituciones con jurisdicción para juzgarlos, siendo necesario para ello la creación de estas normas específicas para no desvirtuar este principio Constitucional, como creemos que, actualmente y en la mayoría de los casos, dejamos de lado.

Vemos con gran asombro que la mayoría de la doctrina y jurisprudencia se ha inclinado en encuadrar este tipo de acciones bajo el Art. 162 del Código Penal, el que establece una pena máxima de dos años de prisión, y teniendo en cuenta lo gravoso y perjudicial del detrimento patrimonial, que resulta de la comisión de la mayoría de los delitos que se cometen a través de la informática, nos parece demasiado benévola la pena que establece la referida norma, por lo que, con más razón es imperiosa la necesidad de la creación de las figuras penales que venimos pregonando.

Admitimos necesaria la creación de un capítulo específico dentro del digesto penal vigente donde debería asentarse un articulado referido con exclusividad a los delitos sobre los que nos venimos refiriendo.

Que ello así planteado no hace mas que echar por tierra nuestro convencimiento al comenzar este trabajo, por cuanto la introducción de la informática en los distintos niveles de nuestra sociedad no puede, al menos en forma inmediata, traer aparejada la seguridad que creemos perdida o deficiente, tal cual fuera planteado en nuestra idea original.

Por consiguiente luego de analizar la diversa bibliografía consultada, advertimos que países de mayor desarrollo tecnológico nos han demostrado que con intencionalidad, buen criterio y decisión política han logrado recuperar parte de esa seguridad que pretendemos. También vemos con optimismo que si en nuestro país logramos salir del letargo legislativo en que nos encontramos, creando normas autónomas que describan claramente el accionar de quienes por

medio de su capacitación personal o no, vulneran los mecanismos de control, que en algunos sectores, al menos, se han implementado como desarrollo tecnológico, podremos restablecer parte de la seguridad perdida.

BIBLIOGRAFIA

- "Congreso sobre Derecho Informático" - Año 1989 - Facultad de Derecho de Zaragoza - María Cinta Castillo Jiménez y Miguel Ramallo Romero.

- "Ley de Propiedad Intelectual" nº 11.723.

- "Programa Regional de Cooperación en Informática y Microelectrónica" - Año 1991 - Mario Barreto Gugelmeier.

- "Revista La Ley" - Año 1997 - nº 120 - "La estafa mediante medios mecanizados" - Sandro F. Abraldes.

- "Revista La Ley" - Año 1997 - nº 76 - "Banca, Comercio, Moneda Electrónica y la firma digital" - Horacio M. Lynch.

- "Delincuencia Informática: El software como objeto de conductas disvaliosas" - por Carlos Alberto Cruz.

- "Delincuencia Informática" - Santiago Mir Puig.

- "Revista del Derecho Industrial" - Año 1995 - Nº 21 - Editorial Depalma.

La Regulación de los Datos Sensibles en la Directiva 95/46/CE

JULIO JOSE ELIAS BATURONES

Licenciado en Derecho y experto en Criminología

1.- Introducción.

La verdad es que el presente estudio constituye la continuación de uno anterior, en el que mostraba mi interés en analizar como la Ley Española de protección de datos, que respondía a la exigencia constitucional del art. 18.4 de la CE, venía a suponer un retroceso en el ámbito de protección de los derechos fundamentales de las personas en la cuestión de los llamados "datos sensibles", respecto al "mínimo irreductible" previsto en el Convenio 108, que de igual forma, era parte integrante del ordenamiento jurídico interno al haber sido expresamente ratificado y firmado por España.

Pues bien, creo importante completar el tema de los datos sensibles, el principio de consentimiento y sus excepciones, en la Directiva de la CEE, ya que a mi juicio, de la regulación contemplada en la misma en los artículos 7 y 8, se prevé un catalogo de excepciones que posibilita, en el marco de la necesaria reforma legislativa de la ley española para su adaptación a los objetivos y fines de dicha directiva, una merma, aún mayor, de la protección de datos tan fundamentales y básicos; para ello resultará trascendental contrastar el desarrollo positivo de cada una de las diferentes normativas, para darse uno cuenta que abre el abanico de posibilidades, para que por cualquier Estado de la CEE, y en concreto, nuestro país, pueda establecer mayores excepciones en orden a tratar datos sensibles, como las creencias religiosas, la salud, etc... sin necesidad de exigir el previo consentimiento del interesado por razones de diversa índole, que a mi juicio son, como menos, de muy dudosa justificación.

Sin embargo, y con carácter previo a terminar este estudio con mis propias conclusiones, considero que hay que tener en cuenta que las tres normativas vigentes hasta la fecha sobre este tema, son de naturaleza jurídica diferente: Una ley propia que es directamente aplicable, un Convenio europeo (de los países del Consejo de Europa) que establece un marco de reglas básicas sobre protección de datos, que expresamente reconoce que cada Estado debe concretar específicamente tales objetivos y principios, y por último, la Directiva, que como sabemos, obligaría al Estado miembro de la CEE, en este caso, España, en cuanto al resultado a obtener, pero dejando a su elección la forma y medios a emplear, siendo únicamente vínculante el resultado y no los medios.

Dicho de otro modo, que nos encontraríamos con tres normativas, que afectan a este país, por ser la legislación propia, y por pertenecer tanto al Consejo de Europa como a la Comunidad Económica Europea, de distinto espectro de protección y de diferente carácter jurídico, sucesivo en el tiempo; la cuestión será como conjugar los tres factores, en orden a que cumpliendo con sus reglas, no queden desfavorecidos los ciudadanos en su protección.

2.- Estudio concreto de los artículos 7 y 8 de la Directiva, sobre el principio del consentimiento y datos sensibles.

La Directiva 95/46/CE, antes de desarrollar sus disposiciones legales sobre la materia de protección de las personas físicas, en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, tal como viene enunciada, contempla en un número de 72, considerandos que a manera de exposición de motivos, justifica los objetivos a alcanzar en la misma, y concretamente, respecto a los datos sensibles, creo importante destacar los siguientes:

"(30) Considerando que para ser lícito el tratamiento de datos personales debe basarse en el consentimiento del interesado o ser necesario con vistas a la celebración o ejecución de un contrato que obligue al interesado, o para la observancia de una obligación legal o para el cumplimiento de una misión de interés público o para el ejercicio de la autoridad pública o incluso para la realización de un interés legítimo de una persona, siempre que no prevalezcan los intereses o los derechos y libertades del interesado; que, en particular, para asegurar el equilibrio de los intereses en juego, garantizando a la vez una competencia efectiva, los Estados miembros pueden precisar las condiciones en las que se podrán utilizar y comunicar a terceros datos de carácter personal, en el desempeño de actividades legítimas de gestión ordinaria de empresas y otras entidades; que los Estados miembros pueden asimismo establecer previamente las

condiciones en que pueden efectuarse comunicaciones de datos personales a terceros con fines de prospección comercial o de prospección realizada por una institución benéfica u otras asociaciones o fundaciones, por ejemplo de carácter político, dentro del respeto de las disposiciones que permiten a los interesados oponerse, sin alegar los motivos y sin gastos, el tratamiento de los datos que les conciernan;

Considerando que un tratamiento de datos personales debe estimarse lícito cuando se efectúa con el fin de proteger un interés esencial para la vida del interesado;

Considerando que corresponde a las legislaciones nacionales determinar si el responsable del tratamiento que tiene conferida una misión de interés público o inherente al ejercicio del poder público, debe ser una administración pública u otra persona de derecho público o privado, como, por ejemplo una asociación profesional;"

A estos objetivos, la Directiva, en su sección II, del Capítulo II, bajo el título "principios relativos a la legitimación del tratamiento de datos", regula en su artículo 7 el principio del "consentimiento", en los siguientes términos:

"Los Estados miembros dispondrán que el tratamiento de datos personales sólo pueda efectuarse si:

el interesado ha dado su consentimiento de forma inequívoca, o

es 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, o

es necesario para el cumplimiento de una obligación jurídica a la que está sujeto el responsable del tratamiento, o

es necesario para proteger el interés vital del interesado, o

es 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, o

es necesario para la satisfacción del interés legítimo perseguido por el responsable del tratamiento o por el tercero o terceros a los que se comuniquen los datos, siempre que no prevalezca el interés o los derechos y libertades fundamentales del interesado que requieran protección con arreglo al apartado 1 del artículo 1 de la presente Directiva."

En este sentido, el apartado 1 del artículo 1, dice lo siguiente:

"Los Estados miembros garantizarán, con arreglo a las disposiciones de la presente Directiva, la protección de las libertades y de los derechos fundamentales de las personas físicas, y, en particular, del derecho a la intimidad, en lo que respecta al tratamiento de los datos personales."

En lo que respecta a los "datos sensibles", que en la Directiva se conocen bajo la denominación "categorías especiales de datos", con carácter previo a ver el contenido del artículo 8, es conveniente tener en cuenta los siguientes considerandos:

"(33). Considerando, por lo demás, que los datos que por su naturaleza puedan atentar contra las libertades fundamentales o la intimidad no deben ser objeto de tratamiento alguno, salvo en caso de que el interesado haya dado su consentimiento explícito; que deberán constar de forma explícita las excepciones a esta prohibición para necesidades específicas, en particular cuando el tratamiento de dichos datos se realice con fines relacionados con la salud, por parte de personas físicas sometidas a una obligación legal de secreto profesional o para actividades legítimas por parte de ciertas asociaciones o fundaciones cuyo objetivo sea hacer posible el ejercicio de las libertades fundamentales,

(34). Considerando que también se deberá autorizar a los Estados miembros, cuando esté justificado por razones de interés público importante, a hacer excepciones a la prohibición de tratar categorías sensibles de datos en sectores como la salud pública y la protección social, particularmente en lo relativo a la garantía de la calidad y la rentabilidad, así como los procedimientos utilizados para resolver las reclamaciones de prestaciones y de servicios en el régimen del seguro de enfermedad, la investigación científica y las estadísticas públicas; que a ellos corresponde, no obstante, prever las garantías apropiadas y específicas a los fines de proteger los derechos fundamentales y la vida privada de las personas;

(35). Considerando, además, que el tratamiento de datos personales por parte de las autoridades públicas con fines, establecidos en el Derecho constitucional o en el Derecho internacional público, de asociaciones religiosas reconocidas oficialmente, se realiza por motivos importantes de interés público;

(36). Considerando que, si en el marco de actividades relacionadas con las elecciones, el funcionamiento del sistema democrático en algunos Estados miembros exige que los partidos políticos recaben datos sobre la ideología política de los ciudadanos, podrá autorizarse el

tratamiento de estos datos por motivos importantes de interés público, siempre que se establezcan las garantías adecuadas;"

Siguiendo con la misma sistemática que en el caso anterior, el artículo 8 de la Directiva desarrolla normativamente estos principios, de la siguiente forma:

"1.- Los Estados miembros prohibirán el tratamiento 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.

2.- Lo dispuesto en el apartado 1 no se aplicará cuando:

el interesado haya dado su consentimiento explícito a dicho tratamiento, salvo en los casos en los que la legislación del Estado miembro disponga que la prohibición establecida en el apartado 1 no pueda levantarse con el consentimiento del interesado, o

el tratamiento sea necesario para respetar las obligaciones y derechos específicos del responsable del tratamiento en materia de Derecho laboral en la medida en que esté autorizado por la legislación y ésta prevea garantías adecuadas, o

el tratamiento sea necesario para salvaguardar el interés del interesado o de otra persona, en el supuesto de que el interesado esté física o jurídicamente incapacitado para dar su consentimiento, o

el tratamiento sea efectuado en el curso de sus actividades legítimas y con las 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 consentimiento de los interesados, o

el tratamiento se refiera a datos que el interesado haya hecho manifiestamente públicos o sea necesario para el reconocimiento, ejercicio o defensa de un derecho en un procedimiento judicial.

3.- El apartado 1 no se aplicará cuando el tratamiento de datos resulte necesario para la prevención o para el diagnóstico médicos, la prestación de asistencia sanitaria o tratamientos médicos, o la gestión de servicios sanitarios, siempre que dicho tratamiento de datos sea realizado

por 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;

4.- Siempre que dispongan las garantías adecuadas, los Estados miembros podrán, por motivos de interés público importantes, establecer otras excepciones, además de las previstas en el apartado 2, bien mediante su legislación nacional, bien por decisión de la autoridad de control.

5.- El tratamiento de datos relativos a infracciones, condenas penales o medidas de seguridad, sólo podrán efectuarse bajo el control de la autoridad pública o si hay previstas garantías específicas en el Derecho nacional, sin perjuicio de las excepciones que podrá establecer el Estado miembro basándose en disposiciones nacionales que prevean garantías apropiadas y específicas. Sin embargo, sólo podrá llevarse a cabo un registro completo de condenas penales bajo el control de los poderes públicos.

Los Estados miembros podrán establecer que el tratamiento de datos relativos a sanciones administrativas o procesos civiles se realicen asimismo bajo el control de los poderes públicos.

6.- Las excepciones a las disposiciones del apartado 1 que establecen los apartados 4 y 5 se notificarán a la Comisión.

7.- Los Estados miembros determinarán las condiciones en las que un número nacional de identificación o cualquier otro medio de identificación de carácter general podrá ser objeto de tratamiento."

3.- Las disfunciones de la Directiva en esta materia respecto a otras regulaciones.

Con el Convenio 108 del Consejo de Europa de protección de las personas en relación con el tratamiento automatizado de datos de carácter personal.

El artículo 6 del Convenio regula, bajo la denominación "categorías particulares de datos", los denominados "datos sensibles", con la siguiente redacción:

"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."

Por lo tanto se puede decir, que del estudio comparativo entre la regulación de los datos sensibles en el Convenio 108 del Consejo de Europa, y el art. 8 de la Directiva de la CEE, nos encontramos con que existen supuestos coincidentes de los datos a proteger, en concreto "el origen racial, las opiniones políticas, las convicciones religiosas, y la salud", así como "vida sexual", en expresión del Convenio, y "la sexualidad", término que utiliza la Directiva, pero que claramente se puede considerar sinónimo o equivalente.

Las diferencias son las siguientes:

En el Convenio 108, se hace referencia a "u otras convicciones", mientras que en la Directiva solo menciona en este apartado "las convicciones filosóficas"; sería cuestión de interpretación si podríamos pensar que junto con las religiosas y filosóficas, que se recogen en la Directiva y que formaría parte de lo contemplado en el Convenio 108, además en este último, pueden preverse otros supuestos diferentes de convicciones, como por ejemplo de tipo ético, o incluso de conciencia; así, la persona, objetor de conciencia respecto a la prestación del servicio militar, ¿estaría protegida su convicción personal dentro del apartado "filosóficas" de la Directiva?: a mi juicio resultaría dudoso afirmarlo, mientras que no cabría ningún tipo de dudas respecto a su protección por el Convenio Europeo, ya que al utilizar una expresión genérica como "otras convicciones", tiene la virtud de no limitar sus particulares supuestos.

Por otro lado, en el Convenio 108 regula un supuesto de dato a proteger, que no tiene el mismo parangón con la Directiva, y es en el punto relativo a "datos de carácter personal referentes a condenas penales", ya que prohibe expresamente su tratamiento automatizado "a menos que el derecho interno prevea garantías apropiadas".

En cambio, en la Directiva, por lo pronto, no se contemplan tales datos en su apartado primero del artículo 8, como hemos podido observar, lo que demuestra que en esta normativa no se le equipara con el mismo valor que el resto de los datos sensibles, que sí son recogidos; ahora bien, hay que reconocer

que en este artículo tampoco es materia olvidada del todo, y en este sentido, volvamos a leer el apartado 5:

"El tratamiento de datos relativos a infracciones, condenas penales o medidas de seguridad, sólo podrán efectuarse bajo el control de la autoridad pública o si hay previstas garantías específicas en el Derecho nacional, sin perjuicio de las excepciones que podrá establecer el Estado miembro basándose en disposiciones nacionales que prevean garantías apropiadas y específicas. Sin embargo, sólo podrán llevarse a cabo un registro completo de condenas penales bajo el control de los poderes públicos."

Sin perjuicio de que en el apartado siguiente de este trabajo se vuelva a estudiar este apartado de la Directiva, cuando se contraste con la norma interna española, es decir, con la LORTAD, hay que decir, en primer lugar, que en la Directiva se habla de "infracciones, condenas penales o medidas de seguridad", mientras que en el Convenio 108 solo se recogen "las condenas penales", excluyendo por lo tanto las medidas de seguridad, o sea, que solo se etiqueta como dato especial a las infracciones penales más duras, como son las condenas penales, mientras que las medidas de seguridad, de carácter más leve en su respuesta normativa, no se le reconoce tal carácter; por lo tanto, en principio podríamos ver que en la Directiva se mejora el catálogo de protección al ampliar, en este supuesto, los datos a proteger con especial regulación, pero creo que no se debe caer en el error, por cuanto que lo que dice expresamente en la Directiva es que tales datos, en definitiva, pueden ser objeto de tratamiento automatizado, si es "bajo el control de la autoridad pública o si hay previstas garantías específicas en el Derecho nacional,...".

En segundo término, hay que tener en cuenta que en la Directiva, asímismo, en este apartado 5, del art. 8, continúa diciendo que "sin perjuicio de las excepciones que podrá establecer el Estado miembro basándose en disposiciones nacionales que prevean garantías apropiadas y específicas", lo que nos llevaría al estudio del artículo 7, apartado 5º de la LORTAD, que en su momento se verá, pero que a mi juicio supone abrir la posibilidad de tratar tales datos por parte de los organismos públicos con demasiada facultad para ello, en merma de la privacidad de las personas afectadas; además hay que tener en cuenta que en el Convenio 108 sólo, respecto a tales datos, se contempla un supuesto de excepción a su prohibición de tratamiento automatizado, en los términos contemplados en el apartado 2, letra a), del artículo 9, que dice lo siguiente:

"Será posible una excepción en las disposiciones de los artículos, 5º, 6º (en el que estarían los datos sensibles) y 8º del presente Convenio cuando tal excepción, prevista por la ley de la Parte, constituya una medida necesaria en una sociedad democrática:

para la protección de la seguridad del Estado, de la seguridad pública, para los intereses monetarios del Estado o para la represión de ***infracciones penales****".*

Ahora bien, lo que sí debe de reconocer, es que en la Directiva, se prevé en el párrafo segundo de este apartado 5, del art. 8, una exigencia de que "los Estados miembros podrán establecer que el tratamiento relativos a sanciones administrativas o procesos civiles se realicen asimismo bajo el control de los poderes públicos", lo que no se contempla en el Convenio Europeo; en este punto, creo que es muy importante dicho control, por cuanto de que de los datos que se pudiera acceder a su tratamiento automatizado de sanciones administrativas, como por ejemplo multas de tráfico, o tributarias, así como de los procesos civiles, especialmente determinante de un posible "perfil" de una persona, que por cuestiones personales y de coyuntura económica, como el paro, se encuentre con procesos sucesivos en el orden civil de reclamación de deudas, lo que si tuviera un acceso vía informática a determinadas entidades, como podían ser bancos, cajas de ahorros, etc., derivaría, claramente, no sólo en una intromisión en su vida privada, sino incluso, con unos perjuicios patrimoniales muy graves; no olvidemos la existencia, real, en el tráfico financiero, de las famosas listas de R.A.I, es decir, de impagados, que de entidad bancaria a otra de igual tipo suelen transmitirse, impidiendo en la mayoría de las ocasiones que se pueda salir de una situación económica difícil.

Sin perjuicio de lo anterior, también hay que destacar el hecho meritorio en la regulación de la Directiva, de contemplar un supuesto no previsto en el Convenio Europeo, como es "la pertenencia a sindicatos", como dato especialmente protegido.

Ahora bien, y se vuelve a repetir, como se decía en los datos relativos a las infracciones penales, la diferencia más transcendental en estas dos normativas, no es tanto cuántos supuestos concretos se consideran como "datos sensibles", ya que la realidad es que son más los coincidentes que los que dispares, sino que lo que de verdad diferencia es que en la Directiva, no obstante a la dicción ejemplar de su apartado primero del art. 8, en sus apartados segundo y siguientes, se prevén unas excepciones que por su amplitud, a mi juicio exagerada, en la práctica

puede convertir la exigencia de protección y prohibición de su primer apartado, en "papel mojado".

Por supuesto, tal enumeración prolija de excepciones de la Directiva, es muy superior a las básicas y escuetas contempladas en el art. 9 del Convenio Europeo, que sólo admite unos supuestos muy concretos regulados en las letras a) y b), de su apartado segundo, que como ya hemos recogido el primer grupo, en la letra a), paso a continuación a reproducir los previstos en la letra b) a efectos ilustrativos de lo que es objeto de crítica:

"para la protección de la persona concernida y de los derechos y libertades de otras personas".

Además, y para mayor escarnio de la protección a los datos sensibles, la Directiva comete el error caso, a mi juicio, de recoger en el apartado 4 del art. 8 que es objeto de comentario, una disposición que en su justa interpretación ampliar sin limitación alguna, los supuestos de excepción a la prohibición exigida en el apartado primero, del siguiente modo:

"Siempre que dispongan las garantías adecuadas, los Estados miembros podrán, por motivos de interés público importantes, establecer otras excepciones, además de las previstas en el apartado 2, bien mediante su legislación nacional, bien por decisión de la autoridad de control."

Por lo tanto, nos encontramos con un supuesto de concepto jurídico indeterminado como es el de "interés público importante"; realmente, me pregunto, ¿qué se quiere decir con esta expresión?, ¿cuántos supuestos pudiera abarcar en el ámbito de "interés público?, ¿quien delimita sus contornos?, etc....

Es en esta cuestión donde considero que la disfuncionalidad entre lo regulado en la Directiva respecto al Convenio 108 de Estrasburgo encuentra su punto álgido de colisión.

Con la ley española de protección de datos-LORTAD.

Como sabemos, con carácter tardío en el tiempo y motivado por exigencias más de tipo internacional que por necesidades internas, en cumplimiento de las previsiones del Acuerdo de Schengen de 14 de junio de 1985, se aprueba la Ley Orgánica 5/1992, de 29 de Octubre, de regulación del tratamiento automatizado de los datos de carácter personal, publicándose en el

B.O.E. de 31 de Octubre de 1992, por lo que se desarrolla, tras catorce años de vigencia, el articulo 18.4 de nuestra Constitución.

Pues bien, los artículos de la L.O.R.T.A.D (como vulgarmente se conoce a esta Ley, y que seguiremos en este trabajo para referirnos a la misma) que hace referencia al principio del consentimiento, por un lado, y los datos sensibles, son los números 6° y 7°, a lo que sumaré el 8°, relativo a la salud, por cuanto su contenido es de igual interés comparativo con las previsiones ya vistas en la Directiva comunitaria.

Comenzando con el estudio del principio del consentimiento, el artículo 6° de la L.O.R.T.A.D, tiene un contenido tanto en su aspecto principal, como en el catálogo de excepciones, que viene igualmente recogido en la Directiva, lo que inmediatamente explicaré con detalle:

"Consentimiento del afectado.- 1. El tratamiento automatizado de los datos de carácter personal requerirá el consentimiento del afectado, salvo que la Ley disponga otra cosa.".

En la Directiva 95/46/CE, en su artículo 7, letra a), se dice, como recordaremos, lo que sigue, respecto a esta cuestión:

"Los Estados miembros dispondrán que el tratamiento de datos personales sólo pueda efectuarse si:

el interesado ha dado su consentimiento de forma inequívoca, o.."

Por lo tanto, podemos afirmar que tanto en la Ley española como en la norma comunitaria, parten del mismo principio general de exigencia del consentimiento del afectado para el tratamiento automatizado de los datos de carácter personal.

Las diferencias empiezan a partir del desarrollo de las excepciones a tal principio, ya que en la L.O.R.T.A.D, en este artículo 6, apartado 2, se dice lo siguiente:

"No será preciso el consentimiento cuando los datos de carácter personal se recojan de fuentes accesibles al público, cuando se recojan para el ejercicio de las funciones propias de las Administraciones Públicas en el ámbito de sus competencias, ni cuando se refieran a personas vinculadas por una relación negocial, una relación laboral, una relación administrativa o un

contrato y sean necesarios para el mantenimiento de las relaciones o para el cumplimiento del contrato."

En la Directiva, prácticamente se reconocen las mismas excepciones, con la única variación respecto al párrafo relativo a que "se recojan de fuentes accesibles al público", cuyo contenido no está previsto exactamente en la misma, si bien podríamos considerar que se encontraría englobado tácitamente en la excepción prevista en la letra e) del artículo 7, que dice:

"o..., es 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..".

No obstante, reconozco que la cuestión no está clara, y que, en todo caso, es susceptible de interpretación o criterio personal, que es criticable, de que "las fuentes accesibles al público" pueda formar parte de "inherente al ejercicio del poder público".

Lo que sí resulta evidente, que la segunda excepción prevista en la Ley española, en el apartado 2, art. 6ª, es decir, "cuando se recojan para el ejercicio de las funciones propias de las Administraciones Públicas en el ámbito de sus competencias", coincide con la expresión utilizada en la normativa comunitaria de "inherente al ejercicio del poder público conferido al responsable del tratamiento", ya que realmente viene a decir lo mismo.

Otro supuesto similar, es la excepción del principio del consentimiento previsto en la L.O.R.T.A.D, que tiene la siguiente redacción:

"...ni cuando se refieran a personas vinculadas por una relación negocial, una relación laboral, una relación administrativa o un contrato y sean necesarios para el mantenimiento de las relaciones o para el cumplimiento del contrato"

Digo que es similar, ya que en la Directiva, en el artículo 7, letras b) y c), igualmente, viene a coincidir con la anterior redacción de la ley española, del siguiente modo:

"b) es 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, o

es necesario para el cumplimiento de una obligación jurídica a la que está sujeto el responsable del fichero.."

Lo único que habría que matizar, es que la expresión de la normativa española "relación laboral, administrativa o contrato", vendría a decir lo mismo que el término utilizado en la Directiva de "contrato y obligación jurídica", aunque en este último supuesto no diferencie si es de carácter negocial, es decir, civil, o laboral o relación administrativa.

Sí en cambio, llama la atención, que a diferencia de lo que ocurre con la redacción del articulo 6º, 2 de la L.O.R.T.A.D, en la Directiva, se prevean no sólo los supuestos de ejecución de las cláusulas contractuales propiamente dichas, sino incluso, las denominadas "medidas precontractuales adoptadas a petición del interesado", lo que a mi juicio escaparía de la relación estrictamente contractual o negocial aceptada por la ley española; es decir, nos encontraríamos de nuevo con una nueva posibilidad no prevista en la L.O.R.T.A.D.

Por otro lado, hay que destacar el hecho de que en la Directiva, se prevé otros dos supuestos de excepción, que en principio, no se recogen en nuestra propia normativa, en concreto, me refiero a las letras d) y f), que tiene el siguiente tenor literal:

"o..., es necesario para proteger el interés vital del interesado, o".

"es necesario para la satisfacción del interés legítimo perseguido por el responsable del tratamiento o por el tercero o terceros a los que se comuniquen los datos, siempre que no prevalezca el interés o los derechos y libertades fundamentales del interesado que requieran protección con arreglo al apartado 1 del artículo 1 de la presente Directiva".

Entrando en el análisis concreto de estas dos excepciones, que no son recogidas en la L.O.R.T.A.D, pero que como se verá más adelante, sería factible su recepción en un futuro muy próximo en estricto cumplimiento de la Directiva, tengo que decir dos cosas:

La primera, es que respecto a que el principio del consentimiento se deje de lado, en aras a la protección "del interés vital del interesado", resulta una obviedad, ya que es una causa de fuerza mayor o de necesidad que justificaría, a mi juicio, plenamente la excepción; por lo tanto es positivo su ampliación, sin perjuicio de los peligros que conllevaría una abusiva utilización de esta excepción

por parte del responsable de los datos, que no en todos los casos estuviera realmente justificada su acción; o dicho de otro modo, que debe utilizarse muy excepcionalmente, y en los supuestos indudablemente de "interés vital ", tal como viene enunciados.

La segunda, que no alcanzo a comprender realmente el significado real de lo previsto en la letra f) del art. 7 de la Directiva, ya que, ¿qué quiere decir que sea necesario para la satisfacción del interés legitimo perseguido por el responsable del tratamiento o por el tercero o terceros a los que se comuniquen los datos?; en verdad afirmo que no lo sé, y que más bien es un trabalenguas jurídico de muy difícil concreción, que en realidad esconde una peligrosa excepción al sacrosanto principio del consentimiento.

Además, se comete el craso error de confrontar tal "satisfacción", con "el interés o los derechos y libertades fundamentales del interesado", por lo que podríamos afirmar, que utilizando una expresión popular, "en la propia ley, tenemos la trampa", o con otras palabras, que a la postre, con esta facultad conferida a los Estados miembros, el principio general y fundamental para la protección de los datos, como es el del consentimiento del afectado, más bien quedaría vacío de contenido real en la práctica.

No hay que olvidar que en la L.O.R.T.A.D, en el artículo 6º objeto de comentario, se contempla una puerta abierta a esta funesta posibilidad, en concreto, en dos apartados y del siguiente modo:

Primero, al final del párrafo primero, que dice:

"El tratamiento automatizado requerirá el consentimiento del afectado, ***salvo que la Ley disponga otra cosa.****"*

Y en segundo lugar, en el apartado tercero del mismo artículo, que a su vez, tiene la siguiente redacción:

"El consentimiento a que se refiere el artículo podrá ser revocado cuando ***exista causa justificada para ello*** *y no se le atribuya efectos retroactivos:"*

Siguiendo con la misma sistemática, voy a entrar a continuación, con el estudio comparativo de los "datos sensibles", de la L.O.R.T.A.D respecto a la Directiva 95/46/CE.

El artículo 7º de la Ley española, aunque con diferencia de trato, recoge los siguientes "datos especialmente protegidos": "Ideología, religión, creencias, origen racial, salud, vida sexual, y datos de carácter personal relativos a la comisión de infracciones penales o administrativas".

En cambio, en el artículo 8, apartado primero de la Directiva, se recogen, además de los previstos en la L.O.R.T.A.D, "el origen étnico", junto con el racial, "las convicciones filosóficas", que sumadas a las religiosas, no estaría expresamente previstos en la ley española, y, especialmente, llamaría la atención de los datos relativos a "la pertenencia a sindicatos", cuya inclusión considero muy acertada.

Por otro lado, nos encontraríamos con otro hecho diferencial, respecto a las infracciones penales o administrativas, que en el supuesto previsto en el apartado 5, del articulo 8 de la Directiva, sólo contemplen las infracciones penales y no las administrativas, y sí en cambio, "medidas de seguridad", que considero no están expresamente protegidas en la L.O.R.T.A.D.

Es decir, que no obstante la similitud de los conceptos aludidos, se observan unas variaciones significativas en el catálogo de los datos sensibles, en el sentido de que en la Directiva se amplia el número de los mismos, lo que en principio, es un hecho positivo para la protección de los mismos.

Por otro lado, hay que destacar que, en la Directiva, como ocurría en el Convenio 108 del Consejo de Europa, no se observa una diferenciación de trato entre unos datos y otros, como ocurre en los apartados 2 y 3 del artículo 7º de la L.O.R.T.A.D, ya que, todos los contemplados en el párrafo primero del art. 8 están sometidos a la misma regla general de prohibición de su tratamiento automatizado, y exigiéndose su consentimiento para levantarla, según podemos ver del apartado segundo letra a) de dicho artículo:

"Lo dispuesto en el apartado 1 no se aplicará cuando:

el interesado haya dado su consentimiento explícito a dicho tratamiento, salvo en los casos en lo que la legislación del Estado miembro disponga que la prohibición establecida en el apartado 1 no pueda levantarse con el consentimiento del interesado, o..."

Llamo la atención de que en la normativa comunitaria, en principio, vuelvo a repetir, se observa un mayor grado de protección de los datos sensibles, en lo que se refiere al reforzamiento del principio del consentimiento, ya que incluso no solo se exige el consentimiento explícito del afectado para que pueda tratarse tales datos, sino que incluso faculta al Estado para que se disponga que ni siquiera con tal consentimiento expreso pueda levantarse la prohibición.

Sin embargo, en la Ley española, de la lectura de los apartados 1º al 3º del artículo 7º, se observa que no solamente no existe tal posibilidad, sino que incluso la exigencia del previo consentimiento del afectado no es exigible en todos los supuestos, sino que parece que exista un doble grado de protección, como si hubiera "datos más sensibles", que sí exigen el consentimiento expreso, en concreto "la ideología, religión y creencias", frente a otros "datos menos sensibles", como serían "el origen racial, la salud y la vida sexual", los cuales, mediante una Ley habilitadora, podrían ser susceptible de tratamiento, obviando la exigencia del previo consentimiento; veamos, en este sentido, la redacción de estos apartados:

"Art. 7º. Datos especialmente protegidos.

1.- De acuerdo con lo establecido en el apartado 2 del artículo 16 de la Constitución, nadie podrá ser obligado a declarar sobre su ideología, religión o creencias.

Cuando en relación con estos datos se proceda a recabar el consentimiento a que se refiere el apartado siguiente, se advertirá al interesado acerca de su derecho a no prestarlo.

2.- Sólo con ***consentimiento expreso y por escrito*** *del afectado podrán ser objeto de tratamiento automatizado los datos de carácter personal que revelen la ideología, religión y creencias.*

3.- Los datos de carácter personal que hagan referencia 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 disponga una ***Ley*** *o el afectado consienta expresamente."*

Es decir, que en este último grupo, no se dice "y el afectado consienta expresamente", como a mi juicio debería haber exigido la normativa española, sino que al poner la disyuntiva "o", se facultaría para que, no sólo no prohibirse taxativamente que, como se prevé en la Directiva, "la prohibición no pueda

levantarse con el consentimiento del interesado", sino que por lo contrario, pueda habilitarse legalmente para su tratamiento sin exigirse conjuntamente tal principio.

Ahora bien, a partir de este momento, la Directiva diferencia su nivel de protección en los datos sensibles, con carácter perjudicial respecto al nivel protegido en la actual redacción de la L.O.R.T.A.D, del siguiente modo:

Apartado 4, del artículo 7° de la Ley española:

"Quedan prohibidos los ficheros creados con la finalidad exclusiva de almacenar datos de carácter personal que revelen la ideología, religión, creencias, origen racial o la vida sexual".

En cambio, en los supuestos en que la Directiva exceptúa para la prohibición del tratamiento automatizado de los datos especiales del apartado 1, del artículo 8, en concreto, el contemplado en la letra d) podemos leer lo siguiente:

"Lo dispuesto en el apartado 1 no se aplicará cuando.

...el tratamiento sea efectuado en el curso de sus actividades legítimas y con las garantías por una fundación, una asociación o cualquier otro organismo si 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 lo datos no se comuniquen a terceros sin consentimiento de los interesados".

Dicho de otra forma, nos encontraríamos con otro supuesto de que si se cumpliera con la facultad prevista por la normativa comunitaria, dejaría en vacío la prohibición del apartado 4° del art. 7 de la L.O.R.T.A.D, ya que se estaría habilitando para que por parte de un partido político, o sindicato, u organización religiosa, o cuasireligiosa (pensemos en un momento en las múltiples sectas que han surgidos en los últimos tiempos) se almacenaran datos personales, no ya sólo de sus miembros, que en sí es muy peligroso, sino incluso de los que se denominan "personas que mantengan contactos regulares", es decir, con simpatizantes entre otros, relativos a sus propias creencias.

Por otra parte, la Directiva contempla, en sus letras b), c), y e), supuestos de excepción a la prohibición del tratamiento de los datos, que por su contenido

podrían estar justificados, si bien, no están contemplados en la normativa española, y que son los siguientes:

"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 ésta prevea garantías adecuadas."

Al tratarse de una materia de Derecho laboral, entiendo que sólo puede hacer referencia a datos relativos a la "pertenencia a sindicatos", que no está previsto por la Ley española, por lo que no cabría su inclusión, o bien, a datos que se refieran a "la ideología", en este caso en su vertiente sindical, que en todo caso, y por expresa prohibición legal del apartado 2, del artículo 7° de la L.O.R.T.A.D, hasta que no se reforme, estaría expresamente prohibido, a no ser que consientan expresamente, y por escrito, los afectados para que se verifique tal tratamiento automatizado; lo que de todas formas nos encontraríamos, sería en una reforma legislativa que a mi juicio mermaría el nivel de protección actual en esta materia.

"c) el tratamiento sea necesario para salvaguardar el interés del interesado o de otra persona, en el supuesto de que el interesado esté física o jurídicamente incapacitado para dar su consentimiento".

Este apartado de la Directiva contempla un supuesto no previsto en la Ley española, es decir, qué ocurriría en los casos en que el interesado no pueda prestar el consentimiento por estar física o jurídicamente incapacitado para prestarlo, y ser necesario para salvaguardar su interés; sin embargo, se olvida que en estos supuestos, estas personas no deben de quedar al amparo o arbitrio del responsable del tratamiento de sus datos para que considere oportuno utilizar sus datos, por cuanto que no obstante estar física o jurídicamente incapacitado para prestar el consentimiento, se debe recurrir a las vías civiles en donde precisamente para salvaguardar sus derechos más fundamentales, existen medios de completar su deficiencia, como son el nombramiento de defensores judiciales, tutorías, etc., con carácter general.

Por lo tanto, creo que está mal contemplado este apartado, ya que lo primero sería demostrar su incapacidad, física o jurídica, para no prestar el consentimiento, y en segundo término, si fuera así, no debe en ningún caso suplantar la función de salvaguarda de los intereses del incapaz por parte del propio responsable del tratamiento, porque dejaría a éste en clara indefensión, aparte de irrogarle claros perjuicios.

De hecho, y con carácter analógico, en la normativa española nos encontramos con un supuesto muy similar relativo a la salud de una persona, cuando en una situación límite, el afectado no está capacitado para dar su consentimiento al tratamiento "médico"; me refiero a lo que se dispone en el artículo 10º, apartado 6, letra b) de la Ley 14/1.986, de 25 de abril, General de Sanidad, que dice lo siguiente:

"Todos tienen los siguientes derechos con respecto a las distintas administraciones públicas sanitarias:

....

A la libre elección entre las opciones que se le presente el responsable médico de su caso y siendo preciso el previo consentimiento escrito del usuario para la realización de cualquier intervención, excepto en los siguientes casos:

...

Cuando no esté capacitado para tomar decisiones, en cuyo caso el derecho ***corresponderá a sus familiares o personas a él allegadas.***"

Es decir, si en estos supuestos se exigiría la intervención supletoria de los familiares o personas allegadas, siendo evidentemente, unos casos más graves que el tratamiento automatizado de datos personales, ya que afecta no a la intimidad, sino incluso a la propia vida o integridad del afectado, más razón habría para que fueran estas personas quienes prestará el consentimiento en el caso previsto en la norma comunitaria, y no el responsable del tratamiento del dato en cuestión.

Por último, y en tercer lugar, la letra e) del apartado 2, del artículo 8, contempla la siguiente excepción:

"el tratamiento se refiera a datos que el interesado haya hecho manifiestamente públicos o sea necesario para el reconocimiento, ejercicio o defensa de un derecho en un procedimiento judicial".

Tampoco en la Ley española se contempla esta posibilidad, que en cierto modo me deja un tanto perplejo, ya que si lo que se trata es de proteger unos datos personales que por su especial importancia y transcendencia en la vida intima de los afectado, se prohibe su tratamiento automatizado, a no ser que expresamente consienta, ¿qué tiene que ver que lo haya hecho público o no?, y ¿hasta qué punto es necesario su tratamiento automatizado para que se reconozca, se ejercite o se defienda un presunto derecho en un procedimiento judicial?; es

decir, que la Directiva contempla una vez más, y de forma peligrosa para la protección de los datos sensibles, unos supuestos de excepción al tratamiento de tales datos, en aras a unas justificaciones un tanto dudosas, como menos, y como mayor crítica, se puede decir que si se contemplara en un futuro en la legislación española, difícilmente se protegerían en la realidad tales datos, sobre todo teniendo en cuenta el alto nivel de definición y concreción de tales conceptos.

En general, por lo tanto, podemos decir que la diferencia cualitativa más importante entre lo regulado en la L.O.R.T.A.D y en la Directiva 95/46/CE, es precisamente, este cuadro de excepciones a la prohibición del tratamiento y de la previa exigencia del principio del consentimiento, que se contempla en la Directiva, que no estando hasta la fecha contemplado en la ley española, sin embargo, puede servir de motivo, y de exigencia, para su reforma a fin de adecuarse a los objetivos perseguidos en esta normativa, lo que sería muy perjudicial en el nivel mínimo de protección que estamos gozando.

Además no podemos olvidar, que sin perjuicio de que este "cuadro", en principio se encuentra limitado en los cinco supuestos ya estudiados, en cambio, y como ya se decía en el capítulo anterior, hay que tener en cuenta que el apartado 4, de este artículo 8 faculta a los "Estados miembros, por motivos de interés público importante" y con "las garantías adecuadas,...establecer otras excepciones, además de las previstas en el apartado 2, bien mediante su legislación nacional, bien por decisión de la autoridad de control"; por lo que el peligro anunciado se agrava aún más.

No quisiera terminar este apartado, sin analizar un último supuesto, que es el relativo a la salud, y concretamente, contrastar lo contemplado en la Directiva y en la norma española.

En este tema considero que existe una gran proximidad entre lo previsto en el apartado 3, del artículo 8 de la Directiva, y el artículo 8° de la L.O.R.T.A.D.; veamos el contenido de ambas regulaciones:

En la Directiva:

"El apartado 1 no se aplicará cuando el tratamiento de datos resulte necesario para la prevención o para el diagnóstico médicos, la prestación de asistencia sanitaria o tratamientos médicos, o la gestión de servicios sanitarios, siempre que dicho tratamiento de datos sea realizado por 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."

En la L.O.R.T.A.D:

"Sin perjuicio de lo que se dispone en el artículo 11 respecto de la cesión, las instituciones y los centros sanitarios públicos y privados y los profesionales correspondientes podrán proceder al tratamiento automatizado de los datos de carácter personal relativos a la salud de las personas que a ellos acudan o hayan de ser tratados en los mismos, de acuerdo con lo dispuesto en los artículos 8, 10, 23 y 61 de la Ley 14/1986, de 25 de abril, General de Sanidad; 85.5, 96 y 98 de la Ley 25/1.990, de 20 de diciembre, del Medicamento; 2, 3 y 4 de la Ley Orgánica 3/1986, de 14 de abril de medidas especiales en materia de Salud Pública, y demás leyes sanitarias."

En concreto, y dentro de las normativas ordinarias españolas que se citan, merecen destacarse los siguientes artículos:

1.- De la Ley 14/1986, de 25 de abril.

Artículo 10. " Todos tienen los siguientes derechos con respecto a las distintas administraciones públicas sanitarias:

...

A la confidencialidad de toda la información relacionada con su proceso y con su estancia en instituciones sanitarias públicas y privadas que colaboren con el sistema público."

Artículo 61. "En cada Área de Salud debe procurarse la máxima integración de la información relativa a cada paciente, por lo que el principio de historia clínico-sanitaria única por cada uno deberá mantenerse al menos, dentro de los límites de cada institución asistencial. Estará a disposición de los enfermos y de los facultativos que directamente estén implicados en el diagnóstico y el tratamiento del enfermo, así como a efectos de inspección médica o para fines científicos, debiendo quedar plenamente garantizados el derecho del enfermo a su intimidad personal y familiar y el deber de guardar el secreto por quien, en virtud de sus competencias, tenga acceso a la historia clínica. Los poderes públicos adoptarán las medidas precisas para garantizar dichos derechos y deberes."

De la Ley 25/1990, de 20 de diciembre, del Medicamento:

"Art. 85. Receta....5.- Los trámites a que sean sometidas las recetas y órdenes médicas y especialmente en su ***tratamiento informático****, respetarán lo dispuesto en el artículo 10 de la Ley General de Sanidad."*

Por lo tanto, aunque parezca en un principio que tanto la norma comunitaria como la española, en esta cuestión de la permisión del tratamiento automatizado de datos de la salud, sean muy similares, la realidad es que no es así, si tenemos en cuenta la normativa de desarrollo a la que expresamente se remite el artículo 8, "in fine", por lo que las garantías previstas en la normativa interna es mayor que el margen de discrecionalidad que faculta la Directiva 95/46/CE, en el sentido de que esta permisión no solo debería garantizarse con la "presunta" profesionalidad de la persona encargada de su tratamiento, ya sea sanitario sujeto al secreto profesional o no, con todos los debidos respetos a estos profesionales, sino que el respeto a la confidencialidad de la salud debería estar por encima de una salvaguarda, un tanto ambigua, de "la prevención, diagnóstico médico, prestación de asistencia sanitaria, tratamientos médicos o gestión de servicios sanitarios", tal como se recoge en la Directiva.

Sólo en supuestos muy excepcionales y de grave peligro para la salud pública en general, como en las epidemias o peligros serios de contagio de enfermedades transmisibles, se debería aplicar esta excepción, para facilitar la prevención, tal como se recoge en la normativa española, en concreto, en los artículos 2ºy 3º de la Ley Orgánica 3/1986, de 14 de abril, de medidas especiales en materia de Salud Pública, y no con el carácter tan general contemplado en la Directiva; por lo tanto, y vuelvo a repetir, aunque ambas normativas parecen ser muy semejantes, si nos detenemos un poco en su alcance y contenidos, vemos que no es así.

En este sentido, voy a reseñar el contenido de los artículos 2º y 3º de la Ley Orgánica 3/1.986, ya que de su simple lectura, se entiende mejor lo expuesto:

"Art. 2º.- Las autoridades sanitarias competentes podrán adoptar medidas de reconocimiento, tratamiento, hospitalización o ***control*** *cuando se aprecien indicios racionales que permitan suponer la existencia de peligro para la salud de la población debido a la situación sanitaria concreta de una persona o grupo de personas o por las condiciones sanitarias en que se desarrolle una actividad.*

Art. 3º.- Con el fin de ***controlar*** *las enfermedades transmisibles, la autoridad sanitaria, además de realizar las acciones preventivas generales, podrá adoptar las medidas*

oportunas para el control de los enfermos, de las personas que estén o hayan estado en contacto con los mismos y del medio ambiente inmediato, así como las que se consideren necesarias en caso de riesgo de carácter transmisible.".

4.- Alcance normativo de las Directivas en los ordenamientos jurídicos internos.

La razón de ser de este capítulo, que he querido, premeditadamente, que tenga su cabida justamente al final del trabajo y con carácter previo a emitir mis conclusiones personales sobre la materia, es que estamos comentando las consecuencias jurídicas y repercusiones que puedan tener las normas de la Directiva 95/46/CE sobre la Legislación interna, y habrá por lo tanto, que tener en cuenta hasta qué punto, y desde el mismo momento de su publicación el Diario Oficial de la Comunidad Europea (DOCE), tiene o no aplicabilidad en las normas de cada Estado miembro.

Para empezar esta espinosa, pero a mi juicio, importante cuestión, hay que tener en cuenta lo que dispone el artículo 32 de la Directiva, que sirve de pórtico a las "Disposiciones Finales" de la misma:

"1.- Los Estados miembros adoptarán las disposiciones legales, reglamentarias y administrativas necesarias para dar cumplimiento a lo establecido en la presente Directiva, a más tardar al final de un período de tres años a partir de su adopción.

Cuando los Estados miembros adopten dichas disposiciones, éstas harán referencia a la presente Directiva o irán acompañadas de dicha referencia en su publicación oficial. Los Estados miembros establecerán las modalidades de la mencionada referencia.

2.- Los Estados miembros velarán por que todo tratamiento ya iniciado en la fecha de entrada en vigor de las disposiciones de Derecho nacional adoptadas en virtud de la presente Directiva se ajuste a dichas disposiciones dentro de un plazo de tres años a partir de dicha fecha. No obstante lo dispuesto en el párrafo primero, los Estados miembros podrán establecer que el tratamiento de datos que ya se encuentren incluidos en ficheros manuales en la fecha de entrada en vigor de las disposiciones nacionales adoptadas en aplicación de la presente Directiva, deba ajustarse a lo dispuesto en los artículos 6, 7 y 8 en un plazo de doce años a partir de la adopción de la misma. No obstante, los Estados miembros otorgarán al interesado, previa solicitud y, en particular, en el ejercicio de su derecho de acceso, el derecho que se rectifiquen, supriman o bloqueen los datos incompletos, inexactos o que hayan sido conservados de forma incompatible con los fines legítimos perseguidos por el responsable del tratamiento.

3.- No obstante lo dispuesto en el apartado 2, los Estados miembros podrán disponer, con sujeción a las garantías adecuadas, que los datos conservados únicamente a efectos de investigación histórica no deban ajustarse a lo dispuesto en los artículos 6, 7 y 8 de la presente Directiva.

4.- Los Estados miembros comunicarán a la Comisión el texto de las disposiciones de Derecho interno que adopten en el ámbito regulado por la presente Directiva."

Por lo tanto, de la redacción observada de este artículo 32, y muy especialmente de sus apartados primero y segundo, parece desprenderse que se presentaría el siguiente orden cronológico en orden a la obligación impuesta por la Directiva a los Estados miembros para que adopten su normativa interna a lo establecido en la misma:

Primero, respecto a lo más favorable para los interesados, es decir, aquellas limitaciones que tienen como objeto "el derecho de acceso, el derecho a que se rectifiquen, supriman o bloqueen los datos incompletos o inexactos o que hayan sido conservados de forma incompatible con los fines legítimos perseguidos por el responsable del tratamiento", el efecto es **inmediato**, desde la misma publicación de la Directiva.

Segundo, hay un plazo de **tres años**, que cumple por lo tanto, el próximo día 24 de Octubre de 1.998, en donde deberá modificarse **necesariamente** la Ley española para que se cumpla lo dispuesto en la Directiva.

Tercero, en un plazo sucesivo de otros **tres años,** o sea, antes de Octubre del 2001, los "tratamientos ya iniciados en la fecha de entrada en vigor de las disposiciones de Derecho nacional", deberán ajustarse a dichas disposiciones.

Y, por último, y en el caso anterior, cuando se trate de **ficheros manuales**, el plazo se ampliaría, respecto a su ajuste a lo dispuesto en los artículos 6, 7 y 8 (por lo tanto, en lo ya estudiado del principio del consentimiento y datos sensibles), hasta el plazo de **doce años** desde la fecha de entrada en vigor de la Directiva, es decir, el 24 de Octubre del 2007.

Son éstos, plazos que parece desprender que, en todo caso, y como se afirma por cierta doctrina, respecto a la eficacia jurídica directa de las directivas, que por lo pronto, no haya cambiado la legislación vigente hasta la fecha; sin

embargo, y a pesar del respeto que me debe esta orientación, creo que sería conveniente afirmar que la cuestión no es tan pacífica como en un principio se puede pensar.

Es hora, por lo tanto, de analizar la temática relativa a si la Directiva, como norma comunitaria, tiene o no una aplicación o efecto jurídico directo, y su repercusión en este sentido en los ordenamientos jurídicos de los Estados miembros.

Entre otras muchas, la Sentencia de la Sección Octava, Sala 3ª, del Tribunal Supremo, de fecha 25 de Septiembre de 1990 (R.A. 6.888), siendo ponente el Excmo. Sr. Hernández Santiago, en su fundamento jurídico 4º, resume con toda claridad las dos corrientes doctrinales sobre esta trascendental cuestión, en los siguientes términos:

"...la necesidad de que la Directiva en cuestión sea transcrita al Derecho interno no siendo posible que la directa pueda ser objeto de aplicación directa por los Tribunales de los Estados miembros por falta de un acto de recepción, cuestión la suscitada que refleja las dos posiciones que sobre el efecto directivo de las Directivas se han venido mantenido por la doctrina científica y que básicamente se puede sintetizar en quienes entienden que la Directiva es una norma que obliga únicamente al Estado y que precisa una actuación de éste para introducirla en su derecho interno(...) y los que consideran que la Directiva no ha de ser "recibida" en el orden jurídico interno de los Estados, sino que se integra en tal orden por su propia naturaleza(...) el Tribunal de Justicia de las Comunidades se ha decantado."

De esta forma, habría que reconocer que a favor de la primera línea doctrinal, es decir, la que considera que para que la Directiva tenga eficacia se necesita un acto normativo posterior del Estado miembro, o sea, que niega su eficacia directa, se encuentra la dicción literal del articulo 189 del Tratado de la Comunidad Económica Europea, que dice lo siguiente:

"Obligará al Estado miembro destinatario en cuanto al resultado que deba conseguirse, dejando, sin embargo, a las autoridades nacionales la elección de la forma y los medios".

No obstante, y como en esa misma sentencia se reconoce, el Tribunal de Justicia de las Comunidades Europeas, ha reconocido no ya sólo la primacía de tales normas comunitarias, sino que ésta es una consecuencia del efecto directo de

tales normas, y así lo explica el Tribunal Supremo, en la citada resolución, en su fundamento jurídico 5º:

"...habida consideración de que el artículo 395 del Acta de Adhesión establece que "los nuevos Estados miembros pondrán en vigor las medidas que sean necesarias para cumplir desde la adhesión las disposiciones de las Directivas y decisiones definidas en el artículo 189 (...), y recogiéndose en el artículo 2º, "Desde el momento de la adhesión (...) los actos adoptados por las Instituciones comunitarias obligarán a los nuevos Estados miembros (...) en las condiciones previstas en los Tratados y en el presente Acta", no parece que pueda existir obstáculo legal alguno que impida la aplicación legal al caso concreto, que aquí enjuiciamos, la Directiva...".

En otra sentencia del mismo Alto Tribunal, de su Sección 5ª, Sala 3ª, siendo su ponente el Excmo. Sr. González Navarro, de fecha 1 de Junio de 1990 (R.A. 6.307), puntualiza esta posición, en su fundamento jurídico sexto, del siguiente modo:

"(...) Este Tribunal debe añadir que no ignora la tendencia de las instituciones comunitarias a redactar Directivas cada vez más precisas que dejan un muy estrecho margen de maniobra a los Estados miembros (...) Tampoco ignora este Tribunal que en alguna ocasión el Tribunal de Justicia de la Comunidad Europea ha extendido el efecto de la aplicación directa a las Directivas, pero, en definitiva, aun en este posicionamiento jurisprudencial, el Tribunal de Luxemburgo lo que viene a decir es que "conviene examinar en cada caso si la naturaleza, la economía y los términos de la disposición en cuestión son susceptibles de producir efectos directos en las relaciones entre el destinatario y los terceros.."

Por lo tanto, una vez expuestas las dos tendencias doctrinales, que recoge el Tribunal Supremo, creo conveniente completar esta cuestión con la doctrina jurisprudencial del Tribunal de Justicia de las Comunidades Europeas, que tanto se hace referencia en los apartados reseñados de las resoluciones anteriores.

Remontándonos a unas décadas, se puede afirmar que desde el principio de la existencia de las Comunidades Europeas, el T.J.C.E ha establecido, con claridad nítida, el principio de la primacía del Derecho comunitario respecto al derecho interno de cada Estado miembro; así, se puede sintetizar esta doctrina en la sentencia *Costa versus E.N.E.L*, de fecha 15 de julio de 1.964, en el que se dice lo siguiente:

"Tal y como resulta del conjunto de estos elementos procedente de una fuente autónoma, el derecho nacido del Tratado, en razón de su naturaleza específica original, no puede oponérsele judicialmente un texto interno, de cualquier clase que sea, sin perder su carácter comunitario y sin que se cuestione la propia base jurídica de la Comunidad...La transferencia operada por los Estados, desde su ordenamiento jurídico interno al ordenamiento jurídico comunitario, de los derechos y obligaciones contenidos en las disposiciones del Tratado, implica, pues, una limitación definitiva de sus derechos soberanos, contra la cual no puede prevalecer un acto unilateral ulterior incompatible con la noción de Comunidad."

Ahora bien, lo que ocurre es que cuando el T.J.C.E se ha manifestado en relación a la eficacia directa de lo previsto en una Directiva, exige el cumplimiento de dos requisitos fundamentales: El primero, que el plazo de adaptación a la normativa interna haya vencido, y el segundo, que lo haya sido de forma incompleta o defectuosa.

Y no sólo se queda ahí, sino que el mismo T.J.C.E, ha establecido que, una vez cumplidos ambos requisitos, aún no siendo invocada la norma comunitaria por una persona afectada, el tribunal o juez del Estado miembro tendría la obligación de resolver teniendo en cuenta que, en todo caso, debe interpretar la norma interna a la luz de las disposiciones de la Directiva.

Así, por ejemplo, la Sentencia de 11 de Julio de 1.991 (*caso Verholen),* en su parte dispositiva, se puede leer lo que sigue:

"El Derecho Comunitario no se opone a que un órgano jurisdiccional nacional aprecie de oficio la conformidad de una normativa nacional con las disposiciones precisas e incondicionales de una Directiva cuando el plazo de adaptación del Derecho nacional a la misma haya vencido, en el caso de que el justiciable no haya invocado ante el órgano jurisdiccional los derechos que le confiere la Directiva"

Y en la importante sentencia de fecha 13 de Noviembre de 1990, conocida como caso *Marleasing*, en un apartado de la misma, se afirma, asimismo que:

"...de ello se desprende que, al aplicar el Derecho Nacional, ya sea disposiciones anteriores o posteriores a la Directiva, el órgano jurisdiccional nacional que deba interpretarla, está obligado a hacer todo lo posible a la luz de la letra y de la finalidad de la Directiva, para, al efectuar dicha interpretación, alcanzar el resultado a que se refiere la Directiva, y de esta forma, atenerse al párrafo tercero del art. 189 TCEE"

Para terminar con esta doctrina jurisprudencial del TJCE, creo conveniente citar la sentencia de 19 de noviembre de 1991, caso *Francovich*, ya que en la misma se puede observar, la siguiente puntualización, que considero muy acertado en la presente cuestión:

"...la facultad del Estado miembro de elegir entre una multiplicidad de medios posibles para conseguir el resultado prescrito por una Directiva no excluye la posibilidad, para los particulares, de alegar ante los órganos jurisdiccionales nacionales los derechos cuyo contenido puede determinarse con suficiente precisión basándose únicamente en las disposiciones de la Directiva".

Traigo a colación este párrafo entresacado de la sentencia del caso *Francovich*, ya que viene muy oportuno en relación a lo previsto en el apartado segundo, del artículo 32 de la Directiva 95/46/CE, "in fine", es decir, que cuando los interesados reclamen a sus Estados miembros "el derecho de acceso, y el derecho a que se rectifiquen, supriman o bloqueen los datos incompletos, inexactos o que hayan sido conservados de forma incompatible con los fines legítimos perseguidos por el responsable del tratamiento", en estos supuestos la Directiva es de directa e inmediata aplicación, sin necesidad de esperar los plazos de adaptación al principio enumerados.

De todo lo expuesto, creo conveniente resumir diciendo que si bien es cierto que la Directiva, por propia definición, y con carácter general, no es una norma de obligado cumplimiento y directamente aplicable en todos los Estados miembros, como ocurre, por lo contrario, con el **Reglamento**, ya que del propio tenor literal del artículo 189 del Tratado constitutivo de la C.E.E "obligaría en cuanto al resultado a obtener, dejando a los Estados miembros la elección de la forma y medios a emplear", no por ello quiere decir que, en nuestro caso, y respecto a la normativa propia, para el supuesto de que se incumplieron los plazos previstos, se dejen sin efecto las previsiones de la misma; y que además, los particulares podrán perfectamente hacer uso de las disposiciones de dicha Directiva para la defensa de sus intereses, aún contraviniendo lo dispuesto en la L.O.R.T.A.D, que no haya sido aún reformada para su adaptación a dicha norma.

Dicho de otro modo, que encontrándonos en la fecha en que estamos, muy cerca ya del primer plazo de tres años previsto, sin perjuicio de que se vaya a cumplir con lo exigido en el art. 32 de la Directiva, lo que está claro es que a partir del 24 de Octubre de 1.998, las normas de la misma serán de directa y

preferente aplicación en nuestro ordenamiento, por lo que tendrá que tenerse este hecho muy en cuenta respecto al tema objeto del presente estudio de los datos sensibles, por las disfunciones y variaciones ya examinadas, junto con los peligros inmediatos ya anunciados en cada caso concreto.

5.- Conclusiones personales.

La realidad es que a lo largo del presente trabajo, y en cada uno de los diferentes apartados y capítulos, he dejado constancia de mis criterios personales en relación con los puntos álgidos y conflictivos que la Directiva 95/46/CE, puede suponer en el tema de la protección de los datos sensibles, por lo que para finalizar, simplemente voy a esbozar unas cuestiones fundamentales, que a modo de epílogo, cerrará este estudio.

Por lo pronto, lo primero que quisiera llamar la atención es que la Directiva, efectivamente, enuncia una serie de objetivos en sus considerandos, que de su simple lectura, pudiera llevar al lector a pensar que viene a mejorar, de forma substancial, el marco de garantías y de protección de datos tan fundamentales como aquellos que revelen "el origen racional 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"; incluso de su contraste con lo previsto tanto en la L.O.R.T.A.D, como en el Convenio 108 del Consejo de Europa, hecho en Estrasburgo el 28 de Enero de 1981, efectivamente parece que sea así, aunque sólo sea por el hecho ya demostrado de que aumenta el número de datos considerados como especialmente "sensibles", como ocurre con "el origen étnico" y "la pertenencia a sindicatos".

Además esta aparente mejoría, vendría apoyada por otro factor como es la posibilidad, contemplada en la letra a), del apartado 2 del artículo 8 de la Directiva, en donde, como ya se ha analizado en profundidad, se refuerza la protección de los datos al prever la posibilidad de que los mismos no puedan ser tratados automatizadamente, incluso aunque sean objeto de expreso consentimiento.

En éstos y otros detalles, parecería que, efectivamente, a la hora de redactar los artículos de desarrollo de la Directiva, ésta cumpliría con el considerando número 11 de los que encabeza la misma, que tiene la siguiente redacción:

"Considerando que los principios de la protección de los derechos y libertades de las personas y en particular, del respeto a 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".

Sin embargo, y a mi juicio, después de entrar "en detalle", los artículos analizados de la Directiva, creo que esta mejoría no es más que pura apariencia, de la que no podemos caer en el engaño.

La razón fundamental por la que he llegado a esta conclusión, es que lo auténticamente importante en la protección de los datos sensibles, y sobre todo, en el respeto al principio del consentimiento, es que sus excepciones estén sometidas a un régimen estricto de necesidad, y a ser posible, reducidas al menor número posible para así evitar la situación, que puede desgraciadamente plantearse, de que al final se deje sin protección real a estos datos, ante un número excesivo de supuestos excepcionales en donde sí cabe su tratamiento automatizado.

En este sentido tendrían cabida los supuestos ya contemplados de las letras a) hasta la f) del articulo 7, respecto al principio del consentimiento, así como de las excepciones, claramente excesivas a mi modo de ver, previstas en el apartado 2 y siguientes del articulo 8, respecto a los datos "sensibles", o "especiales", siguiendo la terminología empleada por la Directiva.

Especialmente grave sería el supuesto contemplado en el apartado 4 de dicho artículo 8°, donde como se recordará, se abría la posibilidad a los Estados miembros de que "por motivos de interés público importantes" establecer otras excepciones, eso sí, "disponiendo de las garantías adecuadas".

Con este apartado se facultaría a España para que reformara su normativa interna en materia de protección de datos, es decir, la L.O.R.T.A.D, y más concretamente, en la materia del presente estudio, los artículos 6° y siguientes, en aras de este principio de "interés público", olvidando que en nuestra legislación interna, y formando parte de la misma, nos vincula los preceptos y normas establecidas en el Convenio 108 de Europa, en donde, como asimismo hemos observado, en su artículo 9° sólo admiten unos supuestos taxativos para dicha excepcionalidad, no encontrando cabida "el interés público" entre ellos, por ser un concepto jurídico indeterminado y de imposible concreción, que admitirá

cualquier tipo de motivación, por muy peregrina que sea, para justificar el tratamiento de un dato sensible sin las debidas garantías para el afectado.

En este sentido, creo importante citar un texto obtenido de la "Memoria explicativa" del Convenio 108, en su apartado 20, que dice lo siguiente:

"La parte central del proyecto de convenio es el capítulo II, que contiene los principios básicos de protección de datos. Cada parte deberá adoptar las medidas necesarias para dar cumplimiento a este ***"núcleo irreductible"*** *en su legislación interna.*

Hay que señalar que el convenio contiene indicaciones claras y precisas sobre el objetivo de cada principio, dejando a cada Parte la modalidad concreta de ejecutarlo dentro de su Derecho Interno.

Los principios del "núcleo irreductible" reconocen a los interesados en todos los Estados en los cuales se aplique el Convenio un determinado mínimo de protección con relación al tratamiento automatizado de datos de carácter personal (...) Por otra parte, el "núcleo irreductible" dará lugar a una armonización de las legislaciones de los Estados contratantes, reduciendo así las posibilidades de conflictos de leyes o de jurisdicción."

Por lo tanto, y para terminar, nos encontramos con la existencia de tres normativas que inciden en la misma materia, y que por lo que ya hemos explicado, tienen una eficacia jurídica directa en nuestro ordenamiento jurídico; no obstante, la ley española, que es la que tiene la misión de recoger las exigencias y objetivos tanto del Convenio 108 como de la Directiva, es la que en su momento deberá tener el acierto o talento de sintetizar un conjunto de facultades, principios, objetivos varios, que no son del todo coincidentes, y dentro del breve plazo concedido.

A mi juicio, partiendo de la normativa más ejemplar y protectora del sistema de protección de datos, en lo que se refiere al tema objeto de estudio, que es el Convenio 108 (por cierto, el más antiguo en el tiempo, paradoja de la vida), lo que de "lege ferenda" debería hacerse es adaptar la normativa española a los objetivos de la Directiva, pero sólo en la medida de acoger aquellas mejoras evidentes en el mecanismo de protección, evitando la tentación de aceptar en nuestro propio ordenamiento unas facultades que por su especial naturaleza jurídica, podría conllevar un auténtico "callejón sin salida", en lo que a los datos a proteger se refiere, y todo ello en defensa de la intimidad y privacidad de los

afectados, que en suma, constituye el valor más prioritario a tener en cuenta en toda esta cuestión.

BIBLIOGRAFIA.

Heredero Higueras, Manuel y Alvarez Rico, Manuel: "Legislación Informática". Editorial Tecnos. Madrid 1993.

Martín-Casallo López, Juan José. "Implicaciones de la Directiva sobre protección de datos en la normativa española". Revista Actualidad Aranzadi, número 20, Madrid, Julio de 1996.

Murillo de la Cueva, Pablo Lucas. "Informática y Protección de Datos Personales (Estudio sobre la Ley Orgánica 5/1992 de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal). Número 43. Madrid 1993.

Sánchez Bravo, Alvaro A. "La regulación de los Datos Sensibles en la L.O.R.T.A.D". Revista Informática y Derecho. UNED. Centro Regional de Extremadura. Mérida.

Ull, Eugenio. "Informática y Derecho para Investigadores. Volumen II, Derecho Informático (Protección de datos personales)". UNED. Madrid.

Informática y Tecnologías de la Información: Breve síntesis de la evolución legislativa de la Unión Europea

BENJAMIN CORTES MARGALLO

Abogado

I. INTRODUCCIÓN.-

La informática, las telecomunicaciones y las tecnologías de la información se han constituído, en el ámbito legislativo comunitario, en componentes fundamentales de lo que se denomina en terminología comunitaria "Los Servicios de Interés General"[1], erigiéndose, por tanto, en una de las piezas más relevantes a la hora de considerar la progresiva construcción de una sociedad europea verdaderamente vertebrada.

En los próximos años, las tecnologías de la información no sólo se convertirán en un pilar de sostenimiento de nuestra sociedad y economía europeas, sino que las infraestructuras en este campo permitirán el tráfico libre y rápido de enormes cantidades de información por toda Europa y, desde el momento en que se produzca la aplicación cotidiana de los nuevos servicios a las necesidades y peticiones de los usuarios de cualquier nivel socioeconómico,

■ [1]Comunicación de la Comisión Europea, 22-Nov.-96, sobre servicios de interés general.

podremos hablar de una sociedad de la información europea efectivamente establecida y consolidada.[2]

La aplicación de las tecnologías de la información y las comunicaciones está repercutiendo en todos los sectores y servicios de nuestra sociedad. Es indudable que estas tecnologías tendrán una clara influencia en los diferentes componentes de nuestra Sociedad y Economía: el crecimiento, la competitividad y el empleo.

La aplicación de las tecnologías debe coadyuvar a la obtención de efectos y resultados tan considerables como son la cohesión social, una organización y estructuración más racional y eficaz, tanto en el sector público como en el privado y, en fin, un acentuado desarrollo de las regiones europeas.

Observamos, pues, que son muy variados los elementos sociales que reciben el poderoso influjo de las tecnologías, para terminar articulándose -ya se está apreciando paulatinamente- de diferente forma a la que tradicionalmente se venía haciendo.

Cambian los métodos de educación y formación, fundamentalmente en el campo de la cualificación de aquellos que mañana inexorablemente serán los verdaderos ejercientes en toda su extensión de la sociedad de la información. Ya incluso se están comenzando a explotar las posibilidades que estas tecnologías ofrecen para que el ciudadano europeo pueda beneficiarse de su propia riqueza y pluralidad lingüística y cultural.

Así el trabajo se transforma y con él, su prestación, las relaciones jurídicas laborales en incluso los eventuales litigios que surjan en caso de discrepancia pensemos en unos servicios prestados en Sevilla mediante teletrabajo a una empresa radicada en Hong-Kong- entre los sujetos intervinientes.

Sin embargo, en este aspecto laboral, no todos son parabienes hacia las nuevas tecnologías. Existe la idea -justificada por la propia realidad- de que la desmesurada aplicación a la industria y a los servicios nos abocará a cotas muy

■ [2] En este sentido se manifiestan las conclusiones de la Presidencia en el Consejo Europeo de Cannes de Junio de 1995(26 y 27)

elevadas del llamado "desempleo estructural", a cambio de unos escasos y altamente cualificados puestos de trabajo. En la actualidad más de la mitad de los desempleados de la Unión, es decir, el 6 % de la población activa, son parados de larga duración por causas estructurales. Según algunos historiadores y economistas nos encontramos en las puertas de sufrir unas transformaciones sociales, económicas y culturales que sólo tienen parangón en anteriores "revoluciones" del desarrollo humano, y por ello las transformaciones que se están produciendo -y que están por manifestarse- conllevarán beneficios....pero también algún cambio traumático.

Pero es conveniente abandonar este tono cuasi-apocalíptico y decir que son indudables las ventajas de la sociedad de la información, no exenta de riesgos, aunque imprescindible en su creación y puesta en funcionamiento siempre que queramos garantizar un crecimiento y empleo sostenibles y de esta forma, continuar el desarrollo de la ansiada Unión. Por tanto, nos debemos imponer un análisis crítico, desvinculado en la medida de lo posible de las arengas y los magnos deseos provenientes de Bruselas, y ponderar los efectos de la aplicación de las nuevas tecnologías sobre nuestra sociedad -que es la europea- y definir de esta forma las medidas complementarias y que atenúen los inevitables desajustes y consecuencias perniciosas, permitiendo así instalar un efectivo equilibrio entre las ventajas económicas, sociales y culturales y, al mismo tiempo, la existencia de inevitables riesgos.

Hablando desde el punto de vista puramente teórico, al comentar los diferentes aspectos de la sociedad de la información parece que nos olvidamos de las limitaciones que pueden surgir en su aprovechamiento no sólo en los Estados miembros económicamente más débiles, sino, dentro de los Estados "motores", sus capas sociales más desfavorecidas. Por esto, la sociedad de la información coloca a la Unión Europea ante un gran desafío que impida la aparición de la temida "sociedad de dos velocidades", con una evidente falla entre los que puedan y los que carezcan, en la que sólo un privilegiado sector de la población pueda acceder a las nuevas ventajas tecnológicas.

Siempre que las políticas que se adopten estén bien dirigidas y aplicadas, la sociedad de la información puede hacer una importante contribución al logro de objetivos sociales básicos: mejora de la calidad de vida de los ciudadanos europeos, elevación de los niveles de eficiencia de nuestra organización económica y social e incremento de la cohesión. Debemos afirmar, por ello que la economía europea no sólo depende del éxito de su industria en el contexto

mundial, sino también de la eficacia y la calidad de su organización social, y en este aspecto, las nuevas tecnologías gozan de un papel protagonista.

II. MEDIDAS Y MARCO REGULADOR GENERAL.-

La política comunitaria, con el fin de contribuir al desarrollo de los anteriormente citados servicios de interés general, como objetivo diferenciado, aunque complementario, del objetivo del Mercado Único, articula de manera progresiva las siguientes medidas:

a) **La promulgación de normas reguladoras claras y estables**. Medida fundamental que construye la vía por la que deben discurrir los sucesivos y seguros pasos hacia la plena sociedad de la tecnología y la comunicación. Son, las normas, un intrumento que garantiza el desarrollo y la operatividad ordenada de todas las redes y sistemas.

Desde 1974, concretamente el 15 de Julio de 1974, fecha de la primera Resolución elaborada por el Consejo, acerca de "Una política informática comunitaria", tanto el Consejo como la Comisión no han cesado de realizar un trabajo legislativo que, en algunos supuestos ha llegado a ser admirablemente prolijo y detallista.

Los instrumentos normativos utilizados tanto por el Consejo como por la Comisión han sido fundamentalmente tres: la Directiva, la Resolución y la Decisión. En menor medida, la Recomendación[3].

Aunque es del sector privado del que realmente se espera que haga la mayor parte de las inversiones necesarias para la implantación de la sociedad de la información, estas inversiones no se realizarán a menos que se cree de una manera ágil un marco regulador claro y estable que fije los principios generales y

■ [3] Curiosamente, su objeto predominante suelen ser las telecomunicaciones de carácter digital. Véanse Rec.del Cons. de 22 de Diciembre de 1986, relativa a la introducción de la Red Digital de Servicios Integrados en la U.E.; Rec. del Cons. de 25 de Junio de 1987, sobre comunicaciones móviles terrestres digitales; Rec. del Cons. de 9 de Octubre de 1990; Rec. del Cons. de 5 de Junio de 1992.

establezca un calendario definido. Esto ha sido destacado en el Consejo del 28 de Septiembre de 1994[4].

Toda esta legislación, de manera breve y concisa, será repasada en el análisis que practiquemos a lo largo de las siguientes líneas.

b) **Los planes directores europeos.** Con el fin de constituir una sólida red de servicios de información que verdaderamente suponen la espina dorsal de la sociedad de la información, contando siempre como factores ineludibles una política coordinada y una financiación para la realización de estas infraestructuras[5].

c) **Las inversiones de fondos comunitarios.** Siempre teniendo en cuenta el marco de la política de cohesión social y económica, especialmente dirigida a las infraestructuras de las regiones menos desarrolladas.

d) **Investigación y Desarrollo**. En aquellos sectores donde se han creado "servicios de interés general", como por ejemplo, y en lo que a nuestra materia respecta, el sector audiovisual y las tecnologías de la información.

■ [4] En este consejo se afirmó que "ante la evolución de las condiciones de mercado, el Consejo subraya la importancia y urgencia de crear un marco legal y reglamentario claro y estable que permita a los operadores del mercado emprender actividades empresariales, invertir y tomar iniciativas para hacer realidad la sociedad de la información".

■ [5] Véase el libro blanco de la Comisión "Hacia un espacio sin fronteras". COM. 96.P. 57.

III. LEGISLACIÓN COMUNITARIA: RELACIÓN DE MATERIAS DETERMINADAS.-

1- *Informática y Telemática.*

Como conveniente premisa de actuación es necesario advertir que el objeto de estas líneas no va a consistir en la práctica, tanto en la consideración de la normativa fundamental y general, como en la legislación más detallada que contemple cada concreta materia, de un análisis exhaustivo de lo publicado respecto del tema que nos ocupa en el Diario Oficial de la Unión.

Dicho lo anterior, abordamos los primeros pasos normativos de la entonces denominada Comunidad Económica Europea acerca de las tecnologías de la información, inicios que venían constituídos fundamentalmente por un bloque normativo compuesto por tres piezas:

- *Resolución del Consejo, de 15 de Julio de 1974*. Esta norma, al promover, considerando su contenido, la adopción de una coordinada y efectiva "política informática comunitaria", supuso un verdadero arranque y punto de partida, abriendo la perspectiva comunitaria hacía un campo desconocido para la inmensa mayoría de los ciudadanos europeos y por ende, para sus gobernantes. Esta norma, además, advierte de la creciente importancia que, a nivel mundial, tendrá el sector de la informática, en relación con el potencial industrial de los socios comunitarios.

Indudablemente, esta norma contiene una evidente intencionalidad por una parte del Consejo de no perder el tren del desarrollo económico, social y tecnológico en el contexto internacional. De esta forma, enlazando el encabezamiento y el término de esta Resolución podríamos comprimir su principal sentido: *" La Comisión de Comunidades Europeas, consciente de la importancia que reviste LA INFORMÁTICA para todos los aspectos de la sociedad moderna y para la Comunidad, y su posición económica y tecnológica en el mundo , invita a la Comisión a presentar al Consejo, antes del fin del año 75, un informe sobre la evolución del sector de la informática en la Comunidad en relación con la situación mundial ".*

En definitiva su carácter iniciático y de construcción de principios y directrices generales en la materia, le ha llevado a ser una norma ponderada y

tenida en cuenta la hora de legislar con posterioridad sobre la materia informática.[6]

- *Decisión del Consejo, de 27 de Septiembre de 1977*. El Consejo es consciente de que la promoción, por parte de la Comunidad Europea, del uso de instrumentos informáticos debe realizarse sobre una base sólida de conocimiento sobre cuáles son los objetivos y cómo ir estableciendo vías para acceder a los mismos. Para ello, mediante la Decisión de 1977, creando un marco específico de objetos de estudio en materia informática, comienza una concreción de los principios genéricos e intencionales contenidos en la Resolución del 74, sobre todo, con la introducción de un glosario de términos novedosos hasta ese momento: *bases de datos, técnicas de programación...*

De esta forma se realiza un tratamiento de la materia, no sólo desde una perspectiva económica, tal como afirma el considerando cuarto de la presente norma, sino también desde el punto de vista de la preocupación acerca de la seguridad y confidencialidad de los datos que son objeto de almacenamiento y procesamiento mediante *" Les ordinateurs "*.[7] Es el **artículo uno** de la Decisión el que establece unos objetivos claros y delimitados, respecto de materias que en años venideros y, con el desarrollo tecnológico, habrían de ser problemas relevantes y adyacentes al uso de los ordenadores. Nos estamos refiriendo a los sistemas de bases de datos, a la protección de los ciudadanos frente a las intromisiones ilegítimas en su intimidad realizadas mediante herramientas informáticas[8] y a la importancia económica de las técnicas de programación como

■ [6] A esta Resolución se han ido refiriendo sucinta y sucesivamente en sus encabezamientos, las normas que trataban la materia informática: "Declaración del Consejo de 27 de Septiembre de 1977", "Resolución de 11 de Septiembre de 1979".

■ [7] Como antecedentes debemos reseñar que el 14 de Noviembre de 1973 y el 20 de Noviembre de 1974, el Comité de Ministros del Consejo de Europa, recomendó a sus Estados miembros, el establecimiento de garantías de protección de los datos integrados en las bases de datos de carácter privado y público.

■ [8] Así el Considerando Tercero de la presente Decisión establece literalmente: " *Considerant que le developtment des applications de l'informatique exige un examen des próblems relatifs a la confidentialité et a la securité des donnes dans leurs aspects techniques, legislatifs et sociaux, notammente en uve de la protection des citoyens vis-a-vis de l'emploi de moyens informatiques...*"

elemento de desarrollo social y económico susceptible de protección y amparo, así como las relaciones e intereses entre los fabricantes y los usuarios.

Observamos, pues, el carácter adelantado de los siete considerandos y tres artículos de esta norma respecto de materias que en los años siguientes se convertirían, en cuanto a la informática, en las cuestiones más relevantes sobre las que la Unión Europea habría de legislar, apuntando así la dirección en la que habrían de encaminarse las propuestas y soluciones a los problemas planteados.[9]

- *Resolución del Consejo de 11 de Septiembre de 1979.*. La perspectiva de esta norma, que pretende el establecimiento de una acción comunitaria de promoción de la tecnología microelectrónica, es netamente economicista y de aprovechamiento industrial de las "Technologies nouvelles". Para ello proyecta como prioritarias la adopción de políticas de formación empresarial continua y asistencia técnica que hagan accesible las herramientas informáticas al mayor número de empresas omunitarias y, con ello, reforzar la tan reiterada competitividad y desarrollo del potencial económico de la "Comunidad", teniendo presente siempre el objetivo de obtener una aceptable producción europea de equipamientos de tecnología microlectrónica y la coordinación de las acciones en el sector de los Estados miembros.

- Con posterioridad a esta primeriza regulación comunitaria, debemos considerar la siguiente normativa que aparece en el Diario Oficial, fundamentalmente ya en la década de los noventa, apreciándose de esta manera a lo largo de los ochenta una significativa escasez normativa en la materia, debido, en gran parte, a una respuesta legislativa de los Estados miembros a los principios y propuestas expuestos desde la Comunidad desde 1974. No obstante y, a pesar de ello, nos encontramos en este periodo dos normas, de contenido análogo y denominación idéntica, pero utilizando revestimientos normativos diferentes. Estamos hablando de la *Decisión 87/95/CEE del Consejo de 27 de Diciembre de 1986 y la Resolución del Consejo de 27 de Abril de 1989*. Del contenido genérico de ambas normas comunitarias, se deriva un interés por obtener la promoción y, por ende,

■ [9] Debemos, así, recordar las Directivas sobre la protección jurídica de programas de ordenador (Directiva 250/91/CE del Consejo de 14 de Mayo de 1991) y la Directiva sobre la protección jurídica de bases de datos (Directiva 96/9/CE del Consejo y del Parlamento Europeo de 11 de Marzo de 1996).

la generalización del uso por particulares y empresas de los Estados miembros de los instrumentos, mecanismos y servicios que ofrecen las tecnologías de la información y las telecomunicaciones.

- Como un establecimiento de principios de actuación, no sólo en el ámbito de la informática sino también en el de las telecomunicaciones, nos encontramos en 1991 con una Resolución (*Resolución del Consejo 18-11-91*) por la que se establecen, en cuanto a la informática, las siguientes pautas normativas fundamentales:

1- La creación de un entorno empresarial favorable para el aumento de la competitividad en la industria tecnológica de la informática, teniendo en cuenta sobre todo a las pequeñas y medianas empresas, así como a los usuarios.

2- Medidas de I+D en el sector de la informática.[10]

3- Hacer hincapié en el esfuerzo de formación a todos los niveles.

- Por otra parte, y como normativa más específica que aborda los problemas derivados de la investigación en el campo de la telemática, considerando sus aplicaciones ordinarias pare el supracitado "interés general", se encuentra la *Decisión 94/801/CE del Consejo de 23 de Noviembre de 1993.*

- Hay que considerar que el Consejo reguló la aplicación práctica de los instrumentos telemáticos en un sector en plena reconversión como es el del transporte. De esta forma, *La Resolución del Consejo de 24 de Octubre de 1994*, acordó que, respecto al tráfico rodado, aéreo y ferroviario eran precisas determinadas acciones a adoptar por la Comisión y Estados miembros, entre las que cabe destacar:

1- Los sistemas telemáticos de información y alerta que sean interoperables para el control del tráfico rodado, así como promoción de la

■ 10 Considerando las acciones que en este sentido se realizan mediante los programas comunitarios de investigación y en especial el programa EUREKA. "Los Servicios de interés general en Europa" . Luxemburgo. Oficina de Publicaciones Oficiales de la Unión Euopea. p. 12.

instalación de equipamientos telemáticos a bordo de vehículos en el trasporte por carretera[11].

2- Unificación de uso entre los Estados de bases de datos coordinadas sobre mapas de carreteras digitalizados.

3- Progresiva instalación de sistemas electrónicos de intercambios de datos sobre el tráfico de buques que transporten mercancías peligrosas o perjudiciales para el medio ambiente.

4- Respecto del transporte ferroviario, el Consejo solicita a la Comisión y a los Estados miembros, que pongan en práctica programas de acción destinados a la creación efectiva de ejes transeuropeos ferroviarios basados en aplicaciones telemáticas. Un ejemplo, por lo que a la Península Ibérica afecta, podría ser el eje París-Barcelona-Madrid-Lisboa, cuya coordinación mediante instrumentos telemáticos aplicados a la alta velocidad reportaría indudables beneficios.

- Directamente relacionada con la materia de la aplicación de la telemática al transporte nos encontramos la *Resolución del Consejo de 17 de Junio de 1997*, relativa al cobro electrónico de cánones de forma telemática en los transportes por carretera, suponiendo, en esencia una aplicación informática que dota a la citada operación de agilidad y seguridad.

- Las transacciones comerciales efectuadas mediante equipos informáticos suponen un aspecto muy relevante necesitado de una respuesta por parte de la Comisión. Así, a través de la *Recomendación de la Comisión de 30 de Julio de 1997* se ofrecen directrices, en cuanto a las relaciones entre emisores y titulares de los instrumentos de pago.

■ [11] Recientemente (4 de Abril de 1997), la Comisión Europea ha adoptado "El programa para aumentar la seguridad del tráfico rodado en las vías comunitarias", en el que se contemplan la aplicación efectiva de sistemas telemáticos tanto a los vehículos como a las propias vías, siendo éste un primer paso para el desarrollo de las " autopistas inteligentes ".

Sobre esta materia igualmente se pronuncia la publicación oficial de la Unión Euopea "La Sociedad de la Información", p. 13: "A finales de 1996 deberán haberse instalado sistemas telemáticos de gestión del tráfico en diez grandes ciudades (treinta en el año 2.000) y 2.000 kilómetros de autopistas telemáticas".

Hay que concluir expresando que la labor normativa en los dos últimos años tanto de la Comisión como del Consejo, se ha concentrado predominantemente en el sector de las telecomunicaciones, más que en el de la informática, habiendo promulgado un gran volúmen de Decisiones, relativas a las redes de telecomunicaciones, conexión de equipos terminales, estaciones móviles y redes públicas de transmisión de datos, cuyo estudio y compilación pudiera ser objeto -por su densidad- de un trabajo independiente.

2- ***Derechos de Autor e Informática.***

Los programas de ordenador y las bases de datos, como creaciones humanas dignas de protección jurídica y que, además exigen relevantes esfuerzos económicos, tecnológicos y humanos, no habían sido tratadas unitaria y sistemáticamente por la legislación comunitaria hasta las Directivas de 91 y 96, en las que se fijan los criterios de coordinación de una normativa en la que los Estados miembros obviaban normativamente o bien regulaban aislada e incluso fragmentariamente tales fenómenos creativos.

- *Directiva 91/250 del Consejo de 14 de Mayo de 1991 sobre la protección jurídica de programas de ordenador.*

Primeramente, hay que observar que esta Directiva fue incorporada a nuestro ordenamiento jurídico a través de la Ley 16/93 de 23 de Diciembre, siendo el contenido normativo de esta disposición legal una verdadera trasposición a nuestro ámbito legislativo de los contenidos de la antedicha norma comunitaria.

Esta Directiva, en opinión de algún autor,[12] tiene como finalidad esencial la homogeneización de la protección jurídica en los Estados miembros de los programas de ordenador. De esta forma, se pretende establecer unas bases análogas de amparo legislativo nacional que, en definitiva, y de manera directa, favorezca el desarrollo del mercado común, considerando así a los programas

■ [12] En este sentido se manifiesta Gómez de la Escalera, J.J. cuando analiza en su ponencia "La Ley 16/93 de 23 de Diciembre sobre protección jurídica de los programas de ordenador". II Congreso Internacional de Informática y Derecho celebrado en Mérida. Págs. 923 y 924.

informáticos en particular y a la tecnología de la información en general, como un sector crucial dentro de la infraestructura industrial de la Unión Europea.

Sin embargo, al decir de Heredero Higueras en su artículo "Derechos inmateriales y Nuevas tecnologías de la información", la esencial finalidad de esta norma comunitaria no era tanto armonizar el derecho de autor sobre los programas, sino contribuir a crear la infraestructura de la libre circulación de los programas dentro de la Unión Europea, mediante unas excepciones a los derechos de los creadores, basadas en la interoperabilidad de los sistemas y los programas. (artículo 6 de la Directiva, al referirse a la "descompilación").

Los once preceptos que contiene esta Directiva realizan un recorrido por cada uno de los aspectos que atañen a las condiciones protectoras del programa de ordenador. Así, comienza por delimitar, de acuerdo con la consideración de obra literaria reflejada en el Convenio de Berna[13], el objeto de protección como creación intelectual propia de su autor en la que se incluye la documentación preparatoria, excluyendo las ideas y principios que fundamentan la creación.

La titularidad de los derechos, la referencia a los derechos exclusivos del titular (art. 2), teniendo también en consideración las excepciones a esta exclusividad (art. 3) y el plazo de protección de 50 años (art. 8) conforman, junto a la anteriormente aludida descompilación, el núcleo esencial de las directrices normativas contempladas en la presente directiva.

- Son reseñables, por su relevancia en cuanto a la relación derechos de autor e informática, la *Directiva del Consejo de 29 de Octubre de 1993*, relativa a la armonización del plazo de protección del Derecho de Autor, con incidencia en nuestra vigente Ley 1/96 de Propiedad Intelectual y la *Resolución del Consejo de 25 de Julio de 1996* sobre edición electrónica y bibliotecas.

- *Directiva 96/9 C.E del Parlamento y del Consejo sobre protección jurídica de las bases de datos*.

■ [13] Convenio de Berna de 9 de Septiembre de 1886 para la protección de obras literarias y artísticas, revisado en París el 24 de Julio de 1971, ratificado por España, por Instrumento de ratificación de 2 de Julio de 1973, publicado en el B.O.E nº 260 de 30 de Octubre de 1974.

El contenido dispositivo de esta norma comunitaria halla su fiel antecedente legislativo en la Propuesta de Directiva de 23 de Junio de 1992, propuesta que resultó modificada con fecha 15 de Octubre de 1993. Este proyecto normativo, en opinión de Álvaro Bermejo -a quien seguimos en esta materia- tenía dos objetivos fundamentales: **Eliminar** barreras jurídicas al establecimiento de un mercado único de las bases de datos, además de constituir un instrumento de remoción de los obstáculos que pudieran impedir la libertad de empresa y de prestación de servicios y **fomentar** la industria de la información y protegerla contra la piratería mediante una armonización de la protección jurídica otorgada por los distintos derechos nacionales.

La Directiva 96/9 establece -y así se deduce de su articulado- una diferenciación entre las bases de datos que contienen elementos originales (una "*creación intelectual de su autor*") y aquellas que no supongan tal esfuerzo creativo.

De esta forma, la presente norma contempla los siguientes rasgos generales definidores:

a) Fija una precisa delimitación respecto de la protección que ya se dispensa (Directiva 91/250) a los programas de ordenador en conexión con el acto creativo de la misma base de datos.

b) Establece, respecto del elemento subjetivo titular, y analógicamente con lo dispuesto en la Directiva 91/250, una determinación de las creaciones individuales, colectivas y mancomunadas. Sin embargo, obvia el tratamiento de las creaciones verificadas por el asalariado, en el ámbito creativo de las empresas.

c) La norma comunitaria, después de relacionar los derechos exclusivos que el autor está facultado para ejercitar (entre ellos, la reproducción, traducción-modificación, distribución y comunicación pública) consigna determinadas excepciones y límites a tales derechos, fundamentados en razones de utilidad científica, académica, de seguridad pública y procesales, siempre ponderándose el evitar -tal como preceptúa el Convenio de Berna- la causación al autor de perjuicios injustificados derivados de la aplicación de los anteriores límites.

d) La presente Directiva contempla el denominado "derecho sui generis" que asiste al fabricante de la base de datos y establecido con el fin de que éste pueda prohibir la "extracción o reutilización" de la totalidad o una parte considerable del contenido de la base de datos. La razón esencial de la existencia

de este derecho, no es otra -en opinión de Álvaro Bermejo- que proteger las importantes inversiones que requiere la realización de una base de datos, independientemente de que la base de datos goce o no de la protección de los derechos de autor.

3- ***Internet.***

Para finalizar este repaso a la normativa comunitaria en materia informática, sería conveniente aludir, siquiera brevemente, a la *Comunicación de la Comisión de 16 de Octubre de 1996 sobre contenidos ilícitos y nocivos de Internet.*

Esta comunicación -que tiene como antecedente la *Recomendación del Consejo de 7 de Abril de 1995*, relativa a los *criterios comunes de seguridad* en las tecnologías de la información- considera a Internet y a su más conocida aplicación, World Wide Web, como una de *las principales piezas de infraestructura mundial de la información y un estímulo fundamental de la sociedad de la información en Europa*, advierte del riesgo que supone la transmisión a través de la "web" de ciertos contenidos potencialmente nocivos, ilícitos o la utilización de la red como vehículo de actividades delictivas. Estos riesgos, es indudable, que pueden afectar a diversos bienes que deben ser objeto de protección: la seguridad económica, de la información y de los Estados, los menores la dignidad humana, la intimidad y la propiedad intelectual.

La Comisión, para evitar los perjuicios que pudieran provocarse por la inclusión en la "red de redes" de contenidos ilícitos y nocivos considera que es necesario adoptar un primer conjunto de medidas para una acción inmediata. Respecto de los **contenidos ilícitos,** la Comisión fija las actuaciones a realizar en tres claros frentes: *la cooperación entre los Estados miembros* en el ámbito de Justicia e Interior para intecambiar información sobre los suministradores de contenidos delictivos y homogeneizar los criterios europeos sobre los contenidos delictivos, *la responsabilidad de los suministradores de acceso y los suministradores de servicios de ordenador central* y, como tercera medida, *el fomento de la autorregulación* de los citados suministradores.

Y, en cuanto a los **contenidos nocivos**, la Comisión interesa el fomento de la utilización de programas informáticos de filtrado[14], la adopción de un código de conducta por parte de los productores de contenidos que se publican en internet, realizándose por su parte un ejercicio de autovaloración sistemática y la actividad de sensibilización en la materia, dirigida a padres y profesores.

Finalmente, la Comunicación de la Comisión propone la celebración en un futuro inmediato de una Conferencia Internacional, en la que Alemania sería anfitriona, con el fin de establecer un amplio y claro marco de cooperación internacional que pudiera concretarse y consolidarse en un Convenio Internacional sobre contenidos ilícitos y nocivos de internet.

Más recientemente, el Consejo y los representantes del los Gobiernos de los Estados miembros, reunidos en el seno del *Consejo de 17 de Febrero de 1997*, mediante la Resolución de la misma fecha, han concretado las actuaciones de seguridad y protección en Internet, haciendo especial hincapié en la cooperación interestatal y el establecimiento de un autocódigo de conducta por parte de los servidores, donde el interés de los menores fuera el elemento preponderante. Todo ello se ha visto reflejado documentalmente en las *Conclusiones del Consejo relativas al Libro Verde sobre la protección de menores y de la dignidad humana en los nuevos servicios audiovisuales y de información.*

■ [14] Existen tres modelos de programas de filtrado:

La lista negra, se aplica mediante el programa-conjunto de filtrado Cyber Patrol que posee la lista "CyberNOT", abarcando unos 7.000 servicios agrupados en doce grupos (violencia,desnudos, racismo, cultos satánicos, drogas, lenguaje malsonante, militancia-extremismo etc..). Los padres pueden bloquear de manera selectiva el acceso a cualquiera o a todos los grupos examinando cada casilla en el gestor de programas.

La lista blanca. Funciona a la inversa. Bloquea todos los contenidos de internet salvo los emplazamientos autorizados expresamente en una "lista blanca". Es una técnica excesiva y muy restrictiva pero ha dado buenos resultados en determinados ámbitos, por ejemplo, en la escuela.

■ **El etiquetado neutro.** Es de reciente creación (agosto del 95). Es conocido generalmente como PICS (Platform for Internet Content Selection, Plataforma de selección de contenidos de Internet) y su utilidad fundamental consiste en separar las dos funciones de valorar y filtrar los emplazamientos y permite un alto grado de flexibilidad y seguridad. En opinión de los expertos, -posición que asume la Comunicación- es la solución más completa e innovadora para tratar los problemas de contenido de Internet.

* "Reglamentos y Directivas en la jurisprudencia comunitaria". José Eugenio Soriano. Editorial Tecnos.

* "La Sociedad de la Información". Publicación oficial de la Comisión de la Unión Europea. Servicios de publicaciones. Luxemburgo.

* "Los Servicios de interés general en Europa". Oficina de publicaciones oficiales de la Unión Europea. Servicio de publicaciones. Luxemburgo.

* "Actas del II Congreso Internacional de Informática y Derecho". Universidad Nacional de Educación a Distancia. Centro Regional de Extremadura. Mérida.

Protección de los Datos informatizados de Carácter Médico

JOSE MANUEL NUÑEZ JIMENEZ

Doctorando Curso "Valor Probatorio de los Documentos Electrónicos" dirigido por el Profesor Carrascosa López. UNED.

I. INTRODUCCIÓN

El empleo del ordenador hace posible recopilar una amplia información sobre cada persona, reuniendo un conjunto de datos que aisladamente nada dicen, pero que al ser presentados en forma sistematizada, puedan dar lugar a una información que el afectado no se imagina ni le agradaría ver en poder de otros. Tengamos presente que un ordenador puede clasificar y relacionar rápidamente, por ejemplo, nuestros datos laborales, económicos, legales, sanitarios, etc, construyendo un detallado perfil de cada individuo.

Precisamente por ello, peligra la intimidad de la persona cuando se relacionan entre sí archivos nominativos, pues la tecnología informática permite ahora, gracias a sus posibilidades casi ilimitadas de captar, almacenar, relacionar y transmitir los datos, reunir de forma personalizada, a partir de informaciones dispersas e incluso anónimas, múltiples facetas de la vida de hombres y mujeres, que pueden ser utilizadas por terceros y depararles perjuicios importantes.

Se convierte en transcendental, por tanto, cualquier dato, por insignificante que éste sea, ya que relacionados con otros puede poner en peligro la intimidad como claramente pone de manifiesto el **Tribunal Constitucional Federal Alemán.**[1]

Teniendo en cuente la importancia de la intimidad y la privacidad como Derechos Fundamentales, la **Constitución Española**, en su art. 18 plasma la garantía al derecho al honor, a la intimidad personal y familiar y a la propia imagen, y al mismo tiempo, emplazó al legislador a limitar el uso de la informática para garantizar el ejercicio legítimo de estos derechos.

Dando cumplimiento al mandato del art. 18 de la Constitución se dictó la Ley Orgánica 5/92, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal, de 29 de Octubre **(LORTAD).**

Esta ley, efectivamente, nació como protección y control a la informática, que era capaz de tratar datos personales con nuevas técnicas que hacían peligrar Derechos Fundamentales de las personas. Por lo tanto, es la respuesta dada por el legislador para proteger a los ciudadanos frente a intromisiones ilegítimas en la privacidad[2], a través de nuevas tecnologías.

Se trata, pues, de proteger al ciudadano de cualquier injerencia en la esfera de su privacidad mediante las técnicas informáticas, de impedir que nuestros datos personales puedan ser recabados, almacenados, utilizados, cedidos,

■ [1] **TRIBUNAL CONSTITUCIONAL FEDERAL ALEMÁN**: Sentencia de 15 de Diciembre de 1983 (rf. 1 BvR 209/83) Ley del Censo. Derecho a la personalidad y dignidad humana... "*de este modo un dato carente en sí mismo de interés puede cobrar un nuevo valor de referencia y, en esta medida, ya no existe, bajo la elaboración automatizada de datos, ninguno sin interés*".

■ [2] **MARZAL HERCE, GLORIA**; "Bases de datos Personales: requisitos para su uso. Comentarios a la LORTAD y normativa complementaria". DEUSTO Bilbao 1996;

"*...en la Exposición de Motivos de la LORTAD se habla de privacidad y no de intimidad: aquélla es más amplia que ésta, pues en tanto la intimidad protege la esfera en que se desarrollan las facetas más singulares reservadas a la vida de la persona -el domicilio donde realiza su vida cotidiana, las comunicaciones en las que expresa sus sentimientos-, la privacidad constituye un conjunto más amplio, más global de facetas de su personalidad que, aisladamente consideradas, pueden carecer de significación intrínseca pero que, coherentemente enlazadas entre sí, arrojan un retrato de la personalidad del individuo que éste tiene derecho a mantener en secreto*".

alquilados o vendidos sin nuestro consentimiento (y/o consentimiento) con total impunidad.

Se pretende imponer unos límites y unas obligaciones a todo aquel que pretenda almacenar datos personales y, sobre todo, pretende controlar quién posee un fichero, cómo se han obtenido los datos personales, para qué se prevé utilizarlos, etc.

Sólo controlando, las personas afectadas, los datos referentes a su personalidad, es como se respetarán sus derechos. La Ley, en aras a una mayor protección, crea un organismo oficial, la Agencia de Protección de Datos, al que nos podemos dirigir tanto para formular reclamaciones como para buscar protección e información.

En definitiva la LORTAD intenta crear un equilibrio entre la privacidad de cada uno y los avances de la técnica. Su verdadera finalidad es proteger a las personas en relación con el tratamiento informatizado de datos. De ahí que no sea el honor o la intimidad lo que se proteja sino el correcto uso y tratamiento de aquellos.

Por lo que motiva todo el problema, es decir, los datos acerca de una determinada persona, éstos deben ser adecuados, pertinentes y no excesivos en relación con el ámbito y finalidades para las cuales se hayan obtenido. Los datos serán cancelados cuando hayan dejado de ser necesarios para la finalidad para la cual hubieran sido recabados y registrados.

Su tratamiento automatizado requerirá el **consentimiento del afectado**, salvo que una ley disponga lo contrario. Los datos deberán ser exactos y puestos al día de forma que respondan con veracidad a la situación real del afectado. Corresponde al titular del fichero asegurar la exactitud de los mismos. Deberán, también, estar archivados de manera que impidan la identificación del interesado durante un período superior al necesario para los fines para los que fueron recabados.

Cualquier persona que proceda a recoger datos de carácter personal tiene la obligación impuesta por la Ley de informar al afectado.

Dentro de todo el posible catálogo de datos personales, existen unos considerados por la Ley como especialmente protegidos, que gozan de un

régimen jurídico distinto al de los demás. Son los denominados "***datos sensibles***".

La LORTAD distingue entre estos grupos de datos sensibles :

a) los que se refieren a la **ideología, religión o creencias**: para protegerlos se exige que el consentimiento del afectado se exprese por escrito y de manera explícita.

b) los referidos a **infracciones penales o administrativas,** que sólo podrán figurar en los ficheros de las Administraciones Públicas.

c) los referidos al **origen racial, salud o vida sexual,** para lo que se exige el consentimiento del afectado pero no por escrito.

Será la protección de la intimidad de las personas, en lo referente a sus datos de salud, el tema central de mi estudio.

II . REGULACIÓN LEGAL DE LOS DATOS MÉDICOS

Hay que partir de la consideración de que estos datos sólo podrán ser recabados, tratados automatizadamente y cedidos, cuando por razones de interés general lo disponga una ley o el afectado consienta expresamente.

El **art. 8 de la LORTAD** contempla los tratamientos automatizados de datos efectuados en el seno de "*las instituciones y los centros sanitarios públicos y privados y las profesiones correspondientes*". El precepto lo que hace es modular, en el contexto de las normas de salud, la norma del art. 7.3 de la Ley y en tal sentido, constituye una norma habilitante de rango legal para la recogida y el tratamiento de datos de salud.

Esta habilitación se acota de acuerdo con estos requisitos :

- limita dicha recogida y tratamiento a las instituciones de la Administración sanitaria, a los centros sanitarios privados y a los "*profesionales correspondientes*".

• la recogida y el tratamiento han de ajustarse a las leyes que el precepto enumera : **la Ley 14/1986, General de Sanidad, la Ley 25/1990, del Medicamento**, y la **Ley Orgánica 3/1986, de Medidas Especiales en Materia de Salud Pública.**

• la cesión de datos debe ajustarse a lo previsto por la LORTAD en su art. 11.2.f.[3]

El art. 8 acota el colectivo de los "***responsables de los ficheros***" de datos de salud. Los órganos de las Administraciones públicas que no ejerzan funciones asistenciales o de investigación epidemiológica no están incluidos en esa habilitación.

La **Orden de 21 de Julio de 1994**, del Ministerio de Sanidad y Consumo, reguló los ficheros gestionados por el Departamento y los clasificó en ficheros de carácter sanitario y de carácter administrativo. De esta forma se dejó zanjado que el tratamiento de los datos de salud está reservado a profesionales cualificados. Las demás personas o entidades que pretendan procesar datos de salud deberán solicitar el consentimiento expreso de los pacientes afectados.

El art. 8 de la Ley General de Sanidad dispone que los estudios epidemiológicos han de basarse en un sistema organizado de información sanitaria, vigilancia y acción epidemiológica.

El art. 23 de la misma Ley habilita a las Administraciones sanitarias a que creen registros y elaboren análisis de información que fueren necesarios para conocer las situaciones de las que pudieran derivarse medidas de intervención de la Autoridad sanitaria. Su art. 61 instaura la historia clínica integrada en las áreas de salud.

La Ley del Medicamento en su art. 85.5 prevé el tratamiento informático de los datos sanitarios.

■ [3] "*El consentimiento... no será necesario... cuando la cesión de datos de carácter personal relativos a la salud sea necesaria para solucionar una urgencia que requiera acceder a un fichero automatizado o para realizar los estudios epidemiológicos en los términos establecidos en el art. 8 de la Ley 14/1986, de 25 de Abril, General de Sanidad*".

Por último, respecto a la última Ley que menciona el art. 8 de la LORTAD, la **Ley de Medidas Especiales de Salud Pública, Ley Orgánica 3/1986,** prevé unas medidas de excepción para situaciones de urgencia :

- existencia de un **peligro para la salud** causado por la *"situación sanitaria concreta de una persona o grupo de personas o por las condiciones sanitarias en que se desarrolla una actividad"* : las autoridades sanitarias pueden realizar todo tipo de medidas sin requerir el consentimiento de los afectados.
- situación de **epidemia**: no se requiere el consentimiento.
- **escasez de medicamentos**

En estos supuestos, sólo se tendrá incidencia en el uso y tratamiento de los datos de salud, si las medidas a adoptar requieren crear unos ficheros y procesar datos de las personas objeto de las medidas especiales. Debe existir una disposición legal dictada por razones de interés legal que las regule.

La primera disposición específica relativa al tratamiento automatizado de los datos de salud es la **Instrucción 2/1995, de 4 de Mayo, de la Agencia de Protección de Datos,** referente a la recogida y usos de datos de salud como consecuencia de la contratación de un seguro de vida en forma conjunta con la concesión de un préstamo hipotecario o personal. Contempla la recogida de los datos del solicitante del préstamo, así como el consentimiento del afectado y la cesión de los datos.

El uso de los datos de salud ha trascendido el ámbito de las historias clínicas o expedientes médicos e incluso el marco de la estricta relación médico-paciente.

El uso de estos datos excede el campo de los sistemas de información automatizados: su uso ya no se ciñe al empleo del ordenador, sino que ha pasado a otros sistema y soportes, como las tarjetas de memoria, y comprende procesos no tradicionales, como loa análisis de ADN, los análisis genéticos, los estudios de genoma humano, etc. Por ello, el **Consejo de Europa** elaboró un borrador de Recomendación sobre el uso de estos datos, excepciones del consentimiento, acceso a ellos, etc. Culminó en la Recomendación R.94 de 19 de Marzo de 1994 sobre bancos de Tejidos Humanos, elaborado por el Comité de Ministros de los Estados Miembros del Consejo de Europa.

III. LA PROTECCIÓN DE LOS DATOS MÉDICOS AUTOMATIZADOS

III.1. Consideraciones previas

En el pasado, la relación médico-paciente tuvo un carácter cuasi sacro y por ello, el secreto de este tipo de información estaba prácticamente asegurado. Los datos sanitarios pertenecen al círculo más íntimo de la persona. Hace años estas informaciones rara vez salían de los centros médicos. Actualmente, debido a los avances informáticos, se ha atacado gravemente la confidencialidad de estos datos.

Así, se convive en una situación donde los profesionales sanitarios necesitan la creación de grandes bases de datos que faciliten su labor y, debido a su fácil almacenamiento, el personal no médico también tiene la posibilidad de poder acceder a ellas.

De forma generalizada, los datos de carácter médico se localizan en los siguientes lugares :

- **consultas médicas**
- **instalaciones hospitalarias**
- **compañías de seguros**
- **departamentos de personal: es el más peligroso**.

Estos datos en forma alguna deben tener acceso a ellos personal no sanitario. Existen casos en los que, incluso manteniendo la base de datos totalmente protegida, no se toman las debidas medidas de seguridad, permitiendo, por ejemplo, que a efectos contables, el pagar una determinada cantidad en concepto de medicinas, proporcione una información sanitaria, inequívoca, de esa persona.

Este tipo de datos no debían figurar en una base de personal que suele ser muy accesible a gran número de empleados de la empresa.

La LORTAD señala que "*el responsable del fichero deberá adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos y eviten su*

alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural'.[4]

III.2. El secreto profesional del médico

El secreto médico se presenta como una de las modalidades del secreto profesional, calificado por la naturaleza de la actividad. No se trata de un derecho fundamental, sino de una medida consecuente con la prohibición de interferir de forma ilegítima en la esfera íntima del paciente. Los Derechos Fundamentales realmente protegidos mediante el secreto médico, son los derechos al honor, a la intimidad personal y familiar y a la propia imagen, conceptos cuyo contenido esencial está constituido por valores inmateriales, pertenecientes al fuero de la conciencia individual, fundados en el sentimiento subjetivo de que quien los padece, al ver desvelada su intimidad o puesta en entredicho su reputación y buen nombre, decae en la consideración ajena.

El secreto médico se establece sobre la base de la existencia de la relación médico paciente, dando origen a un contrato tácito entre ambos. Aquél, incluirá la naturaleza de la enfermedad y las circunstancias que concurran en la misma

El campo donde queda peor parado este *"pacto"*, es en el de las relaciones de la **Medicina de Empresa** con la ***Medicina* de la Seguridad Social**; aquí la obligación de sigilo queda mal parada. Chocan la obligación moral con el paciente de reservar todos los datos de su enfermedad y el compromiso con la empresa o con el gestor de la Seguridad Social de tenerles informados de la morbilidad y pronóstico de las afecciones de sus trabajadores. La solución ideal sería llegar a un compromiso ecléctico que salvaguardara los intereses del enfermo y de la empresa. En el terreno de lo pragmático, el médico tratará de defender todo lo posible el secreto de sus pacientes, aunque sometido a las obligaciones reglamentarias que su adscripción a este tipo de medicina le impone.

Por lo que se refiere a la **historia clínica**, se trata de un documento asistencial resultante de la relación médico paciente, en el que se reflejan todos los datos de la anamnesis, exploración, tratamiento, curso evolutivo y catamnesis

■ [4] **LORTAD**, artículo 9.

final, así como, en su caso, de la necropsia de los enfermos asistidos, tanto en la medicina privada, como en la pública y hospitalaria.

El médico sólo es el depositario de la historia clínica y guardián de su contenido, debiendo quedar protegido por el secreto médico; está obligado a conservarla con prudencia y a poner el máximo cuidado en protegerla contra toda indiscreción que lleve a hacer público su contenido, como señala el **art.15.3[5] del Código de Ética y Deontología Médica**.

Solamente puede hacerse uso de los datos contenidos en los archivos, en el curso de investigaciones científicas, siempre conservando el anonimato de los pacientes a los que corresponden las historias clínicas. Así, el Real Decreto de 1 de Marzo de 1996 que establece los protocolos obligatorios, de estudios de los donantes y usuarios relacionados con las técnicas de reproducción asistida, y regula la creación y organización del Registro Nacional de gametos y preembriones con fines de reproducción humana, señala en su art. 9 que la información recogida en la historia clínica de usuarios de las técnicas de reproducción asistida será recogida, tratada y custodiada en la más estricta confidencialidad conforme a lo dispuesto en la LORTAD.

Con el uso de la informática es relativamente sencillo desvelar esta información. El médico nunca debe participar en la creación y mantenimiento de los sistemas informáticos, sin la garantía de que se respetará el derecho del paciente a la intimidad. Debe excluirse radicalmente que un banco de datos médicos quede conectado a una red informática no médica.

La obligación del secreto se mantiene incluso después de la muerte del enfermo, por lo cual, cuando el médico cesa en su actividad profesional, debe proveer a la destrucción de su archivo si de él no se hace cargo su sucesor, o los pacientes hacen constar su oposición, en cuyo caso se les hará entrega de sus respectivas historias clínicas.

■ [5] "*Las historias clínicas se redactan y conservan para facilitar la asistencia del paciente. Se prohibe cualquier otra finalidad, a no ser que se cumplan las reglas del secreto médico y se cuente con la autorización del médico y del paciente*".

En cuanto a los **archivos hospitalarios**, cuando su volumen desborda la posibilidad de almacenamiento y manejo, se tiende a trasladarlos a microfilm o a soporte informático, siempre respetando las normas deontológicas y legales sobre el secreto.

III.3. Especial referencia a la protección de los datos genéticos

III.3.1. Cuestiones polémicas

Los avances científicos cursan, generalmente, por delante del derecho, que se retrasa en su acomodación a las consecuencias de aquéllos. Esta falta de sincronía entre la ciencia y el derecho origina un vacío jurídico respecto de problemas concretos que provocan indefensión al paciente. Ejemplo de estos vacíos legales lo constituye la materia de reproducción asistida teniendo que ajustar el derecho a estas prácticas.

La información sobre el genoma de un individuo representa la más íntima expresión de cuantos factores endógenos intervienen en la conformación de su estado de salud, no sólo actual, sino, también, futuro. Su estudio permite descubrir características propias de la personalidad.

Así, resulta verosímil que el programa genético de una persona encierre datos sobre sus aptitudes intelectuales y manuales, su temperamento y hasta sus inclinaciones sexuales. Sin embargo descifrar estos factores, es algo que la ciencia, hoy día, todavía no está en condiciones de realizar.

En el campo de la genética, y por lo que se refiere a la protección de la intimidad, se dan varias situaciones de conflicto :

- por un lado, la persona a quien esos datos se refieren, ostenta un interés en su protección
- por otro lado, determinadas personas físicas o jurídicas pueden demostrar un interés legítimo pero contradictorio al del titular de los datos.

Estas situaciones conflictivas se pueden agrupar en tres grupos, según se trate:

- de **relaciones en el seno de una familia**

- de **relaciones contractuales**, basadas principalmente en el interés económico.
- de **relaciones con la sociedad**, donde el derecho al respeto de la vida privada puede entrar en conflicto con un interés colectivo.

En este último apartado del trabajo, analizaré las relaciones entre el sujeto titular de los datos y su entorno familiar

III.3.2. El sujeto y el entorno familiar

La genética tiene por objeto detectar la presencia del factor o factores determinantes de enfermedades que, siendo asintomáticas en el momento de realizar el análisis, pueden, eventualmente o con certeza, declararse después. El conocimiento de la presencia del factor genético permitirá así el tomar las medidas conducentes a prevenir la enfermedad, a retrasar su aparición o a limitar sus efectos.

Este conocimiento puede ser de gran ayuda tanto para el sujeto como para los miembros de su familia consanguínea o afín, que así instruidos podrán poner en práctica las adecuadas medidas preventivas o tomar otro tipo de decisiones que afecten a su vida privada.

La primera situación que puede ocurrir es que el propio sujeto tome conciencia de sus datos genéticos. Es el, comúnmente, denominado **derecho a saber**, que en el campo específico del tratamiento automatizado de datos se traduce en el llamado derecho de acceso.

El derecho a saber puede ejercerse, bien directamente, bien a través de otra persona, con la particularidad de que la comunicación al interesado de los resultados del análisis genético se aconseja que vaya acompañada por el asesoramiento genético.

Formando, en muchas ocasiones, parte de este derecho se encuentran los denominados en el *argot* médico **descubrimientos inesperados**. No es raro en medicina, cuando se realiza una intervención o un análisis, descubrir, además de los datos objeto del análisis, otro tipo de datos personales. En estos casos, el sujeto debe ser informado de dichos descubrimientos inesperados en cuanto los mismos tengan carácter médico.

En otro orden de cosas, no toda enfermedad genética dispone hoy en día de terapia, ni siquiera de protección. De muchas de esas enfermedades, lo único que se puede predecir es que se producirán, sin poder ni prevenirlas ni retrasarlas, lo que, con su conocimiento, puede representar para su titular fuente de desasosiego que le impida vivir con la tranquilidad que permitiría la ignorancia. Es lo que se conoce con el nombre de **derecho a no saber**. Tanto la doctrina como el derecho concuerdan en que la decisión de informarse o no corresponde al propio sujeto.

En el entorno familiar todos estos problemas se agudizan. Las características genéticas son transmisibles de una generación a otra, de modo que si una persona es portadora del gen responsable de una enfermedad es casi seguro que dicho gen se hallará presente en otros miembros de su **familia consanguínea**. Desde el ángulo médico, el paciente no es ya un individuo sino la familia entera.

En la inmensa mayoría de los casos, la comunicación de la información se suele realizar sin mayor dificultad: el propio sujeto se encarga de informar a su familia, si bien, está interesado en que, respecto a los demás, se siga protegiendo su intimidad.

Sin embargo, en algunos supuestos, se producen problemas si el sujeto rehusa a comunicarlo. El motivo de esa decisión puede ser muy diverso: mal entendimiento entre la familia o deseo de no preocuparla. En ambos casos, la responsabilidad directa de la comunicación de los datos genéticos incumbe al sujeto, de la misma manera que se reconoce el correspondiente derecho de los parientes a ser informados.

Por lo que respecta a la situación en la que queda el médico, éste se encuentra sometido al secreto profesional, si bien han de valorarse las consecuencias de la decisión a adoptar, teniendo en cuenta la gravedad de la enfermedad de que se trate. Antes de decidir si debe comunicar o no una información personal al resto de la familia contra el parecer del interesado, el médico no sólo deberá ponderar los intereses privados en juego sino que habrá de tener en cuenta también la desconfianza en la profesión médica que su acto puede fomentar. Sin embargo, y a pesar de lo anterior, cuando exista una amenaza seria a la salud de alguna persona, será motivo suficiente para exponérselo.

Los mismos planteamientos pueden darse en el caso de la familia afín. En este caso el incumplimiento de esa regla moral de comunicación, puede corresponder una obligación jurídica.

IV. CONCLUSIONES

El uso de todo tipo de avances informáticos, faculta al titular de un fichero nominativo a recopilar una gran serie de datos sobre una persona, labor que ésta desconoce y a la que, se opondría visceralmente de conocer su existencia.

El ámbito sanitario es uno de los sectores donde es más fácil poder atacar la intimidad de una persona, ya que cualquier miembro del personal administrativo puede acceder a las bases de datos donde figuran las historias clínicas de los pacientes, vulnerando gravemente la Ética profesional que debe caracterizar la labor del médico.

Los datos de carácter sanitario deben corresponder exclusivamente al médico o equipo facultativo que requiera de su conocimiento.

Los trabajos de futuro, en aras de una auténtica y efectiva protección, deben ir encaminados a posibilitar el blindaje de estas bases, de manera que, nadie pueda producir, mediante su revelación, el grave perjuicio de atacar irreparablemente Derechos Fundamentales de la persona. Así, el hecho de desvelar que una determinada persona padece una enfermedad infecto contagiosa, acarrea a ésta, no sólo un desprestigio y rechazo social (pensemos en el SIDA), sino una pérdida de autoestima que en muchos casos, es más grave y definitiva que la propia enfermedad. Una posible solución, consistiría en aplicar las técnicas criptográficas a las bases de datos.

Sin embargo el paso más importante que debe darse es a nivel legislativo. Actualmente, es público y notorio, que gran número de empresas poseen bases de datos de su personal, de carácter médico. La ley debería arbitrar una serie de medidas concretas que aumenten la seguridad en el control de estos sistemas. Hasta ahora, la LORTAD no ha hecho más que una declaración de los principios generales en esta materia, poniendo de relieve los derechos de que goza la persona afectada, sin resolver los ataques gravísimos a la intimidad.

Sin embargo, debe exigirse a la Agencia de Protección de Datos que controle minuciosamente las bases de almacenamiento, evitando los trasvases de información no autorizados, mediante medidas de choque que acaben con la impunidad de los titulares de los ficheros. Solamente aplicando las sanciones millonarias que la propia Ley establece y creando medidas preventivas (técnicas criptológicas), se evitarían estas situaciones conflictivas.

BIBLIOGRAFÍA

- ACHA ITURMENDI, J.J. (1996) "*Situación actual de la informática y los datos personales. Algunas reflexiones sobre la aplicación real de la LORTAD*". Informática y Derecho nº 12, 13, 14, 15 UNED Mérida.

- CÓDIGO DE ÉTICA Y DEONTOLOGÍA MÉDICA

- DE SOLA, Carlos (1994) " Privacidad *y datos genéticos. Situaciones de conflicto. I*" Revista de Derecho y Genoma humano nº1. Julio-Diciembre

- DEL PESO NAVARRO, Emilio (1996) "*La protección y la seguridad de los datos automatizados de carácter médico*" Informática y Derecho nº12, 13, 14, 15 UNED Mérida.

- DEL PESO NAVARRO, Emilio (1994) "*La figura del responsable del fichero de datos de carácter personal en la LORTAD*" Informática y Derecho nº6,7 UNED Mérida.

- GISBERT CALABUIG, J.A. (1991) "*Medicina legal y toxicología*" Editorial Salvat. Barcelona pp. 77-83.

- HEREDERO HIGUERAS, M. (1996) "*La Ley Orgánica 5/92 de Regulación del Tratamiento de los Datos de Carácter personal. Comentario y textos*" TECNOS Madrid pp. 95-116.

- *INFORME DEL GRUPO DE TRABAJO SOBRE INFORMACIÓN GENÉTICA Y SEGUROS DE SALUD.* Revista de Derecho y Genoma humano nº1, Julio-Diciembre 1994.

• MARZAL HERCE, Gloria (1996) "*Bases de datos personales. Comentarios ala LORTAD y normativa complementaria. Requisitos para su uso*".DEUSTO Bilbao pp. 29-50.

• OROZCO PARDO, Guillermo (1994) "*Los derechos de las personas en la LORTAD*" Informática y Derecho nº 6, 7 UNED Mérida.

• RAMOS GONZÁLEZ, M.A. (1994) "*La seguridad y la confidencialidad de la información y la LORTAD*" Informática y Derecho nº 6, 7 UNED Mérida.

• ROMEO CASABONA, C.M. (1994) "*Aspectos jurídicos del consejo genético*". Revista de Derecho y Genoma humano nº 1 Julio-Diciembre pp. 153-157.

• SÁNCHEZ BRAVO,A.(1994) "*La regulación de los datos sensibles en la LORTAD*" Informática y Derecho nº 6, 7 UNED Mérida.

• YANES, Pedro (1994) "*Seguros de personas e información genética. I*" . Revista de Derecho y Genoma humano nº1, Julio-diciembre.

El Valor Probatorio de los Documentos Informáticos en el Registro Civil

ANTONIO SALVADOR FRIAS DEL VAL

Cuerpo Superior de Administradores Civiles del Estado

I) INTRODUCCIÓN Y METODOLOGÍA.

1°) Introducción.

La implantación de las nuevas tecnologías de la información y, en concreto, de la informática a la práctica totalidad de los aspectos de las sociedades modernas, tanto en su vertiente individual como colectiva, supone uno de los mayores cambios en los hábitos de comportamiento habidos en los últimos tiempos. Con tales tecnologías se han visto modificados no sólamente los métodos de trabajo y producción, sino las comunicaciones personales y sociales, eliminándose las barreras de tiempo y espacio habidas hasta tiempos recientes y facilitándose el acceso a un considerable potencial de información a todos los usuarios de dichos medios informáticos, incluso desde el propio domicilio personal.

Dicho proceso de cambio social acelerado comporta un cambio en la legislación de los distintos países, con el fin de poder dar respuesta al cúmulo de nuevos problemas jurídicos para los que las normas hoy vigentes sólo pueden dar respuesta de forma parcial e incompleta, dado que la realidad social a

la que tales normas responden no recogía la problemática que los nuevos medios tecnológicos están desvelando a medida que éstos se extienden en todos los ámbitos de la sociedad.

Pero este cambio en la legislación, lógicamente debería ir precedido, o al menos paralelo, a un cambio en la mentalidad jurídica de los especialistas, que en no pocas ocasiones responde a moldes acuñados en una realidad social distinta a la que ya se plantea en el momento presente y a la que en un futuro próximo parece que nos dirigimos.

El panorama descrito, si bien puede ser aplicado a numerosas ramas y aspectos del Derecho, presenta una especial significación en el ámbito del Registro Civil en nuestro país, ya que en el mismo están recogidos los datos personales de los ciudadanos atinentes a su estado civil, lo que obliga, por una parte, a que la institución registral civil responda a las demandas sociales de publicidad de tales datos con la rapidez y eficacia que la sociedad demanda y, por otra parte, se hace necesario mantener los principios tradicionales de respeto a la intimidad de las personas y familias y de seguridad y fiabilidad de los datos que obran recogidos en el Registro Civil.

La legislación vigente en la actualidad en relación con el Registro Civil data del año 1958, con la aprobación de la Ley del Registro Civil, y de 1959 cuando se aprobó el Reglamento de la misma, textos que, con reformas parciales, se mantienen en vigor hasta nuestros días. Ello conduce a derivar que la normativa recogida en estos textos normativos responde de forma insuficiente a la introducción generalizada de las nuevas tecnologías de la información en el ámbito del Registro Civil, ya que los presupuestos de hecho sobre los que tales normas se sustentaban se ven sobradamente superados por la referida tecnología.

El presente estudio se plantea en un momento en el que se comienzan a dar los primeros pasos tendentes a implantar una informatización generalizada de las oficinas registrales en España, lo que necesariamente deberá ser un proceso lento, en el que las experiencias piloto previas deban poner de relieve los diversos aspectos del proceso. En este sentido, durante el año 1996 fue desarrollado en el Registro Civil de Murcia un planteamiento experimental, cuyos resultados servirán para la futura generalización de dicha informatización.

El objeto del presente trabajo se centrará en examinar un aspecto parcial atinente a la referida informatización del Registro Civil, como es el valor

probatorio de los documentos electrónicos en este ámbito, examinando si los mismos pueden ser admitidos sin perturbar ni pugnar con la normativa vigente en este sector del Registro Civil o bien si la eventual introducción de la informática en las oficinas registrales necesitaría una adaptación de la regulación en la materia, con el fin de que los documentos existentes en el ámbito registral sigan manteniendo los principios de fe pública registral, seguridad, publicidad y respeto a la intimidad de las personas, a los que antes se ha aludido, sobre los que el Registro Civil se sustenta.

2º) Metodología.

En el estudio siguiente se comenzará por determinar las características que, según la doctrina científica y la jurisprudencia, deben reunir los documentos para ser considerados como tales, derivándose de dichas características su valor probatorio en el mundo del Derecho *(1º El Documento: ideas generales).*

En el segundo apartado de este estudio se examinarán las características que reúnen los documentos llamados informáticos y si tales características son equiparables con las que en el apartado anterior habíamos establecido como propias de los documentos considerados desde un enfoque tradicional del término *(2º El Documento Informático: características y valor probatorio).*

En el apartado tercero se comenzará por realizar una aproximación a la naturaleza jurídica genérica de los documentos existentes en el ámbito del Registro Civil en España, pasando seguidamente a examinar las características de tales documentos individualmente considerados *(3º Los Documentos en el Registro Civil: ideas generales).*

Seguidamente, en el apartado cuarto se abordarán los extremos dirigidos a determinar si los documentos expedidos a través de las nuevas tecnologías informáticas en el ámbito del Registro Civil reúnen las características que, a la luz de la legislación aplicable en la materia y de conformidad con lo expuesto en el apartado anterior, deben tener dichos documentos para mantener el valor probatorio que la Ley les asigna *(4º Los Documentos Informáticos en el Registro Civil).*

En el último apartado se presentarán las conclusiones que hayan podido derivarse de los apartados desarrollados con anterioridad, con especial

detenimiento en las conclusiones que se refieran propiamente al sector registral civil, objeto específico de este estudio *(III Conclusiones).*

En el trabajo se incluye un Anexo con diversas citas bibliográficas sobre la materia tratada a lo largo del estudio.

II) DESARROLLO

1° El Documento: ideas generales.

1.1) Concepto tradicional.

En el sistema jurídico español, al igual que en resto de los sistemas occidentales, los medios probatorios giran fundamentalmente en torno al instrumento documental. La configuración del documento como elemento probatorio adquiere una preponderancia especial en los ordenamientos continentales de tradición napoleónica, como es el español.

No existe en nuestra normativa una definición expresa y taxativa de lo que debamos entender por documento con carácter general, si bien sí existen definiciones parciales en determinados sectores jurídicos. Cabe afirmar que desde una concepción tradicional del término, el documento se configura únicamente como la representación de un pensamiento escrito en papel. Tal concepto es el que podemos derivar de los *artículos 596* y siguientes de la *Ley de Enjuiciamiento Civil y 1.215* y siguientes del *Código Civil.*

Desde el enfoque representado por la teoría que identifica documento con *"escrito"*, éste consiste en una representación de voluntad, conocimiento o cualquier expresión del pensamiento, plasmada sobre un soporte en papel, mediante signos convencionales, que deriva su autenticidad y fuerza probatoria de la firma que acompaña al mismo, la cual identifica al autor del documento y permite deducir la asunción del contenido documental por parte de éste[1].

■[1] Es tradicional la definición que del "documento" efectúa el Profesor Prieto Castro, para el cual documento es "el objeto o materia en que consta por escrito una declaración de voluntad o de

1.2). Teorías sobre el "documento".

En el punto anterior se hacía referencia a la teoría tradicional que identifica *"documento"* con *"escrito plasmado en papel"*, teoría fundamentada en que dicha identificación permite captar de forma tangible y directa el contenido del documento, reconocer al autor del mismo y posibilita valorar si se ha producido una modificación ulterior del instrumento, notas todas ellas que permiten asignar un valor provatorio específico a las pruebas documentales.

La teoría anterior viene siendo puesta en cuestión por diversos tratadistas, determinada línea jurisprudencial y, por último, las últimas y más recientes reformas legislativas en aspectos parciales de nuestro ordenamiento jurídico.

Para los anteriores, el documento es un mero *"instrumento de representación"*. *Carnelutti* señala que documento es *"una cosa que hace conocer un hecho"*. Se observa por tanto en esta afirmación que el carácter representativo del documento adquiere un papel preponderante en la valoración y configuración del mismo[2]. Todo tipo de mensaje, incluido en cualquier clase de soporte (además del soporte papel), mediante signos convencionalmente acordados (no necesariamente signos alfabéticos o numéricos tradicionales), podría ser considerado como *"documento"*, derivando su fuerza probatoria de las garantías existentes para apreciar en el mismo la inalterabilidad del mensaje y la identidad del autor.

Dentro de la teoría de la *"representación"* es donde debemos enclavar el *"documento electrónico e informático"*, como se desarrollará más adelante,

conocimiento o cualquier expresión del pensamiento según resulta de los preceptos de la legislación positiva".

■[2] En el trabajo presentado por Rouanet Moscardó en el Congreso sobre Derecho Informático celebrado en Zaragoza en 1989 con el nombre de "Valor probatorio procesal del documento electrónico" el mismo conceptuaba el documento como "un objeto normalmente escrito en el que, por tanto, se plasma algo mediante letras u otros signos trazados o impresos sobre el papel u otra superficie, pero que excepcionalmente puede no ser escrito, y es un objeto en el que puede representarse un hecho natural o un acuerdo de voluntad (hecho voluntario, acto o negocio) o ser el resultado de una actividad o de un procedimiento".

caracterizado por las mismas notas esenciales que configuran como tal al documento tradicionalmente considerado como *"escrito"*[3].

1.3). Tipos de documentos y su valor probatorio.

Si atendemos al valor probatorio que la Ley de Enjuiciamiento Civil y el propio Código Civil asignan a los documentos, se deben diferenciar los documentos privados, firmados o no por particulares, y los documentos públicos autorizados por un fedatario o empleado público. Mientras los documentos públicos poseen pleno valor probatorio frente a terceros (*artículo 1.218 C.c.*), los documentos privados adquieren su fuerza probatoria del reconocimiento de las firmas que los autorizan.

La *Ley de Enjuiciamiento Civil*, en su *artículo 578* enumera los medios de prueba de los que se podrá hacer uso en juicio, recogiéndose: la confesión en juicio, los documentos públicos, los documentos privados y la correspondencia, los libros de los comerciantes, el dictamen de peritos, el reconocimiento judicial y los testigos.

Por su parte, el *artículo 1.215* del *Código Civil* determina que las pruebas podrán efectuarse mediante: instrumentos (prueba documental), por confesión, por inspección personal del Juez, por testigos y por presunciones.

Según la más reciente doctrina y jurisprudencia se estima que si bien la relación de los medios de prueba debe considerarse limitativa, no rige sin embargo en nuestro ordenamiento jurídico el principio de apreciación tasada de la prueba, sino un sistema mixto, según el cual se asume el criterio de prueba legal para los medios probatorios consistentes en instrumentos públicos y el sistema de libre apreciación de la prueba *"conforme a la regla de la sana crítica"* para los restantes medios de prueba no excluidos expresamente por la Ley.

[3] Siguiendo al Profesor Valentín Carrascosa "Si entendemos que existe documento privado cuando se fij en un soporte material un mensaje, en un lenguaje destinado a su comunicación, no vemos inconveniente para que un documento electrónico cumpla dichas características, asumiendo la misma naturaleza y valor".

Carrascosa López, Valentín, "Valor probatorio del documento electrónico". **Informática y Derecho nº 8.** 1995, pág. 172.

1.4). La jurisprudencia y el documento electrónico.

Con el fin de realizar un mero apunte sobre la opinión jurisprudencial en relación a la admisión del valor probatorio de instrumentos no caracterizados por las notas tradicionales de los documentos escritos, centrando la materia desde este punto de vista, se debe comenzar por poner de relieve una evidente evolución que comienza en una negativa frontal a la consideración de los medios probatorios basados en las nuevas tecnologías hasta su paulatina y progresiva admisión.

Parece que tanto la Jurisprudencia del Tribunal Supremo, como la del Tribunal Constitucional, admiten un concepto amplio del *"documento"*, sin que éste quede circunscrito al instrumento escrito en el que parecía estar pensando el legislador al aprobar la Ley de Enjuiciamiento Civil y el Código Civil. Un primer argumento expositivo podría consistir en el representado por el párrafo primero del *artículo 3* del *Código Civil* según el cual un criterio básico de interpretación de las normas del ordenamiento jurídico consiste en la *"...realidad social del tiempo en el que han de ser aplicadas (las normas) ..."*, realidad social en la que obviamente no se encontraban presentes los medios probatorios representados por las nuevas tecnologías[4].

Por otra parte la *Constitución*, en su *artículo 24.2* contempla como derecho fundamental la posibilidad de utilizar todos los medios de prueba pertinentes para la defensa, norma que si bien se plantea desde un enfoque penal, posee sin duda un carácter expansivo al resto del ordenamiento jurídico. Por ello, la relación de medios probatorios prevista en el *artículo 578* de la *Ley de Enjuiciamiento Civil* y en el *artículo 1.215* del *Código Civil* no debe entenderse herméticamente cerrada, sino con un carácter abierto a otros medios probatorios[5].

■[4] La Sentencia de la Sala Primera del Tribunal Supremo de 5 de febrero de 1.988, en su Fundamento Jurídico Primero afirma "2. Todavía más, de alguna manera dichos medios técnicos pueden subsumirse en el concepto mismo amplio de documento, en cuanto cosas muebles aptas para la incorporación de señales expresivas de un determinado significado".

■[5] Sentencia de la Sala Primera del Tribunal Supremo de 30 de noviembre de 1.992, en su Fundamento de Derecho Primero.

El problema central no parece ser la admisión del *"documento electrónico"* como medio probatorio, sino el valor que la jurisprudencia asigna a dicha prueba. En este sentido cabe exponer dos fases en el desenvolvimiento jurisprudencial de tal apreciación probatoria, siguiendo algunas de las consideraciones de *Julio José Elías Baturones* sobre esta materia[6].

Una primera fase es la representada por una postura reticente a la aceptación de los instrumentos probatorios basados en las nuevas tecnologías, a los que, dada la dificultad para garantizar su autenticidad, la jurisprudencia niega prácticamente un valor probatorio por sí mismos[7].

En un segundo momento, se acepta el valor probatorio de los medios basados en las nuevas tecnologías, si bien su autenticidad debe venir adverada por otros medios probatorios[8]. Esta adveración supone la garantía de seguridad de la que algunos medios probatorios, sustentados en nuevas tecnologías, carecen con carácter general, dada su facilidad para ser modificados y manipulados sin dejar constancia de la manipulación, según el criterio sustentado por esta visión jurisprudencial[9], tesis apoyada por otra parte por diversas Sentencias del Tribunal Constitucional[10].

■[6] Elías Baturones, Julio José, "La Jurisprudencia ante el documento electrónico: su aceptación como prueba documental", **Tapia, octubre-noviembre 1.996**, pág. 65.

■[7] Sentencia de la Sala Primera del Tribunal Supremo de 30 de noviembre de 1.981.

■[8] La Sentencia de la Sala Primera del Tribunal Supremo de 30 de noviembre de 1992, con relación a lo "progresos científicos" afirma que "...En todo caso su utilización probatoria exige siempre la necesaria y precisa adveración y certificación de autenticidad, veracidad y fidelidad que encuentra cauce procesal adecuado mediante el reconocimiento judicial sometido a las reglas de procedimiento y valoración previstas...".

■[9] La Sentencia de la Sala Primera del Tribunal Supremo de 17 de abril de 1989 indica con referencia a la reproducción de la imagen o la voz que "...En todo supuesto documental es necesario un plus de credibilidad (...), que en los supuestos de reproducción mecánica puede operar en dos direcciones distintas: a) Como objeto de prueba en cuanto se estime que la imagen o la voz corresponden de modo efectivo a la persona y b) Como tal documento, cuando su reproducción de un hecho pasado (...) sea adverada por distintos medios probatorios, cual el testifical."

■[10] Sentencias del Tribunal Constitucional núm. 128/1988, de 27 de junio y núm. 190/1992, de 16 de noviembre.

Entendemos que en el estado jurisprudencial actual sobre la materia, no cabe hablar, al menos por el momento, de una aceptación plena de los medios probatorios sustentados sobre las nuevas tecnologías, como modalidad independiente y singularizada de prueba documental, y por tanto, el carácter probatorio de tales instrumentos estará ligado a las garantías de autenticidad, seguridad, inalterabilidad y perdurabilidad que se predican del resto de pruebas documentales[11].

1.5). El documento electrónico en la normativa vigente.

Nuestro ordenamiento jurídico carece de normas de aplicación general que aborden la plena admisión de los documentos emitidos por medios electrónicos, informáticos o telemáticos y el valor probatorio que pudiera asignarse a los mismos.

No obstante, en los últimos años se asiste a una paulatina admisión de tales documentos y medios probatorios, en diversas normas, tanto legales como reglamentarias, que otorgan plena validez y eficacia a los documentos emitidos y transmitidos por medios basados en las nuevas tecnologías, fundamentalmente de tipo informático. Toda esta normativa sectorial presenta un elemento común, en el que se basa normalmente la admisión de estos instrumentos con plenos efectos, elemento consistente en la necesidad de que quede garantizada, por los medios que en cada caso se determinen, la integridad y autenticidad del documento en cuestión.

Sin ánimo de exhaustividad y únicamente a efectos ejemplificativos, cabe hacer alusión a determinadas normas que han asignado al documento electrónico un carácter inequívocamente documental, supeditando su valor probatorio a las garantías con las cuales tales documentos hayan sido producidos.

■[11] Según estima el Prof. Valentín Carrascosa "...podemos afirmar que el documento electrónico adquiere valor de prueba documental, con el alcance que señala el art. 1.225 y ss. del Código Civil, equiparándose así a cualquier otro documento privado, cuya eficacia probatoria no sería inmediata, teniendo que ser reconocido por las partes o autentificado por Notario, para hacer prueba plena en juicio". Op. citada en nota 3, pág. 172.

La *Ley 16/1985 del Patrimonio Histórico, de 25 de junio de 1985 (BOE 29-6-85)*, en su *artículo 49*, conceptúa al documento como toda expresión en lenguaje natural o convencional, así como *"...cualquier otra expresión gráfica, sonora o en imagen, recogidas en cualquier tipo de soporte material, incluso los soportes informáticos"*.

La *Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial (BOE 2-7-85)*, admite la utilización en los procesos judiciales de medios técnicos de documentación y reproducción, siempre que reúnan las debidas garantías de autenticidad (*artículo 230*).

La *Ley 24/1988, de 28 julio de 1.988, del Mercado de Valores (BOE 29-7-88)*, en su *artículo 5*, admite la representación de acciones mediante anotaciones en cuenta sustentadas en registros informáticos. En el mismo sentido se pronuncia la *Ley 19/1989, de 25 de julio de 1989 (BOE 27-7-89)*, que modifica el *artículo 38* de la *Ley de Sociedades Anónimas*.

La *Ley 30/1992, de 26 de noviembre (BOE 27-11-92), reguladora del Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común*, establece, en su *artículo 45*, los preceptos siguientes, los cuales se transcriben en su integridad, dado el interés que los mismos presentan para el tema objeto de este estudio:

"1. Las Administraciones Públicas impulsarán el empleo y aplicación de las técnicas y medios electrónicos, informáticos y telemáticos, 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.

2. Cuando sea compatible con los medios técnicos de que disponen las Administraciones Públicas, los ciudadanos podrán relacionarse con ellas para ejercer sus derechos a través de técnicas y medios electrónicos, informáticos o telemáticos, con respeto de las garantías y requisitos previstos en cada procedimiento.

3. Los procedimientos que se tramiten y terminen en soporte informático garantizarán la identificación y el ejercicio de la competencia por el órgano que la ejerce.

4. Los programas y aplicaciones electrónicas, informáticos o telemáticos que vayan a ser utilizados por las Administraciones Públicas para el ejercicio de sus potestades, habrán de ser previamente aprobados por el órgano competente, quien deberá difundir públicamente sus características.

5. Los documentos emitidos, cualquiera que sea su soporte, por medios electrónicos, informáticos o telemáticos por las Administraciones Públicas, o los que éstas emitan como copias de originales almacenados por estos mismos medios, 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 éstas u otras Leyes".

En desarrollo de este artículo, el *Real Decreto 263/1996, de 16 de febrero (BOE 29-2-96)*, reguló la utilización de técnicas electrónicas, informáticas y telemáticas por la Administración General del Estado.

La *Ley 37/1992, de 28 de diciembre de 1.992 (BOE 29-12-92), reguladora del Impuesto sobre el Valor añadido*, permite, en su *artículo 88*, que la repercusión del impuesto se efectúe mediante factura o documento análogo, que podrá emitirse por vía telemática, siempre que se garanticen los requisitos que reglamentariamente establezca la Administración *(Real Decreto 29-12-92; BOE 31-12-92)*.

Dentro del ámbito registral, al que se aludirá con mayor extensión más adelante, cabe mencionar la *Ley Orgánica 7/1992, de 20 de noviembre (BOE 21-11-92)*, que introduce la posibilidad del tratamiento automatizado de las inscripciones registrales, posibilidad que debía ser desarrollada reglamentariamente. Por su parte, el *Real Decreto de 30 de marzo de 1990*, que modifica el *Reglamento Hipotecario* permite la utilización de medios informáticos en su ámbito competencial.

La *Ley Orgánica 10/1995, de 23 de noviembre (BOE 24-11-95)*, que aprueba el nuevo *Código Penal*, establece en su *artículo 26*, la consideración que a efectos penales posee el concepto de documento:

"A los efectos de 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".

Las transmisiones informáticas de declaraciones de datos en numerosos ámbitos sectoriales como pueden ser los de aduanas, Sistema Nacional de Compensación Electrónica Interbancaria, en materia tributaria, de Seguridad Social, Administración de Justicia o de expedición de Títulos académicos y profesionales, entre otros, se encuentran profusamente reguladas por una extensa normativa dictada en cada sector.

La enumeración anterior puede ofrecer una semblanza de la amplia extensión alcanzada en nuestro ordenamiento jurídico en lo que respecta a la aceptación del *"documento informático"* como instrumento con lugar propio y definido junto con otros conceptos jurídicos más tradicionalmente asentados. La trascendencia jurídica y el valor que a efectos probatorios se asigne a tal figura estará directamente relacionado con el cúmulo de garantías que rodeen a su confección, conservación y transmisión, aumentando tal valor en la medida en que se garantice la autenticidad, integridad y seguridad de su contenido[12].

2. El documento electrónico: características y valor probatorio.

Podemos efectuar una primera aproximación a la definición de *"documento electrónico"* afirmando que es aquel instrumento producido por medios electrónicos, por lo que por extensión, consideraremos *"documento informático"* todo aquel que haya sido producido por medios informáticos.

Esta primera aproximación, obviamente incompleta, debe ser perfilada con la detenida exposición de las características que de alguna manera han sido predicadas de los documentos tradicionalmente considerados y su

■[12] Como afirma el Profesor Valentín Carrascosa López en op. cit. en nota 3 (pág. 165) "... podríamos llegar al caso de una discriminación legal, no tanto de las personas, como de las situaciones, dado el carácter sectorial del reconocimiento que nuestro legislador hace del documento electrónico, por lo que insistimos en la necesidad de que sea la normativa general la que regule para todos los supuestos la admisión, efectos y requisitos del documento electrónico como elemento probatorio ...".

posible asimilación a las características que presentan los *"documentos informáticos"*. Tales notas características aluden por una parte a los aspectos formales del documento y, en segundo término, a los aspectos que debe reunir el documento para derivar del mismo un valor probatorio con trascendencia en el mundo jurídico.

a) Soporte material.

El primer aspecto al que podemos hacer alusión está referido al soporte material en el que el contenido del documento se encuentra plasmado. El concepto tradicional de documento escrito identifica este requisito con el *"soporte papel"*. Pero tal identificación no puede dejar al margen otros soportes materiales que históricamente se utilizaron para plasmar de forma perdurable y representativa otros aspectos de la vida social e individual (piedra, papiros, pieles, murales ...).

Con relación a los documentos producidos mediante las nuevas tecnologías, no es posible obviar aquellos soportes materiales basados en cintas de video o audio, películas fotográficas, cintas magnéticas, discos ópticos o cualquier otro tipo de material.

Dentro de los *"documentos informáticos"*, no presentan mayores problemas a estos efectos aquellos documentos generados en papel y que tienen su origen en mecanismos electrónicos informáticos.

En segundo lugar cabría hacer referencia al documento en pantalla, procedente de un disco fijo o móvil, cuyo soporte material estaría formado por la propia pantalla donde el mismo se proyecta, si bien su carácter evanescente genera reparos en cuanto a la necesaria perdurabilidad que, en principio, debe caracterizar al documento.

Por último, se debe aludir al documento grabado en el propio disco, ya sea el disco fijo del ordenador o cualquier disco magnético u óptico móvil, que haya sido incorporado al mismo de forma directa o mediante cualquier procedimiento de incorporación de imágenes de un documento previamente existente en papel.

b) Factor representativo.

Sobre el soporte antes aludido debe existir una representación de objetos, hechos, ideas, conceptos o voluntades personales. Este carácter representativo que se atribuye al documento lo diferencia de otros medios probatorios.

No parece existir obstáculo alguno para considerar que este elemento representativo se encuentra presente en el *"documento informático"*, donde pueden quedar plasmados todo tipo de extremos susceptibles de ser recogidos en forma representativa, con mayor o menor grado de identidad con relación al objeto real representado.

c) Signos convencionales.

Un tercer elemento a considerar está formado por aquellos vehículos que sirven para plasmar en el soporte material la representación del objeto correspondiente. Desde un enfoque tradicional, los signos convencionales característicos utilizados para esta finalidad son los constituidos por los signos de escritura o representación gráfica, en su caso.

No obstante lo anterior, no parece que los signos convencionales utilizados en el lenguaje escrito o gráfico sean los únicos que se deban considerar, puesto que existen otros vehículos de representación que, con referencia al *"documento informático"* está constituido por los *"bits"* ordenados de conformidad con un sistema de *"algebra binaria"* determinado.

Algunos tratadistas del tema han afirmado que el documento debe ser un instrumento inteligible por sí mismo, sin necesidad de ningún medio interpuesto que permita captar su contenido, por lo que, basándose en la necesidad de utilizar *"descodificadores"* para hacer inteligible el lenguaje informático, niegan la condición documental al *"documento informático"*. Esta postura doctrinal no posee un suficiente apoyo legal ni jurisprudencial, ya que el requisito de tener que contar necesariamente con un elemento auxiliar para generar o captar el mensaje del documento no parece que sea una condición suficiente para negar la condición documental a todos los efectos al objeto producido con la intervención de dichos medios técnicos.

d) Firma.

Como se ha señalado en el punto 1, la firma documental constituye un elemento distintivo que permite, por una parte, atribuir el contenido de un documento a un sujeto personal y, en segundo lugar, derivar de la misma el consentimiento del autor sobre el contenido plasmado en el soporte. Se distinguen por tanto dos elementos funcionales de la firma, como son la identificación y la autentificación, de donde se derivan buena parte de los efectos probatorios que el ordenamiento jurídico atribuye a la prueba documental.

El hecho de que en la actualidad la firma sea entendida con un carácter manuscrito, no es obstáculo para admitir asimismo como firma todo signo del que se pueda derivar la identidad del que suscribe el documento y la voluntad de adherirse a su contenido (*"animus signandi"*). Por otra parte no existe en el ordenamiento jurídico una definición general sobre lo que deba ser entendido a efectos jurídicos por firma y, salvo excepciones concretas, tampoco se exige la existencia de firma manuscrita.

La firma en el *"documento informático"* no puede ser, manuscrita, si bien existen toda una serie de mecanismos electrónicos capaces de cumplir, creemos que sobradamente, las funciones atribuidas tradicionalmente a la firma manuscrita.

Entre los mecanismos antes referidos cabe aludir a los códigos secretos, los métodos criptográficos y los métodos de reconocimiento de rasgos biométricos, que se exponen brevemente a continuación solamente en lo que a sus implicaciones jurídicas afecta, dejando al margen otros aspectos técnicos ajenos a este estudio.

El código secreto está formado por una combinación de números y/o letras que identifica al emisor del mensaje y que, al ser conocido por el destinatario, permite a éste atribuir el mensaje a su emisor. La funcionalidad del método depende de forma directa de la confidencialidad del código secreto del emisor.

Los métodos criptográficos consisten en la codificación del mensaje a transmitir, incluyendo los elementos de identificación personal del

emisor, codificación que se lleva a cabo mediante el uso de claves y algoritmos[13]. Los sistemas criptográficos pueden ser simétricos cuando una misma clave o algoritmo permite realizar el ciframiento y desciframiento del mensaje. Los sistemas asimétricos serán aquellos que necesitan una clave o algoritmo para cifrar y otra distinta para descifrar el mensaje.

Por último, cabe aludir a los sistemas de reconocimiento de rasgos biométricos del emisor, métodos éstos en periodo de estudio y progresivo afianzamiento, consistentes en el reconocimiento de la voz, la imagen, huellas dactilares etc. Así mismo cabe incluir dentro de este apartado los sistemas de reconocimiento de firmas, basados no sólamente en el reconocimiento informático de grafismos, comparándolo con un modelo de referencia, sino en el reconocimiento de la firma original por medición de la velocidad de escritura, impulso, presión de escritura etc.

Se debe tener en consideración que la plasmación de la firma digital en un documento informático permite, dependiendo de los programas y aplicaciones utilizados, bloquear la eventual modificación posterior del documento, por lo que éste queda *"blindado"*, con lo que se incrementa de forma capital la fiabilidad del sistema en cuanto a los contenidos del documento.

La mera enunciación de los métodos citados permite cumplir las finalidades de identificación personal y autentificación del *"documento informático"*, satisfaciendo en muchos casos con ventaja las funciones que tradicionalmente se han atribuido a la firma manuscrita en los documentos.

e) Integridad.

La trascendecia de un documento en cuanto a su valor probatorio depende, en primer térm no, de la integridad del contenido de dicho documento. Un documento no puede quedar seccionado en parte de su contenido, ya que ello sería desvirtuar el mismo e inutilizarlo prácticamente como prueba en el mundo

[13] La Norma ISO 7498 define la Clave o "Llave" a estos efectos como "... una serie de símbolos comandando las operaciones de ciframiento y de desciframiento...". La Norma ISO 2382 define un "Algoritmo" como "... un conjunto finito de reglas determinadas que sirven para resolver un problema por medio de un número finito de operaciones...".

jurídico. Se ha afirmado por parte de algunos estudiosos del tema que un *"documento informático"*, transmitido por vía electrónica podría no ser recibido en su integridad por el destinatario o ni siquiera ser recibido en forma alguna, lo que provocaría una inseguridad jurídica que revertiría en el valor probatorio que asignásemos a estos documentos.

No obstante lo anterior, en el momento actual de la técnica es perfectamente posible no sólo tener constancia de que el documento se ha recibido por parte del destinatario, sino que se ha recibido en su integridad. El procedimiento utilizado para esta finalidad es el conocido como *"sellamiento"* del mensaje, según el cual el mensaje completo se condensa de forma algorítmica y acompaña al mensaje durante la transmisión, siendo recalculado al final de dicha transmisión en función de las características del mensaje realmente recibido. Cuando todos los datos precisos no aparezcan en el mensaje transmitido, el sello recalculado no coincidirá con el sello original, poniéndose de manifiesto que en la transmisión existió un problema y el destinatario no dispone del mensaje completo.

Los medios técnicos disponibles en la actualidad permiten asimismo hacer saber al emisor que el destinatario ha *"abierto su buzón"* de correo electrónico y presumiblemente ha leído el mensaje.

Anteriormente se ha hecho alusión a la capacidad de determinados sistemas informáticos para *"blindar"* un documento, una vez que sobre el mismo se ha plasmado la firma digital correspondiente, lo que supone la imposibilidad de proceder a ulteriores modificaciones del mismo.

f) Autenticidad.

Intimamente unido con la característica anterior, se encuentra la nota de autenticidad documental, la cual es relativamente fácil de predicar de los documentos tradicionales escritos, al apreciarse si ha existido alteración o modificaciones del mismo posteriormente a su firma. Esta nota ha sido puesta en entredicho con referencia a los *"documentos informáticos"*, ya que los mismos son susceptibles de ser modificados, sin que sea posible, dadas sus características, apreciar dicha modificación.

Con referencia al mundo de la informática, esta característica debe examinarse ligada de forma necesaria a la seguridad en las transmisiones

electrónicas y a la imposibilidad de modificar un documento informático sobre el cual se ha plasmado una firma digital. Al hacer referencia a la firma se examinaban los procedimientos que permitían una razonable seguridad en la transmisión de los datos informáticos, evitándose mediante códigos secretos, sistemas de encriptación o medios de reconocimiento de rasgos biométricos que el mensaje enviado pudiera ser interceptado en su viaje hasta el destinatario, métodos a los que se deben añadir la imposibilidad de modificar un documento sobre el que se haya plasmado una firma digital.

La autenticidad del mensaje recibido corre en paralelo con su confidencialidad y la seguridad de la que dotemos a las transmisiones, características éstas que en el momento actual pueden predicarse con mayor rigor de los documentos informáticos que incluso de los documentos tradicionales plasmados sobre papel. Como dato meramente anecdótico, cabe hacer referencia a la prohibición existente en USA, hasta tiempos recientes, de utilizar el sistema de encriptación conocido como PGP, dada la práctica imposibilidad policial de interceptar los mensajes transmitidos, lo que en algunos supuestos favorece determinados tráficos ilegales.

Según lo expuesto, las notas de integridad y autenticidad de las que los documentos derivan buena parte de su valor probatorio en el mundo del Derecho, pueden ser conseguidas en el ámbito de los *"documentos electrónicos"*, con la aplicación de las necesarias medidas de seguridad que de forma necesaria deben ser incorporadas a los sistemas informáticos.

Otro problema distinto de los hasta ahora expuestos, consiste en la utilización de las medidas de seguridad informáticas, desde dentro de las distintas organizaciones, de forma discrepante con la voluntad de quien debiera en principio tomar las decisiones sobre un tema determinado. No obstante, este problema, sin duda existente y de gran importancia, debe solventarse haciendo extensivo el ámbito de responsabilidad a todo el colectivo personal interno emisor del mensaje, con independencia de que en un momento posterior pudieran depurarse las responsabilidades a que hubiera lugar.

g) Conservación.

Determinados sectores doctrinales, así como algunas regulaciones positivas establecidas en la materia, han puesto de relieve la necesidad de que el documento, para ser considerado como tal y poder derivar del mismo el valor probatorio atribuido al *"documento"* desde un enfoque tradicional, debe perdurar en el tiempo. Esta característica, más que un requisito propio e independiente del resto de caracteres antes definidos, debe acompañar al documento en general y al electrónico en particular para que éste adquiera una relevancia probatoria equiparable a los documentos en soporte de papel.

En contra de la conservación y perdurabilidad temporal del documento electrónico juegan, por una parte, el deterioro de los soportes informáticos donde se hayan almacenado los datos y, por otra parte, el deterioro o destrucción documental ocasionado por la concurrencia de los conocidos como *"virus informáticos"*, *"bombas lógicas"* o cualquier otro dispositivo o programa informático ideado para destruir los bancos de datos informáticos.

No parece que la característica de conservación y perdurabilidad en el tiempo del documento informático pueda ser predicada como una nota para valorar el carácter y el valor probatorio del documento electrónico, puesto que, por más que pueda ser deseable e incluso necesaria la instalación de medidas de seguridad y dispositivos de defensa contra estas eventualidades, en tanto el documento exista en su integridad mantendrá todo el valor probatorio que al mismo se le asigne, con independencia de las medidas de seguridad que se hayan adoptado para su conservación y mantenimiento.

3°). Los documentos en el ámbito del Registro Civil: ideas generales.

3.1). Naturaleza Jurídica.

Antes de pasar a exponer los documentos existentes en el ámbito registral civil conviene realizar algunas reflexiones sobre la naturaleza de los Registros Civiles en España, de la cual se derivará el valor que la legislación vigente atribuye a los documentos existentes y producidos en la institución registral.

El Registro Civil se encuadra dentro del sector de registros a los que la normativa vigente atribuye la función de hacer efectiva la publicidad de situaciones jurídicas diversas relativas al *"estado civil"* de los ciudadanos. Este tipo de Registros cumple fundamentalmente la función de dotar de certidunbre a las relaciones jurídicas[14]. Por ello, su característica definitoria radica en potenciar el principio de *"seguridad jurídica"* previsto en el *Texto Constitucional (Art. 9.3 C.E.)*[15].

Por sus notas definitorias el Registro Civil se sitúa dentro del mismo grupo clasificatorio donde se encuentran asimismo el Registro de la Propiedad Inmobiliaria, el Registro de la Propiedad Intelectual, el Registro de la Propiedad Industrial, el Registro de Hipoteca Mobiliaria y Prenda sin Desplazamiento, el Registro de Valores Anotados, el Registro Mercantil, el Registro de Cooperativas, el Registro de Venta a Plazos o el Registro de Actos de Ultima Voluntad.

Todos los Registros mencionados se encuentran dentro del ámbito del *Derecho Civil (Artículo 149, apartado 1º, 8ª CE)*, lo que les diferencia en sustancia de una serie de Registros Administrativos, cuyo funcionamiento se dirige básicamente a dotar a la Administración de información para el desarrollo de sus actividades, Registros estos últimos cuyos datos cumplen una función diferente a las inscripciones obrantes en los Registros que hacen efectiva la publicidad de *"situaciones jurídicas"*[16].

Las inscripciones que obran en el Registro Civil constituyen la *"verdad oficial"* de las situaciones jurídicas, sirviendo de instrumento de publicidad de los hechos relativos al estado civil de las personas. Para que esta *"verdad oficial"* se llegue a constituir, el ordenamiento jurídico establece un sistema rígido de acceso de datos al Registro Civil, así como de rectificación de los datos obrantes

■[14] Leyva de Leiva, J.A. "Planteamiento general de los Registros públicos y su división en Registros Administrativos y Registros Jurídicos", **Revista Crítica de Derecho Inmobiliario, nº 591, marzo-abril 1.989,** pág. 298.

■[15] García García, J.M. "La función registral y la seguridad del tráfico inmobiliario", **Revista Crítica de Derecho Inmobiliario, nº 625, noviembre-diciembre 1.994,** pág. 2248.

■[16] Pau Pedrón, Antonio, **Curso de Práctica Registral**, Madrid: U.P.C., 1.995, pág. 21.

en las inscripciones, bien mediante expediente gubernativo o bien a través de sentencia judicial. El Encargado del Registro deberá calificar la legalidad del acto o documento cuyos datos deban acceder al Registro, calificación que incluye la pertinencia del asiento de conformidad con otras inscripciones que ya figuren en el Registro.

Con el fin de dotar de mayores dosis de seguridad jurídica a los datos proclamados por el Registro, el ordenamiento jurídico asigna a los datos inscritos unas atribuciones de especial relevancia probatoria. Así, el *artículo 1.2* de la *Ley del Registro Civil, de 8 de junio 1.957 (BOE 10-6-57)*, dispone que:

"El Registro Civil constituye la prueba de los hechos inscritos. Sólo en los casos de falta de inscripción o en los que no fuere posible certificar del asiento, se admitirán otros medios de prueba; pero en el primer supuesto será requisito indispensable para su admisión que, previa o simultáneamente, se haya instado la inscripción omitida o la reconstitución del asiento"[17].

En relación a lo anterior, y con el propósito de clarificar el contenido de lo expuesto, se debe indicar que las inscripciones del Registro Civil hacen fé pública de algunos de los datos contenidos en las diversas inscripciones y no de todos los datos recogidos en las mismas. Los datos de los que cada inscripción hace fé están especificados en los *artículos 41, 69 y 81 LRC*, para las inscripciones de nacimiento, matrimonio y defunción respectivamente.

Según lo anterior, con carácter general se puede afirmar que las inscripciones de nacimiento harán fe *"... del hecho, fecha, hora y lugar del nacimiento, del sexo y, en su caso, de la filiación del inscrito"*. Las inscripciones de matrimonio hacen fe *" ... del acto del matrimonio y de la fecha, hora y lugar en que se contrae"*. Por último, las inscripciones de defunción hacen fe *"... de la muerte de una persona y de la fecha, hora y lugar en que acontece"*. El hecho de que las inscripciones hagan fe o no del dato correspondiente se convierte en un extremo de especial importancia a la hora del procedimiento a utilizar para la rectificación de los mismos (*artículos 92 y siguientes L.R.C. y artículos 93 y siguientes R.R.C.*).

■[17] En términos similares se expresa el artículo 327 del Código Civil.

Los Libros de Inscripciones del Registro Civil gozan de la condición de *"documento público"* (artículos 1.216 y siguientes del C.c. y artículos 596 y siguientes de la L.E.C.), con el privilegiado valor probatorio que el ordenamiento jurídico español atribuye a estos documentos[18].

La *Ley del Registro Civil*, en su *artículo 7*, otorga asimismo valor de *"documento público"* a las certificaciones expedidas por el Registro Civil. En el mismo sentido se pronuncia el *artículo 596.6* de la *Ley de Enjuiciamiento Civil*.

3.2) Clases.

En el ámbito registral civil, cabe efectuar una primera clasificación de los Libros utilizados en las oficinas registrales, clasificación que será de utilidad expositiva a la hora de examinar la materia propia de este trabajo. En primer término se puede hacer referencia a los *Libros Principales y a los Auxiliares*. Son *Libros Principales* aquellos en los que constan, divididos por Secciones, los asientos registrales, asientos que podrán ser inscripciones, con pleno valor probatorio y anotaciones con mero carácter informativo. A su vez las inscripciones podrán ser principales o marginales, según abran folio registral o bien reflejen incidencias posteriores a dicha inscripción principal. Los asientos del Registro que afecten a una misma persona deberán estar interconectados mediante la práctica de las *"notas marginales de referencia"* a que hubiere lugar.

Los *Libros Auxiliares* poseen un carácter instrumental, y aunque de primordial importancia para el funcionamiento interno del Registro, sus asientos no sirven directamente la finalidad de publicidad propia del Registro Civil. Por tal razón el valor probatorio de sus asientos no gozan de las mismas atribuciones que el de los *Libros Principales*. Son *Libros Auxiliares*: el Libro Diario, el Libro de Personal y Oficina, Expedientes, Abortos, Ficheros, Fes de Vida, Cuadernos Auxiliares y Otros documentos. Dada la sustancial diferencia existente entre éstos Libros y los Principales, en cuanto a su valor probatorio, dejaremos su examen al margen de este estudio.

■[18] Ver apartado 1.3, pág 12.

Junto a los Libros anteriores de carácter interno a la oficina registral, la publicidad de los datos obrantes en el Registro de cara al exterior se lleva a cabo mediante la expedición de *"certificaciones"*, las cuales, como se ha señalado anteriormente, gozan de la condición de documento público.

Merece una referencia individualizada los Libros llevados en el Registro Civil Central, donde junto con los *Libros de Inscripciones* divididos en Secciones, para la práctica de los asientos para los que el Registro Civil Central tiene competencia, se llevan asimismo los Libros formados por los duplicados de las inscripciones practicadas en los Registros Civiles Consulares de España en países extranjeros, así como el *Libro de Matrimonios Secretos.*

Por su carácter instrumental dejamos fuera de nuestro estudio los documentos utilizados en la tramitación de los expedientes gubernativos en las oficinas registrales, documentos que presentan un campo especialmente abonado para su automatización, en aras de una mayor flexibilidad, rapidez y mejora del servicio prestado.

Seguidamente se exponen brevemente las características que deben reunir tanto los documentos donde constan las inscripciones, como los destinados a posibilitar fundamentalmente la publicidad de los asientos, paso éste previo para examinar en el próximo apartado si los *"documentos informáticos"* que pudieran ser emitidos por los Registros Civiles reúnen los requisitos necesarios establecidos por la normativa registral para los documentos definidos en su ámbito.

3.3) Libros Principales.

El Registro Civil se encuentra dividido en cuatro Secciones. La primera será de *"Nacimientos y general"*, la segunda de *"Matrimonios"*, la tercera de *"Defunciones"*, y la cuarta será la de *"Tutelas y representaciones legales"* (*Artículo 33 L.R.C.*). Cada una de las Secciones se llevará en Libros distintos. Los Libros estarán formados por hojas fijas o por hojas móviles, foliadas y selladas, donde se expresarán la Sección y tomo del Registro (*artículo 105 R.R.C.*). Por folio u hoja registral se entiende la parte del Libro dedicada a cada una de las inscripciones principales y sus asientos marginales, con independencia del número de sus páginas (*artículo 131 R.R.C.*). A estos efectos se consideran inscripciones principales las primeras inscripciones de nacimiento, matrimonio, defunción y la

primera de cada tutela o representación legal, el resto de los asientos se practicarán de forma marginal a sus correspondientes inscripciones principales.

Los asientos se extenderán sin dejar folios o espacios en blanco, siendo nulas las adiciones, apostillas, interlineados, raspaduras, testados o enmiendas que no se salven al pie del asiento antes de firmarlo (*artículo 34 L.R.C.*).

Los asientos deberán ir firmados por el Encargado y el Secretario del Registro respectivo (*artículo 37 L.R.C.*). Asimismo, el asiento practicado en virtud de declaración será también firmado por el declarante o por dos testigos a su ruego (*artículo 36 L.R.C.*)

3.4) Libros del Registro Civil Central.

En relación con los Libros llevados en el Registro Civil Central (*artículo 99 R.R.C.*)[19], además de los Libros ordinarios destinados a los asientos para cuya práctica es competente este Registro, divididos por Secciones, en el mismo se llevan también los Libros formados con los duplicados de los asientos practicados por los Registros Civiles Consulares de España en los paises extranjeros. Dichos duplicados deberán estar convenientemente firmados con firmas originales, por la autoridad consular que los autorice, siendo incorporados al Registro Civil Central mediante la oportuna diligencia de incorporación, asimismo firmada por la autoridad correspondiente de este Registro.

Los duplicados deberán tener idénticas dimensiones y formatos que los folios de los Libros ordinarios, los cuales serán encuadernados convenientemente una vez que se alcance el número de folios pertinente (*artículos 118 y 119 R.R.C.*).

Por su parte, los duplicados de los asientos practicados en el Registro Civil Central serán asimismo remitidos a los Registros Consulares correspondientes, los cuales incorporarán tales duplicados a sus Libros.

En el Registro Civil Central se llevará también el *Libro de Matrimonios Secretos*, donde se inscribirán los matrimonios de conciencia celebrados

[19] El Real Decreto 2721/1979, de 5 de octubre, reguló los Libros del Registro Civil Central.

ante la Iglesia, si así lo solicitan ambos contrayentes y los matrimonios civiles celebrados en secreto por dispensa (*artículo 78 L.R.C. y 121 R.R.C.*).

3.5)- Certificaciones y Libro de Familia.

Como se ha reflejado anteriormente, la publicidad de los datos contenidos en el Registro Civil se realiza, de manera principal, a través de la expedición de certificaciones, si bien tal publicidad también puede llevarse a cabo mediante el examen directo de Libros y documentos en el propio Registro y a través de la expedición de notas simples sin valor probatorio alguno, medios éstos que deben calificarse de marginales en relación con la expedición de certificaciones, ámbito en el se centrará el examen de este apartado.

Según se desprende del *artículo 28 RRC* las certificaciones pueden ser *"positivas"* o *"negativas"*, según hagan constar los datos recogidos en el Registro o la ausencia de los asientos interesados. Las certificaciones positivas pueden ser a su vez *"literales"* y *"en extracto"*, distinción que dadas sus características puede tener gran relevancia de cara a la informatización del ámbito registral.

Las certificaciones literales *"...comprenden íntegramente los asientos a que se refieren ..."*, con lo que son aquí de especial importancia las reglas sobre protección de la intimidad personal y familiar.

Por el contrario, en la certificaciones en extracto u ordinarias se harán constar los datos de los que la inscripción hace fe, los cuales varían según que la inscripción sea de nacimiento, matrimonio o defunción, de conformidad con lo que resulte de las inscripciones modificativas que se hayan practicado con posterioridad, sin expresión de éstas, indicándose también en las mismas las notas de referencia oportunas que conecten la inscripción con otras secciones del mismo u otros Registros Civiles distintos.

Las certificaciones en extracto contienen un menor número de datos susceptibles de ser protegidos en cuanto a su publicidad que las certificaciones literales, las cuales en buena parte de los casos se expiden mediante fotocopia del asiento.

Las certificaciones deberán ir firmadas por el Encargado o Secretario autorizante, o bien por el personal registral autorizado al efecto.

Constituye igualmente un instrumento de publicidad registral la expedición del Libro de Familia, en el cual constará la inscripción del matrimonio de los padres, en caso de existir, y las inscripciones de los nacimientos de los hijos. El Libro de Familia posee valor de certificación en extracto de los asientos que contiene.

4. Documentos Informáticos en el Registro Civil.

4.1. Normativa específica en materia de informatización del Registro Civil.

La *Ley Orgánica 7/1992, de 20 de noviembre (BOE 21-11-92)*, modificó el *artículo 6 de la Ley del Registro Civil*, estableciendo de forma breve que:

"...Las inscripciones registrales podrán ser objeto de tratamiento automatizado".

En la Ley se añadía una *Disposición Adicional* en la *Ley del Registro Civil*, en la cual se preceptuaba que:

"A los efectos establecidos en el artículo 6 de la presente Ley las referencias que en la misma se realizan a los libros y asientos marginales, podrán entenderse referidos a los ficheros automatizados registrales y al tratamiento de éstos".

Asimismo, la *Ley Orgánica 7/1992* introdujo la *Disposición Final Tercera de la Ley del Registro Civil*, según la cual

"Reglamentariamente se establecerán los requisitos, la forma de practicar los asientos y expedir certificaciones y las demás condiciones que afecten al establecimiento y gestión de los ficheros automatizados de datos registrales".

En los aspectos atinentes al Registro Civil las disposiciones de la *Ley Orgánica 7/1992* carecen del carácter de Ley Orgánica.

En el ámbito reglamentario, el *Real Decreto 1917/1986, de 29 de agosto*, había modificado el *artículo 105 del Reglamento del Registro Civil*, con una entonces discutible cobertura legal. En dicho Real Decreto se determinaba que

"... El Ministerio de Justicia podrá igualmente decidir, sin perjuicio de la conservación de los Libros, la informatización de los Registros y la expedición de certificaciones por ordenador".

Por último, la *Orden de 30 de noviembre de 1.995 (BOE 21-12-95)* dispuso el inicio de una experiencia piloto de informatización del Registro Civil de Murcia.

De lo anterior, se desprende que la regulación específica del proceso de informatización en el ámbito del Registro Civil se caracteriza por una muy exhigua normativa en la materia, por lo que debemos acudir a otros sectores del ordenamiento jurídico que presentan con el registral civil unas interrelaciones evidentes, aunque no una identidad absoluta.

Como ha quedado expuesto en apartados anteriores los Registros Civiles en España son registros administrativos públicos, cuyo órgano directivo es la *Dirección General de los Registros y del Notariado* del Ministerio de Justicia, que están gestionados por razones históricas por el personal perteneciente a la Administración de Justicia, y cuyo ámbito sectorial dentro del ordenamiento jurídico se enclava dentro del Derecho Civil. Notas todas ellas que sin duda configuran una muy especial situación a la hora de determinar el sector jurídico dentro del cual debemos buscar los principios rectores del proceso informatizador del Registro Civil.

Se debe rechazar la búsqueda de principios generales aplicables en la materia dentro de la normativa específica dictada en el ámbito judicial (*Ley Orgánica 16/1994, de 8 de noviembre*, que modifica la *Ley Orgánica del Poder Judicial*). El *Acuerdo del Consejo General del Poder Judicial de 7 de junio de 1.995 (BOE 13-7-95)*, que desarrolla la referida Ley, aprobó el *Reglamento nº 5, de 7 de junio*, referido a los aspectos accesorios de las actuaciones judiciales, en el cual se regulan los ficheros informatizados donde consten los datos atinentes a actuaciones jurisdiccionales, por una parte, y los ficheros automatizados relativos a las actuaciones en materia de expedientes gubernativos, centrados en las relaciones funcionariales o laborales del personal al servicio de la Administración de Justicia. Parece que quedan fuera de esta normativa los ficheros informatizados en el ámbito del Registro Civil, de forma manifiesta los ficheros que contengan inscripciones registrales y de manera más matizada los ficheros que pudieran contener las actuaciones referidas a los

expedientes tramitados en las oficinas registrales, dado que su naturaleza es ajena a la función jurisdiccional.

Más acorde con la naturaleza propia de los Registros Civiles se presenta la normativa reguladora de la materia dentro de la *Ley 30/1992, de 20 de noviembre (artículo 45.5)* y en el *Real Decreto 263/1996, de 16 de febrero (BOE 29-2-96)*, por el que se regula la utilización de las técnicas electrónicas, informáticas y telemáticas por la Administración General del Estado, norma que desarrolla el referido artículo.

El *artículo 3, apartado d)*, del indicado Real Decreto presenta una definición de *"documento"* como:

"Documento: entidad identificada y estructurada que contiene texto, gráficos, sonidos, imágenes o cualquier otra clase de información que puede ser almacenada, editada, extraida e intercambiada entre sistemas de tratamiento de la información o usuarios como una unidad diferenciada".

Por su parte, el *artículo 4 del Real Decreto*, al abordar las garantías generales para la utilización de soportes, medios y aplicaciones electrónicas, informáticas y telemáticas establece en sus *apartados 2 y 3* los siguientes principios, que se transcriben literalmente dada su importancia:

"2. 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."

"3. 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 la personas autorizadas.

b) La prevención de alteraciones o pérdidas de los datos e informaciones.

c) La protección de los procesos informáticos frente a manipulaciones no autorizadas".

En el *artículo 6, apartado 1 del Real Decreto 263/1996* se aborda la validez de los documentos electrónicos, estableciéndose que:

"Los documentos emitidos por los órganos y entidades del ámbito de la Administración General del Estado y por los particulares en sus relaciones con aquellos, que hayan sido producidos por medios electrónicos, informáticos y telemáticos en soportes de cualquier naturaleza 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 o utros sistemas de identificación."

En relación a las copias y su validez el *apartado 2 del artículo 6* establece que:

"Las copias de documentos originales almacenados por medios o en soportes electrónicos, informáticos o telemáticos, expedidas por los órganos de la Administración General del Estado o por sus entidades vinculadas o dependientes, tendrán la misma validez y eficacia del documeto original siempre que quede garantizada su autenticidad, integridad y conservación."

De los principios anteriormente expuestos se desprende que los documentos electrónicos gozan de plena validez y efectos probatorios siempre que los sistemas técnicos correspondientes garanticen la autenticidad, integridad, identidad del autor y la autenticidad de su voluntad. El sistema deberá garantizar asimismo la confidencialidad del documento y su conservación.

Una vez establecidos los principios anteriores, que deben regir el proceso informatizador en el Registro Civil, en los apartados siguientes se abordan diversas hipótesis de trabajo, examinando si las mismas reúnen las características que hemos definido anteriormente.

4.2. Alcance de la informatización en el ámbito del Registro Civil.

Como ha quedado expuesto anteriormente, la legislación reguladora del proceso de informatización es de una extraordinaria parquedad, lo

que propicia una pluralidad interpretativa sobre el alcance que debe adoptar la referida informatización de los Registros Civiles en España.

El primer problema interpretativo se presenta al tener en consideración que la modificación del *artículo 105* del *Reglamento del Registro Civil* es anterior a la aprobación de la *Ley Orgánica 7/1992,* que introduce en el *artículo 6 de la Ley del Registro Civil* la posibilidad del tratamiento automatizado de las *"inscripciones registrales"*.

Teniendo en consideración que la extensión del *artículo 6 de la Ley del Registro Civil* en esta materia es superior a la regulación contenida en el *artículo 105* del *Reglamento del Registro Civil,* desde un enfoque interpretativo extremo cabría incluso estimar que el referido *artículo 105* del *Reglamento del Registro Civil* habría quedado derogado por la *Ley 7/1992*, posibilitándose incluso la desaparición de los Libros y Folios tradicionales, al quedar sustituidos éstos por los ficheros informáticos.

La anterior interpretación podría verse reforzada si aplicamos en este ámbito las reflexiones que se han venido poniendo de manifiesto en el apartado 3 de este estudio, referidas a la consideración de los *"documentos informáticos"* como documento con efectos probatorios plenos, ya que los asientos serían representaciones plasmadas en signos convencionales, estarían reflejadas en un soporte material, autorizadas por la firma electrónica de los funcionarios responsables y su valor probatorio dependería directamente de la autenticidad y fiabilidad de la que se dotara a los programas informáticos de tratamiento de la información.

No obstante, la hipótesis teórica de trabajo indicada en el párrafo anterior, parece, por su radicalidad, inadecuada y difícil de mantener sin poner en peligro algunos de los cimientos sobre los que tradicionalmente se ha basado el funcionamiento de la institución registral. Pero su mero planteamiento como posibilidad teórica legalmente admisible, ilustra sobre lo que parece una excesiva escasez normativa a la hora de regular una materia cuyos fundamentos básicos

deberían estar abordados desde un nivel de norma legal[20], sin que pueda admitirse una autorización genérica para que la materia se regule por vía reglamentaria.

El proceso interpretativo de la normativa en vigor en la materia debe reconducirse a sus justos límites, estimándose vigente en toda su extensión la redacción del *artículo 105 del Reglamento del Registro Civil*[21], al no vulnerar los contenidos genéricos registrales previstos en la *Ley Orgánica 7/1992*, artículo en el que se establecen dos principios esenciales que van a determinar en buena medida el proceso global de informatización de los Registros Civiles, principios que pueden formularse como: *1. Necesidad de conservar los Libros registrales en soporte tradicional de papel y 2. Posibilidad de expedir certificaciones por ordenador.*

4.3. Fases del proceso de informatización.

4.3.1 Informatización de los Libros Auxiliares.

La informatización de los *Libros Auxiliares* llevados en las oficinas registrales no presenta, en principio, excesivos problemas legales, dado su carácter instrumental, ya que los asientos que se consignan en dichos Libros no poseen el carácter probatorio que se asigna a los asientos obrantes en los Libros Principales y sin que dichos asientos estén directamente destinados a cumplir las exigencias del principio de publicidad, que sí deben ser atendidas por los asientos de los Libros Principales.

Dadas las características de estos *Libros Auxiliares*, su informatización no será objeto de un tratamiento específico en este trabajo, aunque sin duda el proceso merezca una atención particular, si tenemos en consideración su directa repercusión sobre el ámbito de intimidad de las personas, el cual debe quedar plenamente protegido de invasiones indebidas.

■[20] Se defiende la necesidad de que tal nivel legislativo adoptara el rango de Ley Orgánica, al afectar la informatización de los datos personales obrantes en el Registro Civil a la intimidad de las personas (artículo 18,4 C.E.).

■[21] Interpretación, por otra parte, mantenida por la Dirección General de los Registros y del Notariado, y puesta de manifiesto en la Orden de 30 de noviembre de 1.995, que aprobaba la experiencia piloto de informatización del Registro Civil de Murcia.

4.3.2. Informatización de los Libros Principales.

La primera consideración que se debe efectuar consiste en poner de relieve la multitud de matices y posibilidades que caben en la aplicación del proceso informático al ámbito registral, respetándose en todo caso los dos principios antes reseñados y que se reflejan en el *artículo 105 RRC*, así como los principios generales aplicables a los documentos electrónicos, a los que se ha hecho referencia en el *apartado 4.1*.

Seguidamente se plantearán dos hipótesis de trabajo, a las que nos referiremos como **Modalidad A) y Modalidad B)**, examinándose las características que reúnen cada una de las indicadas modalidades propuestas en relación con el valor probatorio de los documentos registrales.

A) MODALIDAD A)

Esta modalidad está dividida en dos subfases, en la primera de las cuales se practicará la inscripción registral y en la segunda se incorporará la imagen del asiento al fichero informático.

a) Práctica de la inscripción registral principal.

El tratamiento informatizado de los Libros Principales debe ser enfocado desde el principio consistente en la *"conservación de los Libros"*, conservación que se debe entender como la conservación del soporte material en papel tradicional. Ahora bien, los Libros pueden consistir materialmente en *"Libros"* integrados por *"hojas fijas"*, o formarse por la posterior encuadernación de *"hojas móviles"* foliadas y selladas, en las que previamente se hayan hecho constar los asientos correspondientes, según preceptúa el *artículo 105 RRC*[22].

■[22] Parte de los Libros del Registro Civil Central se forman por hojas móviles, donde constan los asientos registrales practicados por los Consulados de España en paises extranjeros, debidamente foliados, sellados y firmados, los cuales son posteriormente encuadernados (Real Decreto 2721/1979, de 5 de ocubre,BOE 3-12-79, sobre los Libros del Registro Civil Central).

La primera aplicación del proceso de informatización puede partir, en buena lógica, de la realización del asiento registral mediante la aplicación del oportuno programa informático creado al efecto, lo que repercutiría de forma directa en la claridad de los datos plasmados en el asiento, problema éste que, pese a su obviedad, no debe ser despreciado.

Una vez confeccionado el documento, la necesidad de mantener la inscripción en soporte papel exige que el documento producido informáticamente sea generado por impresora en el papel, con el formato y las características que reglamentariamente deban determinarse.

Una vez que el asiento haya sido producido en papel, el documento deberá ser debidamente autorizado por el Encargado y Secretario competentes, con sus firmas plasmadas de manera manuscrita. Posteriormente, el documento así generado y firmado deberá ser incorporado a *"Libros carpetas"*, *"Libros encuadernados"* tradicionales o *"Libros encuadernados"* en formatos nuevos que faciliten la plasmación de asientos marginales, vía impresión mecánica, que se practiquen con posterioridad.

Hasta el momento el proceso informatizador propuesto solamente ha intervenido para llevar a cabo la confección y generación del documento, manteniéndose, por otra parte, todas las características tradicionales que la Ley y el Reglamento del Registro Civil asignan a los Libros Principales, incluida la firma manuscrita de los funcionarios autorizantes del asiento y del declarante, en su caso, respetándose escrupulosamente el principio de conservación de los Libros en su soporte material de papel.

b) Incorporación de asientos a ficheros informáticos.

El segundo principio que preside el proceso de informatización consiste en la posibilidad de *"expedición de certificaciones por ordenador"*. No define el artículo *105 RRC* si esta expedición debe quedar reducida a certificaciones en extracto o extenderse a la expedición de certificaciones literales. No obstante, se debe tener en consideración que la informatización íntegra de los asientos permitiría a su vez la expedición de certificaciones tanto en extracto como literales. Por tanto, vamos a contemplar la hipótesis de trabajo que permita la completa e íntegra incorporación de los asientos a ficheros informatizados.

Antes de concretar un sistema informático que permita la expedición de certificaciones mediante ordenador, conviene efectuar unas reflexiones previas sobre la naturaleza y características que debe adoptar un fichero informático del cual se van a expedir directamente certificaciones con valor de documento público, del que se va a predicar todo el valor probatorio propio de tales documentos.

En primer lugar, la aplicación informática que permita el almacenamiento de los documentos correspondientes debe garantizar la integridad del documento, sin que sea posible su modificación al margen de los procedimientos legalmente previstos.

La segunda nota a tener en consideración viene constituida por la necesidad de que exista una identidad plena entre los asientos obrantes en los Libros Principales en soporte de papel y los asientos grabados en el soporte informático.

En tercer lugar, se debe indicar que si desde el fichero informático se van a poder expedir certificaciones, lógicamente el asiento incorporado al soporte informático debe revestir completas garantías de legalidad y procedencia, lo que sólamente se logra si el asiento se encuentra autorizado con la firma del Encargado y Secretario competentes.

Antes de plantear un sistema apropiado que reúna todas las características anteriores, sería oportuno contemplar la práctica habitual de las oficinas registrales, ya que el éxito del proceso informatizador no puede estar ajeno al funcionamiento diario en el seno de los Registros Civiles, donde en no pocas ocasiones el extraordinario volumen de asientos y certificaciones que deben ser practicados y expedidas impediría un minucioso control de identidad de todos y cada uno de los datos que se incorporasen al soporte informático con respecto a los obrantes en los Libros en soporte de papel. El banco informático con los datos incorporados deberá garantizar plenamente los datos de los que posteriormente se dará publicidad mediante la expedición de la correspondiente certificación.

Por otra parte, si la expedición de certificaciones por ordenador obligase a confrontar los datos de las certificaciones generadas por ordenador con los datos de los Libros Principales en soporte de papel no se habría ganado en la necesaria agilidad perseguida con la informatización.

Las notas anteriormente definidas y las necesidades de funcionamiento interno citadas creemos que quedarían garantizadas con la incorporación al fichero informático de *"la imagen del folio registral"*, elaborado conforme se ha indicado en punto a) anterior, debidamente autorizado con la firma del personal competente, incorporación que los actuales medios técnicos posibilitan en el momento presente.

Una vez planteado el sistema anterior de incorporación de las imágenes de los asientos al fichero informático, se deben definir determinadas características que revistan al proceso de la necesaria fiabilidad y garantía.

En primer término, los sistemas habituales normalizados de incorporación de imágenes a soportes informáticos no reconocen, sin más, documentos originales de aquellos que cabría calificar como copias, ni distingue los documentos originales de los irregularmente modificados. Bastaría por tanto incorporar un asiento literal firmado a un procesador de textos *"standar"*, para posteriormente modificarlo a voluntad e incorporarlo al fichero informatizado desde donde se van a expedir de forma directa las certificaciones. Con ello quedarían vulneradas todas las garantías registrales que deben acompañar a los documentos del Registro Civil, aunque obviamente requeriría la concurrencia de una acción delictiva llevada a cabo, en la mayoría de los supuestos, por funcionario al servicio de la Administración, posibilidad que, por tanto, debe ser contemplada con carácter excepcional.

No obstante, a fin de evitar el problema expuesto en el párrafo anterior deben entrar aquí en aplicación todos los medios técnicos expuestos en el apartado 3 de este estudio, en relación con la firma digital. El programa informático que se elabore deberá, como paso previo a cualquier incorporación de imágenes al fichero informático, proceder al reconocimiento de la firma plasmada en el documento original. Dicho reconocimiento informático no sólamente debe extenderse a la consideración de los rasgos físicos de la escritura, sino a los caracteres biométricos de la misma, es decir, al reconocimiento dinámico de la firma consistente en comparaciones sucesivas de la firma manuscrita del documento con un modelo de referencia radicado en el sistema informático,

comparación llevada a cabo según diferentes criterios (velocidad de escritura, presión de la mano, rasgos etc)[23].

El proceso anterior puede ser completado con el reconocimiento de materiales o marcas específicas contenidas en el folio registral, antes de la incorporación de su imagen. Por último la tarea mecánica del reconocimiento de autenticidad podrá quedar asimismo garantizada con el reconocimiento previo del documento cuya imagen se deba incorporar al fichero informático llevada a cabo por el funcionario competente, lo que garantizará, más aún si cabe, la autenticidad del documento incorporado.

c) Práctica de asientos marginales.

Dentro de esta modalidad, la práctica de asientos marginales en el folio registral principal, su firma manuscrita y su posterior incorporación al fichero informático no debería representar especiales problemas técnicos ni jurídicos, ya que una vez practicado el asiento marginal en el soporte informático, éste debería ser plasmado en el folio registral principal generado en papel correspondiente, vía impresión gráfica, y posteriormente firmado por los funcionarios responsables, siendo incorporada la nueva imagen del folio completo al fichero informático, debiendo tal incorporación de la nueva imagen al fichero automatizado anular e inutilizar la imagen precedente donde no constaba el asiento marginal practicado.

En la medida en que los medios técnicos informáticos consigan garantizar la autenticidad del documento incorporado al fichero informático desde donde se van a expedir las certificaciones correspondientes se estará cumpliendo el requisito necesario para la admisibilidad del sistema, del cual derivaremos el valor probatorio de los certificados emitidos.

En resumen, esta modalidad estará constituida por los siguientes pasos: práctica del asiento mediante ordenador, impresión en papel del asiento practicado, firma manuscrita del asiento, incorporación del folio registral al Libro

■[23] Amory, B y Thunis, X., "Dématérialisation, authentification et responsabilité, le droit continental, les trasactions internationales assistées par ordinateur", **Litec**, 1987, págs. 71 y siguientes.

correspondiente y, por último, incorporación de la imagen del folio registral al banco de datos informático, desde donde se procederá a la expedición de certificaciones.

B) MODALIDAD B).

a) Práctica de la inscripción principal.

Una segunda hipótesis de trabajo es la representada por el sistema según el cual la aplicación informática permitiría la práctica del asiento correspondiente, el cual sería posteriormente firmado por el Encargado y el Secretario competentes, mediante firma electrónica digital, utilizando los códigos restringidos en exclusiva a sus titulares. Dicha firma digital podría conllevar incluso la generación del correspondiente grafismo.

Una vez extendida la firma digital por parte de los funcionarios titulares de las mismas, el asiento debe quedar sin posibilidad de ser posteriormente modificado o alterado en parte alguna de su contenido, por lo que su integridad se garantiza plenamente.

El primer aparente problema a considerar en esta modalidad viene representado por el valor probatorio que la legislación registral atribuya a la firma digital. Deben reproducirse aquí todas las consideraciones realizadas anteriormente sobre la plena admisión probatoria de la firma electrónica, la cual viene siendo admitida con plenos efectos en determinados sectores del mundo jurídico, por disposiciones parciales y fraccionadas que regulan los mismos. Aunque interpretando de forma adecuada la legislación vigente en la materia registral cabría la aceptación de la firma digital con plena eficacia probatoria, sin duda generaría menos conflictos interpretativos la aceptación normativa expresa del valor probatorio de la firma plasmada de forma digital, reconocimiento llevado a cabo de manera genérica en el ordenamiento jurídico español o, en su defecto, introducido en la normativa registral civil[24].

■[24] El proyecto de nueva Ley de las Telecomunicaciones, actualmente en fase de discusión parlamentaria, modifica la normativa precedente en diversos aspectos, entre los que cabe citar el reconocimiento general de la firma electrónica. No obstante habrá que estar a la formulación definitiva que adopte el precepto en la redacción final de la Ley.

b) Generación del documento en soporte papel.

Posteriormente, el asiento deberá ser generado en papel, por vía de impresora, e incorporado al correspondiente Libro de hojas móviles. El documento plasmado vía impresora en papel puede incluso contener el grafismo de la firma de los funcionarios que lo hayan suscrito, grafismo generado al poner en aplicación el código secreto de sus titulares.

c) Asientos marginales.

Un importante aspecto a considerar dentro de esta modalidad B) es el surgido de la imposibilidad de modificar el asiento registral, una vez plasmada la firma electrónica de los funcionarios que lo autorizan, cuando los asientos obrantes en el Registro Civil deben reflajar los cambios y modificaciones producidos en el estado civil de los interesados a lo largo de su existencia, modificaciones que, por extenderse de forma sobrevenida a la práctica del asiento principal, se hacen constar en la actualidad de forma marginal al indicado asiento principal.

No parece excesivamente complejo salvar el obstáculo mencionado, ya que la firma electrónica debe *"blindar"* el espacio ocupado por los asientos una vez firmados, quedando los otros sectores no utilizados del folio registral perfectamente hábiles para hacer constar los sucesos sobrevenidos que alteren o afecten de alguna forma el estado civil del inscrito.

Una vez practicado el correspondiente asiento marginal de forma informática en el asiento obrante en el fichero automatizado, éste deberá ser asimismo firmado por los funcionarios responsables, mediante la utilización de su firma digital.

Por último, el sistema de impresión informática posibilitará la práctica del asiento marginal correspondiente en el propio Folio registral, ya incorporado al Libro de la pertinente Sección, evitándose de esta manera la existencia de *"Hojas móviles"* no encuadernadas (no siempre fáciles de controlar en las grandes macrounidades administrativas) y evitándose asimismo la existencia de dos documentos, folios y hojas complementarias, una con el asiento principal y la otra con el asiento principal más los asientos marginales que se hubieran practicado.

Entre los inconvenientes, más práctico que teórico, que plantea esta modalidad de actuación (modalidad B) cabe mencionar la firma que debe plasmar en el asiento el declarante del hecho que se inscribe, firma que obviamente no podrá ser digital e informatizada, sino plasmada de forma manuscrita en el documento, una vez generado en papel. Con independencia de los usos prácticos que se adoptaran para cumplimentar este requisito, cabría plantear la conveniencia de suprimir el mismo, ya que la firma del declarante siempre queda recogida y plasmada en la documentación necesaria que fundamenta la calificación registral previa que posibilita la práctica del asiento.

En resumen, esta segunda modalidad, que a efectos de identificación hemos designado como Modalidad B), estaría constituida por las fases siguientes: práctica del asiento mediante ordenador, plasmación de la firma digital de los funcionarios autorizantes, impresión del asiento en papel e incorporación del folio registral al Libro correspondiente. Las certificaciones serán expedidas de forma directa desde el banco informático de asientos registrales.

4.3.3. Informatización de legajos y documentos.

La práctica de una inscripción o anotación registral debe ir siempre precedida de la calificación previa de la documentación en la cual se fundamenta el asiento, efectuada por parte del Encargado del Registro.

En el presente estudio no se aborda la problemática referida a la informatización de los indicados documentos, si bien los mismos también son susceptibles de erigirse en objeto de certificación por parte de los funcionarios registrales habilitados al efecto.

La informatización de los documentos o datos contenidos en los mismos no parece revestir una especial problemática jurídica, dado que tales ficheros no estarían propiamente destinados a servir de vehículo para la publicidad registral, que constituye el objeto propio de la institución, si bien se debe poner un especial énfasis en la protección de la intimidad de las personas cuyos datos personales pudieran quedar incluidos en los bancos de datos creados a este fin, extremo al que se ha aludido anteriormente.

4.4. Valor probatorio de las certificaciones emitidas mediante los sistemas propuestos.

Los sistemas anteriormente expuestos deben ser examinados desde un enfoque jurídico, con el fin de determinar si los mismos reúnen todas las características que la legislación registral vigente atribuye a los documentos en el ámbito del Registro Civil, de donde derivaremos el valor probatorio de los documentos emitidos mediante sistemas informáticos.

Se procede a continuación a realizar un examen del valor probatorio documental de las certificaciones que fueran emitidas según las modalidades propuestas.

4.4.1 MODALIDAD A).

En primer término se aprecia que el sistema de informatización propuesto en esta modalidad no supone una ruptura con relación a las prácticas registrales habituales, ya que se sigue manteniendo el soporte de los asientos en papel, la firma manuscrita que autoriza y autentifica los asientos *(Encargado, Secretario y declarante)* y un único folio principal registral, lo que permite la práctica de asientos marginales posteriores y evita la incorporación de hojas complementarias.

Se deben examinar brevemente las características fundamentales del sistema a fin de comprobar su validez de donde derivaremos el valor probatorio de los documentos que se emitan mediante el mismo.

a) Integridad documental.

El fichero que contenga la imagen del documento original, de donde serán expedidas las certificaciones, debe ser inhábil para modificar el contenido del documento, reuniendo exclusivamente las características necesarias que permitan el almacenamiento de imágenes y su recuperación, ya que en otro caso el sistema quedaría invalidado en inicio, al poder ser violadas todas las garantías procedimentales necesarias para la modificación de asientos.

b) Identidad documental de asientos.

El almacenamiento de la imagen garantiza la identidad de los datos que obran en el asiento almacenado, con los datos del folio obrante en el Libro Principal, puesto que se trata de la misma imagen.

En este punto podría presentarse el problema práctico de discrepancia de datos entre el Libro Principal en soporte de papel y la imagen almacenada en ordenador, si por descuido o error el folio registral original o modificado mediante asiento marginal no fuera incorporado al fichero informático. No obstante, el problema puede ser minimizado si los asientos del folio en papel son debidamente diligenciados con la constancia de la pertinente incorporación de imagen al fichero informático.

c) Autenticidad documental y firmas autorizantes del asiento.

La imagen que quedara incorporada al fichero informático incluiría las firmas del Encargado y el Secretario que autorizasen los asientos, así como la firma del declarante, si el asiento se practica en virtud de declaración. Con ello quedan al margen los problemas teóricos planteados por algunos sectores doctrinales, sobre los que ya se ha tratado en el apartado 3 de este estudio, en relación con la firma electrónica, según los cuales la firma electrónica no cumple plenamente las características necesarias que se atribuyen a la firma manuscrita, como son: 1. Signo distintivo personal, 2. Acto volitivo del firmante (*animus signandi*), 3. Identificación (que asegura la relación jurídica entre el acto firmado y el firmante) y 4. Autentificación, mediante el cual el firmante expresa su consentimiento sobre el acto jurídico firmado.

Como ya se ha expuesto en el punto c) precedente, la posibilidad de vulnerar la firma del asiento, mediante la manipulación posterior de la imagen incorporada al fichero informático, al margen del procedimiento legalmente previsto, queda como una hipótesis delictiva incluso más difícil de llevar a cabo que con el sistema de funcionamiento registral actualmente en vigor.

d) Acceso.

El acceso a los datos obrantes en el Registro Civil es una nota derivada de la naturaleza propia de este tipo de Registros públicos, destinados a servir de vehículo de publicidad, en este caso referida al estado civil de las personas.

Cualquier sistema de informatización de los datos del Registro Civil en ficheros informatizados debería tener una especial consideración a la protección de la intimidad de las personas, cuyos datos personales se verán incluidos en los ficheros correspondientes.

Se plantean en este punto problemas de extraordinaria importancia en relación con la posible colisión de derechos constitucionales implicados en este ámbito, como son por una parte el derecho al respeto de la intimidad personal y familiar de las personas *(artículo 18,4 C.E.)* en relación con la utiliación de medios informáticos, y por otro lado, el reconocimiento del derecho de acceso a los registros públicos a fin de obtener la información en ellos contenida *(artículo 105,b) C.E.)* y el derecho reconocido en el *artículo 20, 1 d)* a recibir y comunicar libremente la información, preceptos que puestos en relación conjuntamente con la infomatización de datos personales obrantes en los Registros Civiles podrían llegar a generar lo que algunos autores han denominado el *"mercado secundario de datos"*. Queda meramente planteado este problema, cuya resolución sin duda deberá ser abordada de forma más detenida en otro ámbito[25]. Se debe hacer constar aquí únicamente que la futura informatización de los Registros Civiles en España en forma alguna debiera suponer un ataque a la intimidad personal y familiar de los ciudadanos, por lo que se hace necesario acometer el proceso con una suficiente cobertura normativa que garantice plenamente los derechos reconocidos en nuestra Constitución.

■[25] La hipótesis anterior fue planteada por el Prof. Tomás de la Cuadra Salcedo en la ponencia expuesta en el XI Encuentro sobre Informática y Derecho, celebrado en Madrid, en el mes de abril de 1.997 por el Instituto de Informática Jurídica de la U.P.C.M.

e) Conservación.

Al igual que la nota anterior, cualquier sistema informático que pudiera implantarse en el campo registral debería contemplar de manera especial el problema de la conservación de los soportes, cuyo deterioro se produce con el paso del tiempo.

En el mundo informático la vida media de los soportes utilizados es variable según las condiciones ambientales y el sistema elegido. Se puede afirmar que los sistemas que mantienen una más alta perduración son los basados en soportes de discos ópticos, con unas previsiones de vida media que pueden oscilar entre los 30 y 40 años.

El punto anterior posee una especial trascendencia si tenemos en consideración que según preceptúa el artículo *102 del RRC.* serán remitidos al Archivo Provincial los Libros de Inscripciones cuando hayan transcurrido cincuenta años desde la práctica de las inscripciones principales de defunción y ciento veinticinco años en el resto de inscripciones, lapso de tiempo que supera con mucho la vida media prevista en los soportes informáticos. No obstante, los avances técnicos en la materia permiten razonablemente prever avances significativos en este punto.

4.4.2 MODALIDAD B).

El sistema planteado como Modalidad B) respeta, al igual que el sistema anterior, en su integridad los principios recogidos en el *artículo 105 RRC.* en relación con la conservación de los Libros en su soporte de papel y la posibilidad de expedir certificaciones por ordenador.

A continuación se examinan igualmente las notas características de las que vamos a derivar la capacidad del sistema para expedir certificaciones con pleno valor probatorio.

a) Integridad documental.

Como se ha expuesto, una vez que los funcionarios acreditados han plasmado su firma digital en el soporte informático, la inscripción queda protegida contra cualquier eventual modificación posterior, de donde se infiere

que la integridad del documento queda plenamente garantizada con este procedimiento, sin perjuicio de que marginalmente se puedan practicar los asientos a que hubiere lugar para reflejar las incidencias sobrevenidas en el estado civil del inscrito.

b) Identidad documental del asiento.

Una vez practicado el asiento y plasmadas las firmas correspondientes, el sistema debe generar automáticamente el asiento en soporte de papel, con lo que se mantiene la identidad entre el asiento que figura en el soporte informático y el asiento obrante en el soporte de papel.

Podría plantearse la eventualidad según la cual el asiento marginal practicado en el soporte informático no fuera plasmado en el folio correspondiente en papel, de donde se derivaría una discrepancia entre ambos soportes. El problema podría ser fácilmente solventado si el sistema informático bloqueara la posible expedición de cualquier certificación si antes el mismo no hubiera registrado la plasmación del asiento marginal en el folio registral en papel.

La identidad de los asientos entre ambos soportes, informático y en papel, parece quedar sobradamente cumplida con el sistema propuesto.

c) Autenticidad documental y firmas autorizantes.

En repetidas ocasiones a lo largo de este estudio se ha aludido a la firma electrónica digital como medio hábil para sustituir a la firma manuscrita de los documentos, por lo que se dan aquí por reproducidas las consideraciones realizadas anteriormente en la materia.

La firma digital se constituye en un medio especialmente cualificado para impedir la modificación indebida de los asientos, una vez plasmada la misma, ya que puede originar la imposibilidad de modificar el asiento[26].

■[26] Dávila Muro, Jorge y otros, "Control gubernamental en la protección de datos: proyecto Clipper", **X Años de Encuentros sobre Informática y Derecho,** Pamplona: Aranzadi, 1.997, págs. 25-51.

Procede en este punto llevar a cabo una breve reflexión acerca de la posible transmisión de los códigos secretos generadores de la firma digital por parte del ordenador. Dichos códigos deberían ser conocidos de forma exclusiva por parte de los funcionarios titulares de los mismos, evitándose cualquier transmisión indebida de los mismos, lo que, en cualquier caso, debería hacer incurrir al funcionario en grave responsabilidad.

Por último se debe tener en consideración que la plasmación de la firma digital debe generar al propio tiempo el grafismo correspondiente de la firma del funcionario titular, lo que, en conjunción con el código, posibilitará la legalización o autentificación de firmas si ello fuera preciso.

Entendemos que la firma digital garantiza la identidad del firmante, así como la autenticidad de su voluntad de firmar el documento en cuestión, por lo que los reparos planteados al respecto por algunos sectores doctrinales deberían quedar superados[27].

d) Acceso.

En relación con el acceso a los ficheros informatizados se deben repetir aquí las consideraciones que ya se han realizado anteriormente, con referencia al posible acceso a los ficheros informatizados únicamente del personal autorizado, impidiéndose la generación de posibles *"mercados secundarios"* que funcionasen con la información contenida en los bancos de datos generados en las oficinas registrales, lo que sin duda constituiría una agresión al respeto a la intimidad de las personas que el Registro debe mantener, no sólo con respecto a las inscripciones cuya publicidad está restringida, sino a aquellas inscripciones de libre publicidad.

e) Conservación.

La conservación de los datos registrados en el soporte informático debe quedar garantizada, no solamente contra el paso del tiempo, mediante la necesaria actualización de soportes, sino también y de forma

[27] Gallardo Ortíz, Miguel, "Criptografía, Seguridad Informática y Derecho. Leyes del Ciberespacio", **en Informática y Derecho, nº 4**, 1.994, págs. 473 y siguientes.

primordial contra posibles ataques provinientes de los conocidos como *"virus informáticos"* o *"bombas lógicas"*, lo que sin duda podría originar perjuicios de difícil reparación.

Entra en juego en este punto la necesidad de realizar periódicamente las precisas copias de seguridad, extremo éste que queda aquí meramente planteado, dada la implicación que la realización de dichas copias tiene en relación con el eventual tráfico de información que pudiera llevarse a cabo con las mismas y la posible violación del derecho a la intimidad de los afectados.

4.5. Naturaleza jurídica del fichero informático en relación con los asientos en soporte papel.

Según se desprende del *artículo 105 RRC* la informatización de las inscripciones del Registro Civil conlleva la existencia de dos soportes distintos, uno tradicional conteniendo los asientos en papel y el otro informático. Las dos Modalidades A) y B) antes planteadas como hipótesis de trabajo contemplan la existencia de ambos soportes. Se presenta en este momento la cuestión de dilucidar la naturaleza de cada soporte en cada una de las modalidades propuestas, ya que a pesar de que los sistemas técnicos puedan reducir a su mínima expresión las discrepancias entre ambos soportes, cabe plantear, al menos en teoría, la posible existencia de discrepancias entre un mismo folio reflejado en uno y otro soporte, debidas bien a que la imagen del asiento no se ha incorporado al soporte informático (Modalidad A) o bien a que el asiento firmado electrónicamente no haya sido generado en papel o plasmado en el folio correspondiente en papel (Modalidad B).

Entendemos que las eventuales discrepancias que pudieran producirse entre los dos soportes de las inscripciones deben resolverse en favor de aquel soporte que contuviera la firma original de los funcionarios autorizantes del asiento, ya que sería precisamente tal asiento el que debería tener la consideración de *"matriz"* del cual derivaría la inscripción o asiento en el segundo soporte.

Según lo anterior, en la modalidad que hemos denominado A), el asiento conteniendo las firmas de los funcionarios que lo autorizan es el que se encuentra plasmado en soporte de papel, ya que en el soporte informático simplemente se ha recogido la imagen de dicho folio registral debidamente

autorizado. Por tanto, en este sistema propuesto el soporte que recoge el asiento en papel se erige como *"matriz"*, que resolverá cualquier discrepancia observada con el mismo en la imagen plasmada en el soporte informático.

Por el contrario, en la Modalidad B) las firmas de los funcionarios autorizantes del asiento se plasman de manera digital en ordenador, por lo que en este supuesto el asiento *"matriz"* sería el grabado en el ordenador, del cual posteriormente se debe generar el oportuno asiento en papel. La inscripción (anotación) informática se constituye, por tanto, en el asiento determinante para resolver cualquier discrepancia que pudiera surgir entre los soportes.

La solución propuesta se fundamenta en el mismo criterio seguido por el *Código Civil (artículo 1.220 y siguientes)* y la *Ley de Enjuiciamiento Civil (artículos 597 y siguientes)* a la hora de determinar el valor probatorio de las *"copias"* si éstas discrepan del documento original *"matriz"* con el cual se deban confrontar.

5°). Conclusiones.

Seguidamente se exponen someramente las conclusiones derivadas del estudio precedente:

1ª) La doctrina y jurisprudencia tradicionales que consideraban como *"documento"* únicamente al instrumento *"escrito"* en soporte de papel, va siendo progresivamente sustituida por una visión *"representativa"* del instrumento documental, según la cual se considera como *"documento"* a toda representación, plasmada sobre cualquier tipo de soporte, mediante la utilización de sistemas convencionales de signos, y cuyo valor probatorio derivará de la garantía existente en cada caso en relación con la integridad y autenticidad del documento, así como la autoría y los signatarios del mismo.

2ª) Las más recientes direcciones legislativas, jurisprudenciales y doctrinales admiten, si bien de manera sectorial, esta nueva visión del *"instrumento documental"*, dentro de cuyo ámbito se encuentra el *"documento electrónico, informático y telemático"*.

3°) El documento electrónico y en particular el documento informático goza de similares cualidades que cualquier otro tipo de documento tradicional en soporte de papel, por lo que su valor probatorio deberá tener el

mismo tratamiento que el asignado por la legislación vigente a los documentos públicos y privados. La equiparación entre el documento tradicional en papel y el documento informático, en cuanto a su valor probatorio, se desprende al examinar las características siguientes: soporte material, su componente representativo, los signos convencionales utilizados, la firma autorizante, la integridad, la autenticidad y la conservación del documento.

4º) El Registro Civil se caracteriza por estar destinado a dar publicidad a la sociedad sobre el estado civil de los ciudadanos. Su naturaleza se encuentra dentro del ámbito del Derecho Civil y sus inscripciones y certificaciones son consideradas como documentos públicos que predican la *"verdad oficial"* sobre el estado civil de las personas. Los *Libros Principales y Auxiliares* del Registro Civil, así como la práctica registral de asientos se fundamenta en los conceptos tradicionales de *"documento en papel"* autorizado por la firma manuscrita de los funcionarios competentes, conceptos éstos extensibles a las certificaciones que se utilizan como medio fundamental de hacer efectiva la publicidad registral para la que estos Registros han sido creados. Por tanto, los documentos en el ámbito del Registro Civil se caracterizan por las notas distintivas expuestas.

5º) La normativa dictada en relación a la informatización de los Registros Civiles en España es muy escasa y se caracteriza por una extraordinaria concisión. De dicha normativa se desprende que el proceso de informatización en el Registro Civil deberá respetar dos principios básicos: *1º Mantenimiento de los asientos en soporte de papel y 2º Posibilidad de expedir certificaciones por ordenador.* No obstante los dos principios citados podrían ser obtenidos de multiples formas, por lo que se debe recurrir a otros sectores del ordenamiento jurídico para extraer los principios rectores de donde se puedan derivar las características que deben reunir los documentos informáticos en el ámbito del Registro Civil. Entre la normativa de donde podamos extraer los principios necesarios a aplicar presenta un interés especial la *Ley 30/1992, de 26 de noviembre, y el Real Decreto 263/1996, de 16 de febrero*, que regula la utilización de técnicas electrónicas, informáticas y telemáticas por la Administración General del Estado.

6º) El proceso general de informatización del Registro Civil en España puede contemplarse dividido en tres fases: informatización de legajos y documentos, informatización de los *Libros Auxiliares* e informatización de los *Libros Principales* y emisión de certificaciones. La informatización de los *Libros Principales* y su íntima relación con la expedición de certificaciones es la que se

aborda con mayor detalle en este estudio, planteándose dos hipótesis de trabajo, a las que se alude como Modalidad A) y Modalidad B).

7º) La Modalidad A) consiste en la práctica del asiento principal mediante ordenador, impresión en papel del asiento practicado, firma manuscrita del asiento e incorporación del folio al Libro correspondiente. Posteriormente la imagen del asiento será incorporada a un banco de datos informático, previo reconocimiento de los caracteres gráficos y biométricos de las firmas del folio registral. De igual forma, los asientos marginales se elaborarán en ordenador y serán plasmados marginalmente en el mismo folio registral donde conste la inscripción principal. Posteriormente serán debidamente firmados de forma manuscrita, incorporándose la imagen al banco de datos, previo reconocimiento informático biométrico de firmas, incorporación que anulará el asiento que previamente se encontrara en el banco de datos informatizado. Las certificaciones, ya sean literales o en extracto, se expedirán directamente mediante ordenador, teniendo como base los asientos obrantes en el fichero informatizado.

8º) La hipótesis de trabajo que hemos denominado Modalidad B) consiste en la práctica del asiento principal mediante ordenador, la plasmación de la firma digital de los funcionarios autorizantes del asiento, lo que *"blindará"* el mismo, impidiendo su modificación. Posteriormente el asiento será generado en papel e incorporado a su Libro correspondiente. La práctica de inscripciones marginales se llevará a cabo igualmente en ordenador, donde conste el correspondiente folio principal, el cual será debidamente firmado de manera digital, plasmándose posteriormente el asiento marginal en el folio registral en papel donde constase el asiento principal. Las certificaciones tanto literales como en extracto se expedirán por ordenador, teniendo como base el fichero informático.

9º) Al exigir la normativa registral la existencia de dos soportes conteniendo los asientos, uno en papel y otro en soporte informático, se presenta el problema de determinar la naturaleza y relaciones existentes entre ambos soportes, a fin de determinar su prioridad a la hora de dilucidar posibles discrepancias que pudieran presentarse entre los mismos. Siguiendo los principios derivados del *Código Civil*, la *Ley de Enjuiciamiento Civil* y la propia normativa registral, a la hora de determinar las relaciones entre los documentos originales y sus copias, debe tener prioridad en este caso el asiento *"matriz"* de donde deriva el segundo asiento. En la Modalidad A) el asiento *"matriz"* es el constituido por el

que consta firmado en papel de forma manuscrita y en la Modalidad B) el asiento *"matriz"* es el firmado de manera digital en ordenador.

10°) El valor probatorio de los documentos producidos mediante los dos sistemas propuestos reúnen todos los requisitos que tanto la legislación registral civil, como la legislación derivada del resto del ordenamiento jurídico aplicable en la materia, exigen para dotar a los *"documentos"* del valor probatorio necesario para servir la finalidad que nuestro ordenamiento jurídico asigna a los documentos del Registro Civil, a los que considera dentro de la categoría de *"documentos públicos"*. Dicha conclusión se obtiene tras examinar en cada una de las dos modalidades las siguientes características: *a)* integridad documental, *b)* identidad documental entre los soportes utilizados *c)* autenticidad y firma del documento, *d)* el acceso al documento y *e)* la conservación del documento. A las notas anteriores se debe agregar el examen llevado a cabo sobre las características que propiciaban la consideración del documento electrónico e informático como documento con pleno valor probatorio.

11°) Finalmente se debe poner de relieve la extraordinaria parquedad normativa a la hora de regular una materia como es la referida a la informatización de los Registros Civiles en España, que sin duda afectará al ejercicio de derechos constitucionalmente reconocidos. El proceso de informatización de ningún modo puede suponer una amenaza a tales derechos de los ciudadanos, por lo que se hace necesario revestir a dicho proceso de la cobertura legal y reglamentaria precisa para evitar improvisaciones o desviaciones que pudieran ensombrecer lo que en el momento presente es sentido como una creciente demanda social.

BIBLIOGRAFIA

- *Albadalejo, Manuel*, **Derecho Civil I: Introducción y parte general, Volumen Primero: Introducción y Derecho de las personas**, Barcelona: Bosch, 1.995.

- *Ballesteros Sastre, Fátima* y otros, "Gestión, Tratamiento y Difusión de la Documentación en las Administraciones Públicas", **IV Jornadas Españolas de Documentación Automatizada, Documat 94,** 1.994: Universidad de Oviedo.

- *Caballero Gea, José Alfredo*, **Ley, Reglamento y Expedientes de Registro Civil,** Pamplona: Aranzadi 1.993, 3ª Ed.

- *Cabello de los Cobos y Mancha, Luís Mª*, "Precedentes históricos de la publicidad registral: Adición II", **Boletín del Colegio Nacional de Registradores, nº 11, págs. 264-268.**

- *Cabello de los Cobos y Mancha, Luís Mª*, "Precedentes históricos de la publicidad registral: Adición IV", **Boletín del Colegio Nacional de Registradores, nº 13,** 1.996, págs. 818-828.

- *Carrascosa López, Valentín y otros*, "Derecho de la Prueba y la Informática:problemática y perspectivas", **Informática y Derecho, nº 2,** 1.991.

- *Carrascosa López, Valentín*, "Valor probatorio del documento electrónico", **Informática y Derecho, nº 8,** 1.995, págs. 133-173.

- *Chamoux, F*, "Valor probatorio de los modernos soportes de la información", **Documentación Administrativa, nº 0199,** 1983, págs. 133-173.

- *Davara Rodríguez, Miguel Angel*, **Derecho Informático,** Pamplona: Aranzadi, 1.993.

- *Davara Rodríguez, Miguel Angel*, "El documento electrónico en la vigente Ley de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común", **Revista de Administración Pública, nº 131,** 1993, págs. 455-491.

- *Dávila Muro, Jorge y otros*, "Control gubernamental en la protección de datos: proyecto Clipper", **en X Años de Encuentros sobre Informática y Derecho,** Pamplona: Aranzadi, 1.997, págs. 25-51).

- *Díaz Fraile, Juan Mª*, "La aplicación del Derecho Comunitario en el ámbito registral y notarial: nuevas perspectivas", **Noticias CEE, nº 103-104,** págs. 53-64.

- *Elmazaz Molina, Andrés*, "La Ley 30/92, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común y las Nuevas Tecnologías", **IV Jornadas de Documentación Automatizada, Documat 94**, 1.994, Universidad de Oviedo.

- *Elías Baturones, Julio José*, "La Jurisprudencia ante el documento electrónico. Su aceptación como prueba documental", **Tapia, octubre-noviembre 1.996**, págs. 65-73.

- *Fernando Pablos, Marcos Matías*, " Administración Pública, Informática y ciudadano: perspectiva general", **Informática y Derecho, nº 4,** 1.994, págs. 109 y siguientes.

- *Gallardo Ortíz, Miguel*, "Criptología; Seguridad Informática y Derecho. Leyes del Ciberespacio", **Informática y Derecho, nº 4,** 1.994, págs. 473-479.

- *Gimeno Goméz-Lafuente, Juan Luís*, "Incidencia del Derecho Comunitario en el Derecho Registral", **Revista Crítica de Derecho Inmobiliario, nº 64**, 1.988, págs.31-48.

- *Gómez Fernandez-Cabrera, Jesús*, "Gestión Automatizada de la Información y Documentación en la Administración", **V Jornadas Españolas de Documentación Automatizada, Documat 95,** 1.995: Cáceres.

- *González Aguilar, Audilio*, "EDI: Desafío de una nueva práctica",**Informática y Derecho, nº 4,** 1994, págs.555-567.

- *Gutierrez Francés, María Luz*, "El intrusismo informático (Hacking): ¿Represión penal autónoma?, **Informática y Derecho, nº 12-15**, 1.996, págs. 1.163 y siguientes.

- *Luces Gil, Francisco,* **Derecho Registral Civil,** Barcelona:Bosch, 1.986, 3ª ed.

- Ministerio de Justicia, Comisión Internacional de Estado Civil (Sección española), **Convenios y Recomendaciones de la Comisión Internacional de Estado Civil**, Madrid: Centro Publicaciones Ministerio Justicia, 1.991.

- *Molina Mateos, José Mª*, "Libertad informática y criptología", **Informática y Derecho, nº 12-15**, 1.996, págs. 971 y siguientes.

- *Martínez Miguel, Luís*, "El papel de la informática y las comunicaciones en la modernización de la Administración del Estado", **Informática y Derecho, nº 9-11,** 1.996, págs. 167 y siguientes.

- *Olvera Lobo, Mª Dolores y otros*, "Sistemas de Gestión y Almacenamiento de Información en disco Óptico en las Administraciones Públicas", **IV Jornadas Españolas de Documentación Automatizada, Documat 94,** 1.994: Universidad de Oviedo.

- *Ortíz Navacerrada, Santiago*, "La prueba de documentos en el proceso civil", **Estudio Jurisprudencial, actividad, doctrina y jurisprudencia.**

- *Paez Maña, Jorge y otros*, "El derecho de acceso y distribución de información por vía telemática como derecho fundamental", **Informática y Derecho, nº 12-15,** 1.996, págs. 1.393 y siguientes.

- *Páez Maña, Jorge y otros*, "Aspectos Jurídicos del Suministro de Información Automatizada", **IV Jornadas Españolas de Documentación Automatizada, Documat 94,** 1.994: Universidad de Oviedo.

- *Palomar Olmeda, Alberto*, "La utilización de las nuevas tecnologías en la actuación administrativa", **Revista Española de Derecho, 87**, 1.995 (Págs. 361-384).

- *Pau Pedrón, Antonio*, **Curso de Práctica Registral,** Madrid: UPCO, 1.995.

- *Paz-Ares, Cándido*, "La reforma del Registro Civil", **Boletín de Información del Ministerio de Justicia, 44,** 1.990 (págs. 1306-1330).

- *Peré Raluy, José*, "Panorama del estado civil y del Registro Civil", en **Revista Pretor, nº 80**, 1.974, págs. 192 y siguientes.

- Programa General de Información y UNISIST (PGI-81/ws/25), "El valor probatorio de las microformas: estudio RAMP", (preparado por Georges Weill), París: UNESCO, 1.981.

- Programa General de Información y UNISIST (PGI-88/ws/15), "Las consecuencias jurídicas de la producción de documentos Informáticos por las Administraciones Públicas: estudio RAMP" (preparado por Birgit Fredberg y Paulette Pieyns-Rigo), París: UNESCO, 1.988.

- *Rouanet Moscardó, Jaime*, "Valor probatorio procesal del documento electrónico", **Informática y Derecho, nº 1,** 1.992, págs. 163-175.

- *Ruíz Miguel, Carlos*, "En torno a la protección de los datos personales automatizados", **Revista de Estudios Políticos, nº 84,** 1.994, págs. 237 y siguientes.

INDICE ALFABETICO DE PONENTES Y COMUNICANTES

INDICE ALFABETICO DE PONENTES Y COMUNICANTES

	Páginas
ALVAREZ RICO, MANUEL	1033
ALVAREZ-CIENFUEGOS SUAREZ, JOSE MARIA	499, 745
AMOROSO FERNANDEZ, YARINA	941
BARRIUSO RUIZ, CARLOS	123
CARRASCOSA LOPEZ, VALENTIN	33
CONSENTINO, GUILLERMO	1177
CORTES MARGALLO, BENJAMIN	1247
CURADO FUENTES, ALEJANDRO	1083
DEL PESO NAVARRO, EMILIO	611
DELPIAZZO, CARLOS E.	699
DORMIDO BENCOMO, SEBASTIAN	57
ELIAS BATURONES, JULIO JOSE	881,1217
FERNANDEZ SANCHEZ, CARLOS MANUEL	689
FRIAS DEL VAL, ANTONIO SALVADOR	1281
GARCIA, JOSE ALBERTO	1177
GARCIA-TORRES FERNANDEZ, MARIA JESUS	815
GAYO SANTA CECILIA, MARIA EUGENIA	221
GOMEZ LOECHES, LUIS	777
HEREDERO HIGUERAS, MANUEL	463
JIJENA LEIVA, RENATO JAVIER	1045
JOYANES AGUILAR, LUIS	547
MARTIN COBISA, FERNANDO	1003
MINGUET MELIAN, JESUS MARIA	527
MOLINA MATEOS, JOSE MARIA	575
NUÑEZ JIMENEZ, JOSE MANUEL	1067,1265
OROZCO PARDO, GUILLERMO	143,847,899
PAEZ MAÑA, JORGE	91
PEREZ LUÑO, ANTONIO	721
PRIETO GUTIERREZ, JESUS MARIA	1091
RAMOS GONZALEZ, MIGUEL ANGEL	657
RIBAS ALEJANDRO, JAVIER	111
RODRIGUEZ DE CASTRO, EDUARDO	345

SANCHEZ MECA, DIEGO 447
SUÑE LLINAS, EMILIO 585
TEJERO, DANIEL OMAR 1177
TEJERO, NESTOR FABIAN 1177
TOSCANO, SILVIA SUSANA 735
ULL PONT, EUGENIO 229

ESTADISTICAS GENERALES

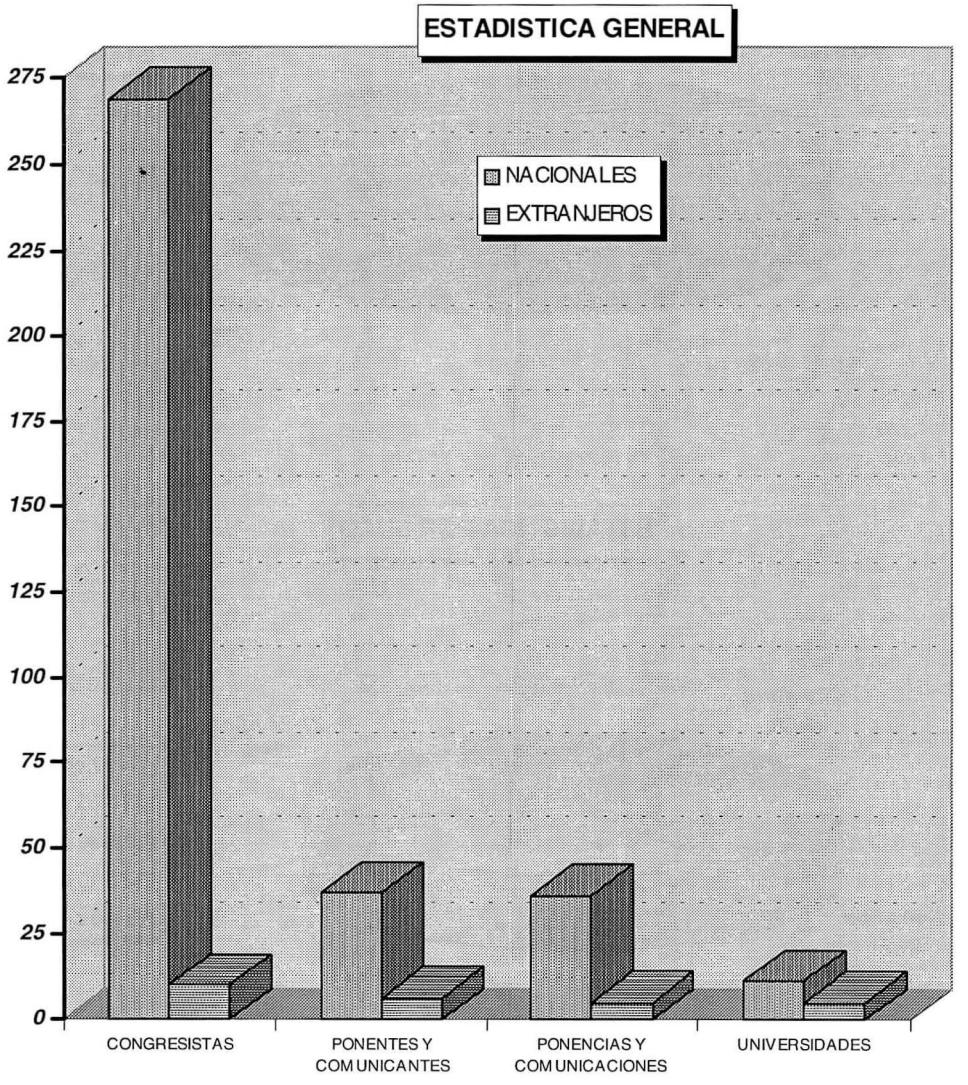
ESTADISTICA GENERAL

	NACIONALES	EXTRANJEROS	TOTAL
CONGRESISTAS*	269	10	279
PONENTES y COMUNICANTES	36	9	45
PONENCIAS y COMUNICACIONES	36	5	41
UNIVERSIDADES	11	5	16

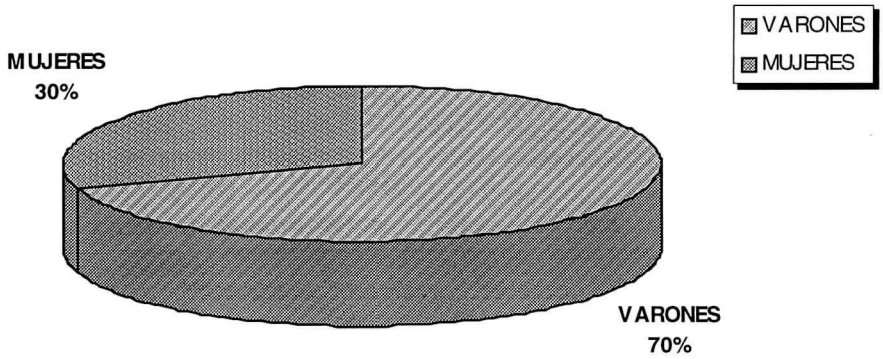
INSTITUCIONES Y EMPRESAS COLABORADORAS: 10

PAISES CON CONGRESISTAS: 6

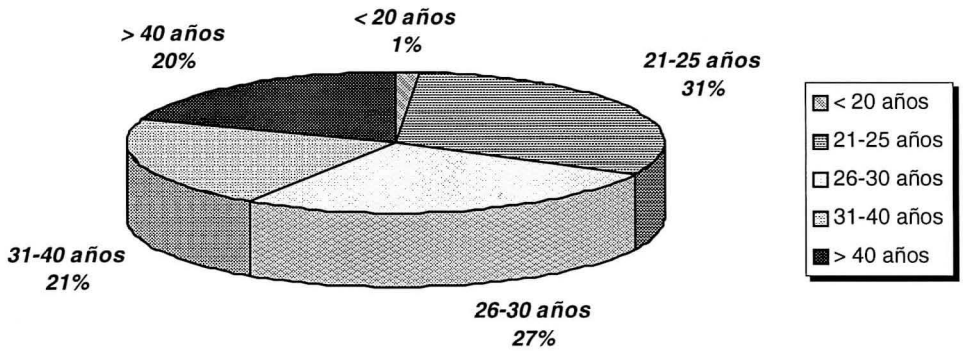
■* INCLUIDOS PONENTES Y COMUNICANTES


ESTADISTICA GENERAL
NACIONALES
EXTRANJEROS
275
250
225
200
175
150
125
100
75
50
25
0
CONGRESISTAS
PONENTES Y COMUNICANTES
PONENCIAS Y COMUNICACIONES
UNIVERSIDADES

ESTADISTICA POR SEXO



ESTADISTICA POR EDAD



RELACION ALFABETICA DE PARTICIPANTES

RELACION ALFABETICA DE PARTICIPANTES

Las direcciones incluidas en esta relación corresponden a inscripciones realizadas en estas Jornadas:

AGENJO CABRERA, FCO. JAVIER
EL PARADOR, 10
06690 GARBAYUELA
(BADAJOZ)
ESPAÑA

ALBA FIGUERO, CARMEN
PEÑA PALACIO DE JUSTICIA
10003 CACERES
(CACERES)
ESPAÑA

ALCON CACERES, JOSE LEON
AVDA. DE LA BORBOLLA, 5
41004 SEVILLA
(SEVILLA)
ESPAÑA
alcon@sevillana.cse.es

ALEGRE CORCHERO, VICENTE
PLAZA STA. MARIA 7 (JUZGADO 2)
06800 MERIDA
(BADAJOZ)
ESPAÑA

ALVARADO PARRON, MIGUEL ANGEL
JUAN RODRIGUEZ SUAREZ, 7-2º C
06800 MERIDA
(BADAJOZ)
ESPAÑA

AMADOR GALVAN, BENITA MARIA
PEÑATO 33
06800 MERIDA
(BADAJOZ)
ESPAÑA

ARENAL LINARES, MANUEL ANGEL
AVDA. GRAL. LOPEZ DOMINGUEZ, 3-404
29600 MARBELLA
(MALAGA)
ESPAÑA
manuel@santandersupernet.com

ARIAS DE SAAVEDRA SANCHEZ, DANIEL
AVDA. EJERCITO ESPAÑOL, 20 BLQ. 1, 3°A
23007 JAEN
(JAEN)
ESPAÑA
darias de@ujaen.es

ARMENDARIZ ISTURIZ, FERMIN
MONASTERIO DE IRACHE, 24.5° C
31011 PAMPLONA
(NAVARRA)
ESPAÑA
feraris@arrakis.es

ARTACHO IZQUIERDO, VIRGINIA
TRAV. RAMBLA STA. EULALIA, 7-1° A
06800 MERIDA
(BADAJOZ)
ESPAÑA

AZUAGA JURADO, MANUEL
SECRET. JUZGADO 1ª INSTANC E INSTRUC. N° 3
VELEZ-MALAGA
(MALAGA)
ESPAÑA

BALSERA MORA, FCO. JAVIER
MATEO GUILLEN Nº 3
06800 MERIDA
(BADAJOZ)
ESPAÑA

BARAHONA Y ALCALDE-MORAÑO, EUGENIO
AV. SANTA MARINA, 25-3º
06005 BADAJOZ
(BADAJOZ)
ESPAÑA

BARRIO RODRIGUEZ, ANA M.
AVD. SUAREZ-BARCENA, 12
06200 ALMENDRALEJO
(BADAJOZ)
ESPAÑA

BEJARANO MOYANO, ANTONIO
VESPASIANO, Nº 27
06800 MERIDA
(BADAJOZ)
ESPAÑA

BEJARANO MOYANO, MANUEL
VESPASIANO, Nº 27
06800 MERIDA
(BADAJOZ)
ESPAÑA

BENITEZ GARCIA, JOSE LUIS
SUAREZ SOMONTE, 43
06800 MERIDA
(BADAJOZ)
ESPAÑA

BENITO SANCHEZ, SOLEDAD
SAGASTA, Nº 5
06800 MERIDA
(BADAJOZ)
ESPAÑA

BERMUDEZ AVILA, MARCOS FCO.
SECRETARIO JUZGADO 1ª INSTANC. E INSTRUC. Nº 1
RORROX
ESPAÑA

BLANCA ORTEGA, FRANCISCO
HEROE SOSTOA, Nº 192-194, PL. 5-A
29003 MALAGA
(MALAGA)
ESPAÑA

BLAZQUEZ BLANCO, Mª DEL PILAR
PONTEZUELAS, Nº 27, B
06800 MERIDA
(BADAJOZ)
ESPAÑA

BLAZQUEZ MANZANO, ALBERTO
DIOCLES, 6, 2º B
06800 MERIDA
(BADAJOZ)
ESPAÑA

BRUSI TERRADES, ALEXANDRE
PUJADA MONTJUIC S/N
17007 GIRONA
(GIRONA)
ESPAÑA
alex@hades.udg.es

CABEZA GONZALEZ, LUIS FCO.
MANUEL DE FALLA, 12-3º IZQ
02005 ALBACETE
(ALBACETE)
ESPAÑA

CACERES GALAN, EDIVIA
URB. "DOMOS IMPERATOR" Nº 19
06800 MERIDA
(BADAJOZ)
ESPAÑA

CACERES GALAN, FRANCISCO Mª
URB. PUENTE ROMANO, 2
06800 MERIDA
(BADAJOZ)
ESPAÑA

CACERES RUIZ, LUIS
RAMBLA STA. EULALIA, Nº16- 3ºB
06800 MERIDA
(BADAJOZ)
ESPAÑA

CALAHORRA GARCIA, IGNACIO JESUS
INSTITUTO Nº6- 1º
42002 SORIA
(SORIA)
ESPAÑA

CALEYA ARENAS, ANTONIO BLAS
JEFATURA SUPERIOR DE POLICIA DE EXTREMADURA
06800 MERIDA
(BADAJOZ)
ESPAÑA

CALPARSORO DAMIAN, JUAN
CIUDAD UNIVERSITARIA S/N
28040 MADRID
(MADRID)
ESPAÑA

CAMINERO VEGAS, RAQUEL
JACINTO BENAVENTE, 1-2º A
34001 PALENCIA
(PALENCIA)
ESPAÑA

CARAPETO SIERRA, JOSE ANTONIO
SAN JUAN DE DIOS 57- 6º I
06003 BADAJOZ
(BADAJOZ)
ESPAÑA

CARBALLO CESTONA, JOSE
Mª DIAZ DE HARO, 3
48013 BILBAO
(VIZCAYA)
ESPAÑA

CARRASCOSA AMIGO, VALENTIN
SANTA LUCIA, 10
06800 MERIDA
(BADAJOZ)
ESPAÑA

CARRASCOSA LOPEZ, VALENTIN
STA. LUCIA, 10
06800 MERIDA
(BADAJOZ)
ESPAÑA
unedmer@arrakis.es

CASILLAS GABARDINO, MARIA EULALIA
AUGUSTO, 26, 2º IZQ.
06800 MERIDA
(BADAJOZ)
ESPAÑA

CASTILLO ESPINOSA, PEDRO
PADRON Nº 4
28925 MADRID
(MADRID)
ESPAÑA

CATALINA AYORA, JUAN IGNACIO
SAN LAZARO, 2
16002 CUENCA
(CUENCA)
ESPAÑA

CEREZO VADILLO, MIGUEL ANGEL
VESPASIANO 10-5º A
06800 MERIDA
(BADAJOZ)
ESPAÑA
mcerezov@hexo.es

CID SALGADO, TOMAS
PROGRESO, 66-6ºD
32003 OURENSE
(OURENSE)
ESPAÑA
sinco@futurnet.es

CIDONCHA RUIZ, JOSE MARIA
LUIS CHAMIZO, 12
06400 DON BENITO
(BADAJOZ)
ESPAÑA

CIDONCHA VAZQUEZ, JUANA MARIA
PINTOR MORALES Nº4, 1ºA
06800 MERIDA
(BADAJOZ)
ESPAÑA

CLARO LOPEZ, FERNANDO
NUEVA ZELANDA, 50
28035 MADRID
(MADRID)
ESPAÑA

CONEJERO MANZANO, FCO. JAVIER
AVDA. REYES CATOLICOS 29- 3º B
06800 MERIDA
(BADAJOZ)
ESPAÑA

CONSTANTINO GARRIDO, JUAN ANTONIO
PONCE DE LEON, Nº6-3ºD
21004 HUELVA
(HUELVA)
ESPAÑA

CORRAL UGENA, AMPARO
c/ CASTELAR, 8, 3º
06800 MERIDA
(BADAJOZ)
ESPAÑA

COSTILLO BORREGO, JOSE CARLOS
GODOBREDO ORTEGA Y MUÑOZ, Nº 32, 6º B
BADAJOZ
(BADAJOZ)
ESPAÑA

CUENA BOY, AMALIA
CIUDAD UNIVERSITARIA S/N
28040 MADRID
(MADRID)
ESPAÑA

CUENCA ROMERO JIMENEZ, FEDERICO TOMAS
AVDA. ESPAÑA EDF. PROCEME IV
CEUTA
(CEUTA)
ESPAÑA

CUERVO ALVAREZ, JOSE
BILBAO, 14- 2º B
05003 AVILA
(AVILA)
ESPAÑA

CHARRO MERINO, ANA CRISTINA
MIGUEL HERNANDEZ, 44
06870 LA GARROVILLA
(BADAJOZ)
ESPAÑA

CHAVARRI MARTINEZ, ENRIQUE
VICENTE GOIKOETXEA, 2
01008 VITORIA-GASTEIZ
(ALAVA)
ESPAÑA

CHIMENO PELLON, MANUEL
Mª DIAZ DE HARO, 3
48013 BILBAO
(VIZCAYA)
ESPAÑA

DE ANDA Y DE ANDA, LORENZO
328 REGAL
LAREDO, TEXAS
(TEXAS)
MEXICO
lor77@valise.com

DE LA CRUZ CARRASC0, MIGUEL ANGEL
CHOPO, Nº 16
21450 CARTAYA
(HUELVA)
ESPAÑA

DE NAVAS CERRAT0, MIGUEL ANGEL
BALDOMERO DIAZ DE ENTRESOTO, 13
06800 MERIDA
(BADAJOZ)
ESPAÑA

DELGADO MENDEZ, ANGEL
VASCO NUÑEZ 56-4ºB
06001 BADAJOZ
(BADAJOZ)
ESPAÑA

DELGADO POZO, SILVIA
BECERROS Nº9
06200 ALMENDRALEJO
(BADAJOZ)
ESPAÑA

DIAZ DONCEL, DIEGO
AVDA. ALEMANIA, 46, 1º A
CACERES
(CACERES)
ESPAÑA

DIAZ-CALERO LOPEZ, JOSE ANTONIO
DIPUTACION PROV. DE GRANADA
18006 GRANADA
(GRANADA)
ESPAÑA
jdcalero@valnet.es

DIEZ RUBIO, FRANCISCO
PROF. ADOLFO MIAJA, 7, 5°B
47014 VALLADOLID
(VALLADOLID)
ESPAÑA

DOMINGO ARCHELOS, Mª JESUS
NTRA. SRA. DE LA MERCED
12530 BURRIANA
(CASTELLON)
ESPAÑA

DOMINGUEZ NOCHE, LUIS ADOLFO
JEFATURA SUPERIOR POLICIA DE EXTREMADURA
CACERES
(CACERES)
ESPAÑA

DORTA LORENZO, ANTONIO JAVIER
LA YEDRA, Nº 5, B LA MANCHA
38430 ICOD DE LOS VINOS
(TENERIFE)
ESPAÑA

DURBAN SALA, MARIA
PLAZA OLERDOLA, Nº9
08023 BARCELONA
(BARCELONA)
ESPAÑA

ERILL PIÑOT, CESAR
ATLANTA, 82
08206 SABADELL
(BARCELONA)
ESPAÑA
cerill@siberia.chpt.es

ESPINO SANCHEZ-GRANDE, ROSARIO
MERIDA, 1
06200 ALMENDRALEJO
(BADAJOZ)
ESPAÑA

ESPINOSA MORENO, BALDOMERO
AVDA. DEL PERU, 30- 5° B
06011 BADAJOZ
(BADAJOZ)
ESPAÑA

FELIPE GARCIA, JAVIER
RONDA DEL PILAR, 2-4°
06002 BADAJOZ
(BADAJOZ)
ESPAÑA

FERNANDEZ CRUZ, JUAN CARLOS
HOLGUIN, 16-2° DCHA.
06800 MERIDA
(BADAJOZ)
ESPAÑA

FERNANDEZ MONTAÑA, ALICIA
ITALIA, 37
06400 DON BENITO
(BADAJOZ)
ESPAÑA

FERREIRA PRIETO, LUIS FRANCISCO
TRAV. DE RAMBLA, 5-1°A
06800 MERIDA
(BADAJOZ)
ESPAÑA

FRANCO RUBIO DE LA TORRE, JOAQUIN DIEGO
PLAZA GABRIEL Y GALAN 6-7, 2° A
37005 SALAMANCA
(SALAMANCA)
ESPAÑA

GALAN CACERES, JUAN-CALIXTO
ADELARDO COVARSI, 9-1° A
6005 MERIDA
(BADAJOZ)
ESPAÑA

GALAN IZQUIERDO, FCO. JAVIER
ISABEL DE AGUILAR, 13
06005 BADAJOZ
(BADAJOZ)
ESPAÑA

GALLARDO GUTIERREZ, MANUEL
AVDA. JUAN CARLOS I, 14
06800 MERIDA
(BADAJOZ)
ESPAÑA

GARCIA BORO, BEGOÑA
AVDA. DE COLON, N° 5
BADAJOZ
(BADAJOZ)
ESPAÑA

GARCIA DE EULALE Y LOPEZ, Mª LUISA
CIUDAD UNIVERSITARIA S/N
28040 MADRID
(MADRID)
ESPAÑA

GARCIA ESCUDERO, FCO. JAVIER
SAN BLAS, 2, 1° C
06200 ALMENDRALEJO
(BADAJOZ)
ESPAÑA
jgescudero@arrakis.es

GARCIA GONZALEZ, CARLOS GUSTAVO
FRAY CRISTOBAL ORAMAL, 7 , 2° D
38430 ICOD DE LOS VINOS
(TENERIFE)
ESPAÑA

GARCIA GONZALEZ, JONAY
FRAY CRISTOBAL ORAMAS, 7, 2° D
38430 ICOD DE LOS VINOS
(TENERIFE)
ESPAÑA

GARCIA MORENO, JUAN LUIS
GEVORA, N° 9
06007 BADAJOZ
(BADAJOZ)
ESPAÑA

GARCIA SANZ, EDUARDO JUAN
JEFATURA SUPERIOR DE POLICIA DE EXTREMADURA
CACERES
(CACERES)
ESPAÑA

GARCIA SOTO, Mª LUISA
LAS LOMAS 1 IZQ. 2º B
06800 MERIDA
(BADAJOZ)
ESPAÑA

GARCIA TRUJILLO, Mª BELEN
DOCTOR FLEMING 12- 5ª E
10001 CACERES
(CACERES)
ESPAÑA

GARZON MURILLO, VICENTE
JEFATURA SUPERIOR DE POLICIA DE EXTREMADURA
BADAJOZ
(BADAJOZ)
ESPAÑA

GODOY PEREZ, PEDRO-ANSELMO
PUBLIO CARISIO, Nº 2
06800 MERIDA
(BADAJOZ)
ESPAÑA

GOMEZ GIL, ALEJANDRO
AV. UNIVERSIDADES 6- 1º IZQ
48007 BILBAO
(BILBAO)
ESPAÑA

GOMEZ PACOMIO, Mª CARMEN
c/ ESPRONCEDA, 11
06800 MERIDA
(BADAJOZ)
ESPAÑA

GOMEZ SOLIS, FCO. JAVIER
LUIS DE MORALES, Nº 8-1º C
06800 MERIDA
(BADAJOZ)
ESPAÑA

GONZALEZ ARRIETA, Mª ANGELICA
CANDELARIO, Nº 2, PORTAL F 6º B
37007 SALAMANCA
(SALAMANCA)
ESPAÑA
angelica@gugu.usal.es

GONZALEZ BUENO, JUAN
GUZMAN EL BUENO, 110
28071 MADRID
(MADRID)
ESPAÑA

GONZALEZ FERNANDEZ, Mª DEL CARMEN
INSTITUTO 27- 4º DCHA.
33201 GIJON
(ASTURIAS)
ESPAÑA

GONZALEZ JIMENEZ, FRANCISCO
COMISARIA DE MERIDA
MERIDA
(BADAJOZ)
ESPAÑA

GONZALEZ VIDAL, CLARA
AVDA. DE TORAL , 14
24550 VILLAMARTIN DE LA ABADIA
(LEON)
ESPAÑA

GUTIERREZ MOGOLLON, MARIA PAZ
ALMIREZ, 7
10910 MALPARTIDA DE CACERES
(CACERES)
ESPAÑA

GUTIERREZ ROMAN, CLAUDIO
COMISARIA DE MERIDA
MERIDA
(BADAJOZ)
ESPAÑA

GUTIERREZ SANCHEZ, MARIA
c/ MARQUESA DE PINARES, 8, 1º B
06800 MERIDA
(BADAJOZ)
ESPAÑA

HERMIRA ANCHUELO, SANTIAGO
MOLINO DE VIENTO, Nº2
28818 SANTORCAZ
(MADRID)
ESPAÑA

HERNANDEZ DIAZ NORIEGA, FRANCISCO
SECRET. JUZGADO 1ª INSTANCIA E INSTRUC. Nº 6
FUENGIROLA
(MALAGA)
ESPAÑA

HERNANDEZ HERRERO, ESPERANZA
DONOSO CORTES, Nº 9
28015 MADRID
(MADRID)
ESPAÑA

HERNANDEZ MARQUEZ, ANGEL
COMISARIA DE MERIDA
MERIDA
(BADAJOZ)
ESPAÑA

HERNANDEZ SOLER, ALBERTO
CRA. ALFONSO XIII, 90
52005 MELILLA
(MELILLA)
ESPAÑA

HIDALGO CONCELLON, JULIO
JEFATURA SUPERIOR DE POLICIA DE EXTREMADURA
BADAJOZ
(BADAJOZ)
ESPAÑA

IZQUIERDO MUÑOZ, LUISA MARIA
PELAYO MORENO 2
06800 MERIDA
(BADAJOZ)
ESPAÑA

JAVATO VERDEJO, Mª JOSE
CTRA. ALCANTARA, Nª 36
10900 ARROYO DE LA LUZ
(CACERES)
ESPAÑA

JIMENEZ CORRALES, Mª ANGELES
RAMON Y CAJAL, 29
13210 VILLARTA DE SAN JUAN
(CIUDAD REAL)
ESPAÑA

JUAREZ RODRIGO, FCO. JAVIER
AVDA. FRANCISCO AGUIRRE, 253- 3° F
45600 TALAVERA DE LA REINA
(TOLEDO)
ESPAÑA

KHAN IGLESIAS, ALEJANDRO
AVDA. MIJAS-ED. VALENCIA 1°
29640 FUENGIROLA
(MALAGA)
ESPAÑA

LEDO AVILA, FRANCISCO
PINTOR LABORDA
06800 MERIDA
(BADAJOZ)
ESPAÑA

LENDINEZ DOMINGUEZ, TERESA
AMBERES, 15
10001 CACERES
(CACERES)
ESPAÑA

LICCIARDELLO BERNABE, TONINO
APDO. 160 (PARTIDA CARROBA S/N)
43870 AMPOSTA
(TARRAGONA)
ESPAÑA
tonino@cerberus.uab.es

LOBATO PASAN, JOSE MIGUEL
LANCHA GARBANCERA 1
10500 VALENCIA DE ALCANTARA
(CACERES)
ESPAÑA

LOBO DELGADO, FCO. JAVIER
CORREDERA HDO. DE SOTO, 4
06380 JEREZ DE LOS CABALLEROS
(BADAJOZ)
ESPAÑA

LOPEZ LOPEZ, MARIA
FRANCISCO DE ALMARAZ, 49
06800 MERIDA
(BADAJOZ)
ESPAÑA

LOPEZ BAZAN, CASTO
JUZGADO Nº3
06800 MERIDA
(BADAJOZ)
ESPAÑA

LOPEZ CABALLERO, ALFONSO
AVENIDA CONSTITUCION, Nº 40
06460 CAMPANARIO
(BADAJOZ)
ESPAÑA

LOPEZ CASTRO, MANUEL
REAL, 14
45071 TOLEDO
(TOLEDO)
ESPAÑA
manuel.lopez@isid.es

LOPEZ SANCHEZ-CABALLERO, PILAR
F.M. PADILLA, 4 E. GUAYASAN
35012 LAS PALMAS
(LAS PALMAS)
ESPAÑA
pilar@sinf.scsgc.rcanaria.es

LOPEZ SERRANO, BELEN
MARCOS GOMEZ 1-1°A
29013 MALAGA
(MALAGA)
ESPAÑA

LOPEZ-GIRALT GARANGOU, FCO. JAVIER
HOSPITAL, Nº 17
17300 BLANES
(GERONA)
ESPAÑA

LUCENA MOLINA, JOSE JUAN
GUZMAN EL BUENO, 110
28071 MADRID
(MADRID)
ESPAÑA

MACIAS VALLE, JOSE ANTONIO
PL. DE LA MARINA, S/N
29015 MALAGA
(MALAGA)
ESPAÑA
jamvalle@sopde.es

MADERA SANCHEZ, MARIA ISABEL
JUZGADO Nº 3
06800 MERIDA
(BADAJOZ)
ESPAÑA

MADRIGAL MONTERO, Mª VICTORIA
UNIVER. PONTIFICIA SALAMANCA
SALAMANCA
(SALAMANCA)
ESPAÑA

MANZANEDO CONDE, ROSA MARIA
ROTA Nº 41-2º
06010 BADAJOZ
(BADAJOZ)
ESPAÑA

MAQUEDA GIL, ELADIO A.
REPUBLICA ARGENTARIA, 15 BAJO B
06005 BADAJOZ
(BADAJOZ)
ESPAÑA
emaqueda @dip-badajoz.es

MARIN GARCIA, ANTONIO
JUZGADO 1ª E INSTANCIA E INSTRUCCION Nº 2
GUADIX
(GRANADA)
ESPAÑA

MARTIN HORMIGO, JOSE
BAHIA, 41
29670 SAN PEDRO DE ALCANTARA
(MALAGA)
ESPAÑA

MARTIN LUIS, CARLOS MARIA
INFANTA ISABEL, 1-6º B
38430 ICOD DE LOS VINOS
(TENERIFE)
ESPAÑA

MARTIN ONCINA, JOSE I.
MORENO DE VARGAS, 4, 2º D
06800 MERIDA
(BADAJOZ)
ESPAÑA

MARTIN PEREZAGUA, ANGEL
PASEO DE MORERAS, 43
45100 SONSECA
(TOLEDO)
ESPAÑA

MARTINEZ ARIAS, JOSE BONIFACIO
SECRET. JUZGADO 1ª INSTANCIA E INSTRUC. Nº 2
MOSTOLES
(MADRID)
ESPAÑA

MARTINEZ CALERO, Mª JOSEFA
GABRIELLA MISTRAL, Nº 38
28035 MADRID
(MADRID)
ESPAÑA

MARTINEZ GOMEZ, RICARDO JESUS
ANTONIO MARTINEZ VIREL, 5-4º I
06011 BADAJOZ
(BADAJOZ)
ESPAÑA

MARTINEZ MIGUEL, ELIA
SAN JULIAN Nº 1
09002 BURGOS
(BURGOS)
ESPAÑA
morgabi@globaldet.es

MATEO CERVERA, FERNANDO
SAN FCO. JAVIER, 14
81511 CABANILLAS
(NAVARRA)
ESPAÑA

MAÑAS VALLE, JOSE ANTONIO
PLAZA DE LA MARINA S/N
29015 MALAGA
(MALAGA)
ESPAÑA
jamvalle@sopde.es

MELENDEZ TEODORO, EZEQUIEL
AVDA. CARDENAL CISNEROS 68 A- 6º A
06007 BADAJOZ
(BADAJOZ)
ESPAÑA
emelendez@bme.es

MENA FERNANDEZ-HUERTAS, JOSE MARIA
HERCULES, 3
06410 TORRESFRESNEDA
(BADAJOZ)
ESPAÑA

MENAYO JIMENEZ, EVA MARIA
VICENTE ALEXANDRE, 2-12
06800 MERIDA
(BADAJOZ)
ESPAÑA

MENDOZA PEREZ, Mª DEL MAR
ALMENDRALEJO, 8- 3º B
06800 MERIDA
(BADAJOZ)
ESPAÑA

MESON, INES DEL CARMEN
AV. SIRIA 1334
4000 S. M. DE TUCUMAN
(TUCUMAN)
ARGENTINA
inesmeson@h otmail.com

MIGUEL RODRIGUEZ, ANGEL LUIS
MARIO ROSSO DE LUNA 15
06800 MERIDA
(BADAJOZ)
ESPAÑA

MIRON RODRIGO, MANUEL
COMISARIA DE POLICIA DE MERIDA
MERIDA
(BADAJOZ)
ESPAÑA

MONTERO MONTERO, FATIMA
JOSE MOLINA RODRIGUEZ, 5-3º D
06800 MERIDA
(BADAJOZ)
ESPAÑA

MONTERO MONTERO, JOSE JOAQUIN
JOSE MOLINA RODRIGUEZ, 5-3º D
06800 MERIDA
(BADAJOZ)
ESPAÑA

MORA AMOR, ALMUDENA
ALMENDROS Nº 10
06400 DON BENITO
(BADAJOZ)
ESPAÑA

MORALES VINAGRE, RAMONA
COPENHAGUE, 1
28820 COSLADA
(MADRID)
ESPAÑA

MORCILLO BALBOA, MIGUEL ANGEL
AVD. CONSTITUCION 22, 4º C
06800 MERIDA
(BADAJOZ)
ESPAÑA

MOTOS CABANILLAS, JESUS
PLAZA DOS MAYO, 1, 1º IZQ.
52006 MELILLA
(MELILLA)
ESPAÑA
g141068103@abonados.cplus.es

MUÑOZ ACERO, MARINA
PALACIO DE JUSTICIA
06800 MERIDA
(BADAJOZ)
ESPAÑA

MUÑOZ ACIARA, ANTONIO
AVD. ANDALUCIA, 45 ESC. 1-1ª A
11007 CADIZ
(CADIZ)
ESPAÑA

NIETO GUILLEN, MIGUEL ANGEL
MATEO GUILLEN, Nº 14-A
06800 MERIDA
(BADAJOZ)
ESPAÑA

NOVA RAMOS, CARLOS JOSE
c/ ALFONSO XII, 21, 4º A
28934 MOSTOLES
(MADRID)
ESPAÑA

NOVA RAMOS, EMILIO F.
SAN JUAN DE DIOS , Nº 6- 2º B
06800 MERIDA
(BADAJOZ)
ESPAÑA

OLIVARES REQUEJO, JOSE LUIS
AVDA. CONCORDIA, 107-4ºA
36700 PONTEVEDRA
(PONTEVEDRA)
ESPAÑA

ORIVE PEÑA, ALFREDO
AVDA. ZUMALACARREGUI, 36- 5º B
48006 BILBAO
(VIZCAYA)
ESPAÑA

ORTEGA DE MUES, MARIANO
c/ Sagrengo, 3, 6º C
28034 MADRID
(MADRID)
ESPAÑA

PABLO DIEZ, JOSE
JEFATURA SUPERIOR DE POLICIA DE EXTREMADURA
06800 MERIDA
(BADAJOZ)
ESPAÑA

PARDILLO HERNANDEZ, AGUSTIN
SECRET. JUZGADO 1ª INSTANC. E INSTRUC. Nº 1
OCAÑA
(TOLEDO)
ESPAÑA

PASTOR MARIN, VICENTE
ALFONSO XII , Nº 92
46520 PUERTO DE SAGUNTO
(VALENCIA)
ESPAÑA

PAVON FERNANDEZ, DIEGO
CAUDILLO FRANCO, 40
ALBALA
(CACERES)
ESPAÑA

PELAEZ FERNANDEZ, PALMIRA
RAMIRO , 53
13730 STA. CRUZ DE MUDELA
(CIUDAD REAL)
ESPAÑA

PEREZ LISBONA, MARIA MERCEDES
SECRET. JUZGADO DE LO SOCIAL Nº 7
MALAGA
(MALAGA)
ESPAÑA

PEREZ MARTINEZ, GUILLERMO
COMISARIA DE MERIDA
MERIDA
(BADAJOZ)
ESPAÑA

PEYROLON JIMENEZ, JULIAN
NUEVA 31
38280 PORTEZUELO-TEGUESTE
(TENERIFE)
ESPAÑA

PILO ACEITUNO, LUIS
AVD. GENERAL CARRACEDO 7, 4º A
06004 BADAJOZ
(BADAJOZ)
ESPAÑA

PORTALO CALERO, JUAN DE DIOS
PABLO NERUDA, 2 BAJO
06180 GEVORA DEL CAUDILLO
(BADAJOZ)
ESPAÑA
jdportalo@audinex.es

POSTIGO TORRES, ANTONIO
AV. MADRID, 23 PORTAL C-2º 1º
28680 SAN MARTIN DE VALDEIGLESIAS
(MADRID)
ESPAÑA

POZO ARRANZ, ASUNCION
RONDA EMERITA, 2-4º D
06800 MERIDA
(BADAJOZ)
ESPAÑA

POZO SANCHEZ, Mª MONTSERRAT
DIEGO Mª CREHUET, 8 A, BJ.
06800 MERIDA
(BADAJOZ)
ESPAÑA

PRIETO PUENTE, JUAN CARLOS
MONJA ETHERIA, 14, 3º
24007 LEON
(LEON)
ESPAÑA

RAMAL CABRERA, BERNARDINO
SECRET. SECCION 1ª AUDIENCIA PROVINCIAL
ALMERIA
(ALMERIA)
ESPAÑA

RAMIREZ PICARZO, TOMAS
MORENO DE VARGAS, 10
06800 MERIDA
(BADAJOZ)
ESPAÑA
unedmer@arrakis.es

RAMIREZ TOLEDANO, JUAN RAFAEL
ALMERIA, 3-5º 1
14009 CORDOBA
(CORDOBA)
ESPAÑA

RAMIRO Y LOZANO, INMACULADA
MARIANO JOSE DE LARRA, 39
06800 MERIDA
(BADAJOZ)
ESPAÑA

RAMOS SANCHEZ, Mª CRISTINA
ESTANCION, 38, 1ª B
47140 LAGUNA DE DUERO
(VALLADOLID)
ESPAÑA

REAL LOPEZ, MANUELA
DIPT. GRANADA. AVDA. DEL SUR Nº 3
18014 GRANADA
(GRANADA)
ESPAÑA

RECIO BLAZQUEZ, SERGIO
SANTA MARIA 18 7° I
42001 SORIA
(SORIA)
ESPAÑA

RICO BONILLA, INMACULADA
PLAZA DEL REY, 6
28004 MADRID
(MADRID)
ESPAÑA

RIESTRA GAYTAN, EMMA
PS. PONTONES 25 PISO 3 B
28005 MADRID
(MADRID)
ESPAÑA
emmeri@cocmax.simucm.es

RODRIGUEZ BAZAGA, FERNANDO
C/ TENIENTE TORRES, 2°
06800 MERIDA
(BADAJOZ)
ESPAÑA
rovial@arrakis.es

RODRIGUEZ BERROCAL, JUAN CARLOS
GOMEZ BECERRA, 12-6° B
10001 CACERES
(CACERES)
ESPAÑA

RODRIGUEZ BLANCO, Mª LUISA
PLAZA DE RIBADEO, N° 9, 3°-B
28029 MADRID
(MADRID)
ESPAÑA

RODRIGUEZ MARTINEZ, ANGEL
PINTOR MORALES, 8-1° E
06800 MERIDA
(BADAJOZ)
ESPAÑA

RODRIGUEZ PEREZ, LUIS
HOSPITAL MEIXOEIRO-MEIXOEIRO S/N
36235 VIGO
(PONTEVEDRA)
ESPAÑA

RODRIGUEZ PROLONGO, JOSE MANUEL
FERNANDO CAMINO, 2
29016 MALAGA
(MALAGA)
ESPAÑA

ROIG NEVOT, ORIOL
MONTSENY, 35-37 1ª B
17005 GIRONA
(GIRONA)
ESPAÑA

ROLDAN GARCIA, Mª DEL MAR
PASAJE HERRERA ORIA, 16-2° B
29007 MALAGA
(MALAGA)
ESPAÑA

ROMERO MERINO, MIGUEL ANGEL
D.G.G.C. - U.C.O. - GUZMAN EL BUENO , 110.
28003 MADRID
(MADRID)
ESPAÑA
gc.uco@mad.servicom.es

ROSA GONZALEZ, Mª JESUS
CABALLERO VILLARROEL, Nº 61
06010 BADAJOZ
(BADAJOZ)
ESPAÑA

ROSA RUIZ, JOSE ANTONIO
GLADIOLOS, Nº 6
29013 MALAGA
(MALAGA)
ESPAÑA

RUIZ VILCHES, JOSE MANUEL
MULACEN, 5- 5º
18005 GRANADA
(GRANADA)
ESPAÑA

SAAVEDRA CHAMORRO, ELENA
MORENO DE VARGAS
06800 MERIDA
(BADAJOZ)
ESPAÑA

SABAN GARCIA, FRANCISCO
ALVAREZ BENAVIDES, 43
41006 SEVILLA
(SEVILLA)
ESPAÑA

SALAMANCA CARRANZA, RAFAEL
MIGUEL UNAMUNO, 8, 2º B
34004 PALENCIA
(PALENCIA)
ESPAÑA
salaman@helcom.es

SALTOR, CARLOS EDUARDO
CJ CERRITO 1249
4000 SAN MIGUEL DE TUCUMAN
(TUCUMAN)
ARGENTINA
morgances@hotmail.com

SANANDRES BARRIGON, JAVIER
ARRABAL, 15
06400 DON BENITO
(BADAJOZ)
ESPAÑA

SANCHEZ CABELLO, JOSEFINA
CIUDAD UNIVERSITARIA S/N
28040 MADRID
(MADRID)
ESPAÑA

SANCHEZ MORAGA, JAVIER
RAFAEL LUCENQUI, 14 7º D
06004 BADAJOZ
(BADAJOZ)
ESPAÑA

SANCHEZ SANCHEZ, MARIA HERMINDA
Gº DE LA PAZ, 7-3º B
48903 CRUCES-BARACALDO
(VIZCAYA)
ESPAÑA

SANTOS TEIJEIRA, ALFONSO
HOSPITAL MEIXOEIRO/MEIXOEIRO S/N
36235 VIGO
(PONTEVEDRA)
ESPAÑA

SANZ GARCIA, Mª DEL CARMEN
CIUDAD UNIVERSITARIA S/N
28040 MADRID
(MADRID)
ESPAÑA

SAUCEDA GARCIA, MANUEL
AVDA. REYES CATOLICOS 35 3° B
06800 MERIDA
(BADAJOZ)
ESPAÑA

SECO CABALLERO, MERCEDES
LUIS DE MORALES, N° 4- 1° C
06800 MERIDA
(BADAJOZ)
ESPAÑA

SEGOVIA RUIZ, FRANCISCO
ALONDRA, Nª 13 -4° D
18014 GRANADA
(GRANADA)
ESPAÑA

SENENT VIDAL, Mª JOSE
UNIVERSITAT JAUME I
CASTELLO
(CASTELLO)
ESPAÑA
senent@uji.es

SERRANO MAESTRE, JOSE MANUEL
ESCUELA DE TRAFICO, N° 3-5
06800 MERIDA
(BADAJOZ)
ESPAÑA

SERRANO RUIZ, JOSE MATEO
URB. PARQUE DEL SOL, BLOQUE 6, 3° C
28260 MADRID
(MADRID)
ESPAÑA

SOBRON ORTIZ, JESUS
VICENTE GOIKOETXEA, 2
01008 VITORIA-GASTEIZ
(ALAVA)
ESPAÑA

SOLER MORENO, Mª TERESA
CIUDAD UNIVERSITARIA S/N
28040 MADRID
(MADRID)
ESPAÑA

SOTO RUIZ, MARIA DEL MAR
BASILIO CUTILLAS, 21
30300 Bº PERAL- CARTAGENA
(MURCIA)
ESPAÑA

TEJEDA SANCHEZ, NIEVES
PIZARRAS, 3
06360 FUENTE DEL MAESTRE
(BADAJOZ)
ESPAÑA
nievests@arrakis.es

TELLEZ GALAN, MARIA ANGELES
REAL, Nº 2
45710 MADRIGALEJO
(TOLEDO)
ESPAÑA

TORRECILLA DAMIANO, PEDRO
CONSTITUCION 20, 2º B
52005 MELILLA
(MELILLA)
ESPAÑA

TRANCON GRAO, JOSE LUIS
AVDA. DEL EJERCITO Nº 7 , 1º D
10600 PLASENCIA
(CACERES)
ESPAÑA

TRIGOSO AVILA, JUAN JOSE
SIMON BENITO BOXOYO, 18
10004 CACERES
(CACERES)
ESPAÑA

VARELA GARCIA, CARLOS
CIUDAD UNIVERSITARIA S/N
28040 MADRID
(MADRID)
ESPAÑA

VELA LOPEZ, CARLOS JAVIER
SANSON CARRASCO, 2-4º-3
29014 MALAGA
(MALAGA)
ESPAÑA

VELARDE CERRATO, Mª GUADALUPE
MARQUESA DE PINARES, 5-3ºC
06800 MERIDA
(BADAJOZ)
ESPAÑA

VELAZQUEZ MOLINERO, MARIA
SANTA LUCIA Nº 10, 2º A
06800 MERIDA
(BADAJOZ)
ESPAÑA

VERDUGO SIMON, PABLO
ALVARADO Nº 4
06800 MERIDA
(BADAJOZ)
ESPAÑA

VILLALOBOS FERNANDEZ, EDUARDO
ORTIZ DE ZUÑIGA, 12
41004 SEVILLA
(SEVILLA)
ESPAÑA
eduardo@talika.cie.us.es

ZAMORANO MAÑANES, DAVID
LA VENTOSA Nº2, 5-B
09001 BURGOS
(BURGOS)
ESPAÑA

ZANZA PLAGARO, SERGIO
CID, Nº12- 2º IZDA.
09200 MIRANDA DE EBRO
(BURGOS)
ESPAÑA

Microsoft®

JUNTA DE EXTREMADURA

FEDERACIÓN IBEROAMERICANA
DE ASOCIACIONES DE DERECHO
E INFORMÁTICA