informática y DERECHO
19-22
20-21
REVISTA IBEROAMERICANA DE DERECHO INFORMÁTICO

JORNADAS

MARCO LEGAL Y DEONTOLÓGICO DE LA INFORMÁTICA

ACTAS
(VOLUMEN I)

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
19-22
20-21
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
19-22
20-21
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: 84-88861-61-3

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

Sumario

Página

PROLOGO..... 13

PRESENTACION:

Instituciones Organizadoras..... 25
Instituciones Copatrocinadoras..... 25
Programa..... 27

PONENCIAS (VOLUMEN I)

"La Regulación Jurídica del fenómeno informático"
VALENTÍN CARRASCOSA LÓPEZ
Director U.N.E.D. Mérida..... 33

"Tecnologías de la Información: Reflexiones sobre el impacto social y humanístico"
SEBASTIÁN DORMIDO BENCOMO
Catedrático. Director Dep. Informática y Automática de la U.N.E.D..... 57

"Derecho Comunitario y Nuevas Tecnologías: Libro Verde y directivas de Bases de Datos"
JORGE PÁEZ MAÑÁ
Consejo Superior Investigaciones Científicas. CSIC..... 91

"Internet: Responsabilidades Legales"
JAVIER RIBAS ALEJANDRO
Abogado especialista en Derecho Informático.
Asesor Jurídico de SEDISI y BSA..... 111

"Contratación Electrónica"
CARLOS BARRIUSO RUÍZ
Abogado, especialista en Derecho Informático..... 123

"Responsabilidad Civil en Materia de Informática"
GUILLERMO OROZCO PARDO
Profesor Titular del Departamento de Derecho Civil. Universidad de Granada...143

"La Sociedad de la Información: Oportunidades y Riesgos"
Mª EUGENIA GAYO STA. CECILIA
Profesora Titular U.N.E.D.....221

"Protección de Datos Personales en Ficheros de Titularidad Pública"
EUGENIO ULL PONT
Profesor Titular U.N.E.D.....229

"Contratación Informática"
EDUARDO RODRIGUEZ DE CASTRO
Abogado, especialista en Derecho Informático. Profesor U.N.E.D. Mérida.....345

"Cuestiones eficaces en torno a la libertad informática"
DIEGO SÁNCHEZ MECA
Profesor Titular U.N.E.D.....447

"La L.O.R.T.A.D. y su futuro"
MANUEL HEREDERO HIGUERAS
Ex-Jefe del Gabinete Jurídico de la Agencia de Protección de Datos.
Consultor de Derecho Informático.....463

"Documento Electrónico"
JOSE Mª ALVAREZ CIENFUEGOS
Magistrado Jefe Gab. Técnico Tribunal Supremo.....499

"Criptología"
JESÚS Mª MINGUET MELIÁN
Profesor Titular U.N.E.D.....527

"Derechos de Autor y uso legal del software"
MESA REDONDA A.L.I.

Presidente: EMILIO DEL MORAL SERRANO.
Secretario de ALI.

Introduce y modera: JESÚS RIVERO LAGUNA
Catedrático del Dpto. OEI/UPM.

Ponentes: JOSE M. FERRER SERVER
Delegado ALI Agencia Proteccion de Datos
AMALIA PELEGRÍN MARTÍNEZ-CANALES
Abogada.
CARLOS DÍAZ DE LA IGLESIA
Director de COMPUTER WORLD.
LUIS JOYANES AGUILAR
Vicedecano Fac. Informática Universidad Pontificia de Salamanca
FELIPE DE ANDRÉS FERNÁNDEZ
Dtor. Gral. Instituto CIBERNOS y ESED

"Derechos de autor y uso legal del software"
LUIS JOYANES AGUILAR
Vicedecano de la Facultad de Informática.
Universidad Pontificia de Comillas..... 547

"Dimensión jurídica de la protección criptológica de la información"
JOSE Mª MOLINA MATEOS
Secretario Asociación Española de Criptología.....575

"Teletrabajo"
EMILIO SUÑÉ LLINAS
Profesor Titular Universidad Complutense.....585

"Auditoría Jurídica de los Entornos Informáticos"
EMILIO DEL PESO NAVARRO
Licenciado en Derecho y en Informática.
Socio-Director de Informáticos Europeos Expertos (IEEE).....611

"Auditoría Informática"
MIGUEL A. RAMOS GONZÁLEZ
Doctor en Informática.
Socio-Director de Informáticos Europeos Expertos (IEEE)..... 657

"Medios eficaces en la lucha contra la piratería"
CARLOS MANUEL FERNÁNDEZ SÁNCHEZ
Director de Programas Antipiratería de Microsoft..... 689

"Marco Legal de la Automatización de la Actividad Administrativa"
CARLOS E. DELPIAZZO
Profesor de la Universidad Mayor de la República Oriental de Uruguay.....699

"Internet y el Derecho"
ANTONIO ENRIQUE PEREZ LUÑO
Profesor Universidad de Sevilla..... 721

"Impacto de las Nuevas Tecnologías y de la Globalización en el Estado Moderno"
SILVIA SUSANA TOSCANO
Abogada. Universidad de Buenos Aires..... 735

"Implicaciones jurídicas de los Sistemas Electrónicos de Comunicación"
JOSE MARIA ALVAREZ-CIENFUEGOS SUAREZ
Magistrado-Jefe del Gabinete Técnico del Tribunal Supremo.....745

COMUNICACIONES (VOLUMEN II)

"El acceso judicial a los datos de carácter personal contenidos en los ficheros automatizados de la Administración Tributaria"
LUIS GOMEZ LOECHES
Licenciado en Derecho.....777

"Los programas de ordenador: analisis de su imposicion directa"
MARÍA JESÚS GARCÍA-TORRES FERNÁNDEZ
Doctor en Derecho Profesor Asociado de Derecho
Financiero Universidad de Granada.....815

"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... 847

"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..... 881

"Notas acerca de la relación entre Informática y la Propiedad Intelectual"
GUILLERMO OROZCO PARDO
Profesor Titular del Departamento de Derecho Civil. Universidad de Granada.....899

"Algunos problemas puntuales. Experiencias Legislativas y Jurisprudenciales en Latinoamérica"
YARINA AMOROSO FERNANDEZ
Especialista del Ministerio de Justicia de Cuba.....941

"Las Nuevas Tecnologías en la Seguridad Social"
FERNANDO MARTIN COBISA
Licenciado en Derecho.....1003

"Informática y Derecho en España"
MANUEL ALVAREZ RICO
Universidad Pontificia de Salamanca en Madrid.....1033

"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)..... 1045

"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.....1067

"Terminología inglesa mas recurrente en el acceso y la recuperación de información en bases de datos bibliográficas"
ALEJANDRO CURADO FUENTES
Profesor de Lengua-Inglesa. E. U. Cáceres. Universidad de Extremadura.....1083

"La Directiva 95/46/CE como criterio unificador"
JESUS MARIA PRIETO GUTIERREZ
Licenciado en Derecho.....1091

"Tras los pasos de la Seguridad perdida. Delitos Informáticos"
GUILLERMO CONSENTINO; JOSE ALBERTO GARCIA;
DANIEL OMAR TEJERO; NESTOR FABIAN TEJERO
Universidad San Juan Bosco de la Patagonia (Argentina).....1177

"La Regulación de los Datos Sensibles en la Directiva 95/46/CE"
JULIO JOSE ELIAS BATURONES
Licenciado en Derecho y experto en Criminología.....1217

"Informática y Tecnologías de la Información: Breve síntesis de la evolución legislativa de la Unión Europea"
BENJAMIN CORTES MARGALLO
Abogado.....1249

"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.....1265

"El Valor Probatorio de los Documentos Informáticos en el Registro Civil"
ANTONIO SALVADOR FRIAS DEL VAL
Cuerpo Superior de Administradores Civiles del Estado.....1281

INDICE ALFABETICO DE PONENTES
Y COMUNICANTES.....1335

ESTADISTICAS GENERALES.....1339

RELACION ALFABETICA DE PARTICIPANTES.....1343

Prólogo

Durante los días 16 al 20 de Septiembre de 1.997, Mérida ha vuelto a ser el punto de encuentro de numerosos profesionales y alumnos de la Informática y del Derecho. De nuevo el Centro Regional de Extremadura de la UNED, en Mérida, a petición de la Delegación de Alumnos de Informática, ha querido estar presente en estas jornadas cuya dirección ha corrido a cargo de don Sebastián Dormido Bencomo, Catedrático y Director del Departamento de Informática y Automática de la UNED y de don Valentín Carrascosa López, Director del Centro Regional de Extremadura de la UNED, en Mérida, con el patrocinio, entre otras instituciones, de la Multinacional MICROSOFT.

El Centro Regional de Extremadura de la UNED en Mérida, cuenta en su haber con más de treinta cursos, jornadas, encuentros, congresos..., sobre la interrelación Informática y Derecho, teniendo el privilegio de haber sido el primer Centro Universitario que se dedicó a esta materia.

En cinco intensos días, se han abordado los temas más candentes sobre la influencia de la Informática en el Derecho y del Derecho en la Informática. De esta forma se ha puesto de manifiesto cómo nuestra sociedad ha sufrido en pocos años, una importante transformación que exige que nuestro Derecho tenga en cuenta a la hora de regular, de una forma coherente y actual, estas nuevas realidades sociales.

A estas Jornadas han asistido unos 300 congresistas, procedentes no solo de Extremadura, sino también del resto de España, e incluso de países del otro lado del Atlántico, como Argentina, México... Debemos destacar la alta cualificación de los asistentes, ya que el 65% de los mismos eran destacados profesionales de ambas materias, entre los que podemos citar: Profesores de Universidad, Fiscales, Jueces, Secretarios Judiciales, Abogados, Informáticos, Técnicos de Diputaciones, miembros del Banco de España... El resto correspondería a alumnos igualmente preocupados por estos temas, entre los que merecen especial mención los 37 Delegados de Centros Universitarios de Informática de la UNED y de otras Universidades Presenciales.

Pese a la dificultad que entraña esquematizar unas Jornadas de tal intensidad como las celebradas en Mérida, no se nos puede escapar cómo los intervinientes han enfocado la nueva problemática Informático-Jurídica desde tres diferentes puntos de vista.

Un primer grupo de ponentes partió de planteamientos filosóficos para adentrarse en el tratamiento de la nueva actitud que debemos tomar ante la transformación sufrida por nuestra sociedad por la presencia de las nuevas tecnologías. La desaparición del espacio y el tiempo como elementos determinantes de las relaciones humanas, hacen que la convivencia exija otros parámetros de calificación. La educación, el comercio, e incluso el propio conocimiento adquiere tintes claramente diferenciados por la influencia de la Informática.

Por todo ello se exige una toma de conciencia que nos lleve a una autorregulación y que nos haga partícipes de los nuevos adelantos con absoluto respeto a las personas, su intimidad y las normas deontológicas.

Un segundo grupo de conferenciantes versaron sus exposiciones sobre temas eminentemente informáticos, mostrando la nueva cara de la técnica, su importancia y sus posibilidades como transformadora de nuestra convivencia. Es precisamente esta nueva tecnología la que puede abrir o cerrar la posibilidad de acceso a la sociedad de la información o transformar las relaciones en un caos de intromisiones y desprotección.

Lo que indudablemente los técnicos en Informática pusieron de manifiesto es la amplia gama de posibilidades que las nuevas tecnologías ofrecen, abriendo así el camino al tercer grupo de ponentes que desde una prisma fundamentalmente jurídico, se adentraron en el estudio de la nueva problemática que la Informática ha creado al Derecho.

La Informática se presenta no sólo como un instrumento que acelera nuestras relaciones jurídicas, transformando indudablemente muchas de sus características, sino que también aparece como un nuevo objeto a regular por el Derecho.

Surgen nuevos delitos, se cualifican otros ya existentes, se comercia a grandes distancias por vía informática, se accede con facilidad a ficheros y bases de datos, y se contrata sobre nuevos objetos y servicios que por sus características, exigen un tratamiento específico, pero por el contrario, nos encontramos con una escasísima regulación sobre este nuevo mundo que nos obliga a utilizar normas que se dictaron en momentos en los que no se imaginaban los avances tecnológicos a los que hemos llegado.

Todos los participantes de estas jornadas, han coincidido en la necesidad de una actualización normativa que parta de una toma de conciencia y autorregulación progresiva, hasta alcanzar la uniformidad internacional que las nuevas características sociales exigen.

Valentín Carrascosa López, Director del Centro Regional de Extremadura en Mérida de la UNED y Presidente de FIADI, hizo un planteamiento global de la regulación jurídica del fenómeno informático, poniendo de manifiesto como una normativa decimonónica no puede responder a unas tan novedosas necesidades. Se cometen "delitos informáticos", se comercia con y sobre la informática, se accede a Bases de Datos..., en definitiva, se han alcanzado grandes cotas de progreso y tecnificación pero se ha olvidado regularlas suficientemente. De esta forma, Valentín Carrascosa planteó los interrogantes que se desarrollarían por los sucesivos profesionales.

Don Sebastián Dormido Bencomo, desde un punto de vista científico, nos hizo reflexionar sobre el impacto social y humanístico que las nuevas tecnologías de la Información han producido, poniendo de manifiesto cómo estos importantes avances no pueden quedar desamparados obviando unas transformaciones de enorme entidad. El Profesor Dormido nos habló de la llamada Revolución Informática, haciendo hincapié en la importancia actual de los computadores, su preeminencia en la sociedad actual, y su presencia como reto y esperanza para el futuro.

Fue don Jorge Paez Mañá, del Consejo Superior de Investigaciones Científicas y renombrado especialista en el estudio de las Bases de Datos, quien nos ilustró sobre la preocupación del Derecho Comunitario ante las nuevas tecnologías, centrando su interesantísima disertación sobre el Libro Verde, las Directivas de Bases de Datos.

El mundo de Internet de tan candente actualidad, y en especial, la responsabilidades legales que su utilización conlleva fue desarrollado por el Abogado Especialista en Derecho Informático y Asesor Jurídico de SEDISI y BSA, don Javier Ribas Alejandro. Internet, podríamos afirmar, supone la desaparición del espacio y del tiempo pero a su vez conlleva una transformación de las comunicaciones y de la vida en general que deben ser minuciosamente tratadas.

Don Javier Ribas, completó su exposición con el estudio de los medios más eficaces de protección de los programas, posiblemente uno de los problemas más novedosos y que sufre más ataques en la actualidad por la falta de toma de conciencia de la que aún adolece nuestra sociedad.

La informática, desde un punto de vista jurídico, se presenta tanto como herramienta como objeto de regulación y es precisamente esta doble concepción la que lleva a los juristas a diferenciar la contratación mediante la informática y sobre la informática.

Don Carlos Barriuso Ruiz, Abogado especialista en derecho informático, fue el encargado en estas Jornadas de ilustrarnos sobre los problemas jurídicos que plantea contratar por medios informáticos, esto es la Contratación Electrónica. Este jurista planteó los problemas que la escasa regulación en la materia provoca a la hora de perfeccionar un contrato por esta vía, haciendo referencia al lugar y momento de perfeccionamiento del contrato, sus requisitos y las armas y defensas con las que contamos para exigir el cumplimiento de un contrato electrónico. Especial mención merece su referencia a la reciente Directiva de la Comunidad Europea 97/7 de 21 de Mayo de 1.997 relativa a la protección de los consumidores en materia de contratos a distancia (DOCE L 144/19 de 4 de Junio de 1.997) que constituye la primera regulación que afronta la venta a distancia con carácter específico y donde se menciona expresamente el correo electrónico, aunque sin contemplar las herramientas de última generación ni las cuestiones fundamentales de la contratación electrónica.

Don Eduardo P. Rodríguez de Castro, abogado especialista en derecho informático y profesor - tutor de la UNED, expuso el tema de la contratación informática en sentido estricto; esto es, la contratación que recae sobre bienes y/ o servicios informáticos.

El referido autor, tras plantear la necesidad de un tratamiento diferenciado de los referidos contratos, realizó un estudio de las características y diferencias fundamentales de esta categoría contractual, deteniéndose en un estudio más pormenorizado de las fundamentales figuras negociales de este área de estudio. Sin agotar todos los posibles contratos informáticos, el referido ponente diseccionó las figuras más representativas como son la Compraventa Informática, la Licencia de distribución, Licencia de Uso, Leasing Informático, el Escrow, el Outsourcing, el contrato Llave en Mano,...

D. Eduardo P. Rodríguez de Castro insistió en la conveniencia de someter las discrepancias que pudieran surgir en la ejecución contractual a la solución Arbitral que de una forma más rápida y especializada las solventen, sin esperar al siempre lento y engorroso procedimiento judicial. Los Arbitros, Informáticos y Juristas especializados, darán siempre un solución más acorde con la realidad contractual de la que venimos hablando.

Dentro del enfoque eminentemente jurídico de la relación Informática y Derecho, don Francisco Hernández Guerrero, Fiscal del Tribunal Superior de Justicia de Andalucía, y don José Luis Alvarez de los Ríos, Fiscal de la Audiencia Provincial de Badajoz, disertaron sobre el candente tema de los Delitos Informáticos.

Puede afirmarse, con don Francisco Hernandez, que no existe un delito informático, sino una criminalidad informática que afecta al orden socio-económoico, al derecho a la intimidad, a la autodeterminación informativa y a la seguridad del tráfico jurídico manifestada a través de los documentos públicos o privados.

Sobre esta base, y tomando como principal instrumento de trabajo tanto la legislación como la práctica jurídica nacional e internacional, los referidos juristas abordaron el estudio de las principales figuras delictivas tipificadas o caracterizadas por acudir a la Informática como elemento diferenciador (tanto en la ejecución de un hecho o en aprovechamiento de sus consecuencias).

Como consecuencia de una lógica coordinación, don Francisco Hernandez Guerrero centró su estudio en el campo del Fraude Informático (Computer Fraud) o Abuso Informático, en el que algunos ordenamientos centran la esencia del delito informático. Por su parte, don José Luis Alvarez hizo un pormenorizado tratamiento de las demás tipos delictivos, especialmente los referidos al ataque a la intimidad.

La última exposición del 17 de Septiembre fue la ponencia sobre Responsabilidad Civil en Materia Informática a cargo de don Guillermo Orozco Pardo, Profesor Titular de la Universidad de Granada. El citado profesor trató la aplicación de las categorías que conforman la teoría general de la responsabilidad civil al campo del tráfico jurídico económico de los bienes y servicios informáticos. En la primera parte de su trabajo hizo una revisión de cual es la situación actual de la obligación de responder que surge cuando se produce un

daño, destacando los conceptos de débito y responsabilidad. En concreto, se analizaron tres supuestos distintos: la responsabilidad por comercialización de productos informáticos, en la que se destacó la obligación por saneamiento por evicción y vicios ocultos, la garantía como contrato accesorio, y la responsabilidad por daños generados por productos defectuosos. En segundo lugar se enjuició la responsabilidad del profesional informático por la prestación de sus servicios, haciéndose especial hincapié en la necesidad de establecer un estatuto jurídico profesional para los informáticos y el desarrollo de un código deontológico. Por último, el citado autor estudió la responsabilidad de los titulares o/y de los encargados de los ficheros automatizados.

La Profesora titular de la UNED, doña Maria Eugenia Gayo Santa Cecilia, disertó desde una perspectiva eminentemente filosófica, sobre la nueva sociedad de la información, una sociedad absolutamente transformada, en la que se nos ofrecen innumerables oportunidades, pero con estas nuevas oportunidades aparecen un sinfín de riesgos que hemos de considerar.

Desde la misma perspectiva filosófica, don Diego Sánchez Meca, Profesor Titular de la UNED, trató las cuestiones éticas en torno a la libertad informática. Hoy, en el siglo XX, en palabras de Sánchez Meca, una tercera generación de derechos hace su aparición inspirada en la solidaridad. Son derechos para los que no es suficiente que algunos individuos o algunas naciones estén decididos a respetarlos, pues no se lograrán las metas a las que apuntan, sin un acuerdo y una colaboración de carácter planetario. Dentro de esta tercera generación de derechos fundamentales hay que situar hoy la libertad informática, entendida como un derecho a la autodeterminación informativa.

Tras este planteamiento, nos sumergimos con Sánchez Meca, en los problemas éticos que plantean las bases de datos e Internet, hasta llegar a conceptos como el de cosmopolitismo y ética planetaria.

La protección de datos personales fue también objeto de un minucioso estudio en las Jornadas celebradas en Mérida. Dada la amplitud del tema, fueron dos ponentes, los que se encargaron de su análisis. Miguel Angel Davara Rodriguez, Director del Instituto de Informática Jurídica de la Universidad Pontificia de Comillas, disertó sobre la Protección de Datos Personales en Ficheros de Titularidad Privada, siendo don Eugenio Ull Pont, Profesor Titular de la UNED, el encargado de ilustrar el tema de la Protección de Datos Personales en Ficheros de Titularidad Pública. El art. 18.4 de la Constitución

Española de 1.978 establece que "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". Partiendo del alcance protector del citado artículo, se adentraron ambos autores, en el estudio de la garantía de los derechos y libertades personales, con una especial atención a la L.O. 5/92 de 29 de Octubre de Regulación del Tratamiento Automatizado de Datos de Carácter Personal.

Otro de los temas que no podían obviarse en unas jornadas sobre la interrelación de la Informática y el Derecho, era el Teletrabajo, que ha sido definido en un informe de la Comisión Europea como aquellas actividades ejercidas lejos de la sede de la empresa (se le denomina también en ocasiones, trabajo a distancia) a través de la comunicación diferida o directa por medio de las nuevas tecnologías. El Profesor Titular de la Facultad de Derecho de la Universidad Complutense de Madrid, don Emilio Suñé Llinás, se encargó de exponer de una forma clara y minuciosa los aspectos que esta nueva situación laboral viene planteando. Así, tras el estudio de la naturaleza jurídica del teletrabajo, acometió su clasificación haciendo referencia a la relación laboral, arrendamiento de servicios o de obra civil, como forma de organización interna empresarial, y como forma de organización interempresarial. El preciso análisis de este ponente le llevó a tratar las ventajas e inconvenientes del teletrabajo, para finalizar tratando el teletrabajo desde el punto de vista de nuestro Derecho Laboral y las iniciativas de la Unión Europea sobre esta materia.

Desde un punto eminentemente técnico, don Jose María Minguet Melián, Profesor Titular de la UNED, expuso el tema de la Criptología. Dicho autor, partiendo del concepto de información y de sistema de información, puso de manifiesto la necesidad de garantizar la seguridad informática y proteger los recursos y el personal informático de las amenazas que se ciernen sobre ellos, como son la intercepción, modificación, interrupción y generación. La Criptología es la ciencia que estudia la escritura secreta, la forma de ocultar el significado de una información, fundamentándose la ciencia criptológica en aspectos de la teoría de la información y de la codificación, de la teoría de números, de la teoría de la complejidad agorítmica y de la teoría de la probabilidad. Minguet trató a su vez, los criptosistemas, los criptoanálisis y las aplicaciones criptográficas, llegando en sus conclusiones a demandar que en los planes de estudios de las titulaciones informáticas, se incluyan asignaturas como los aspectos legales de la informática, seguridad en entornos informáticos, criptología, etc..

La materia tratada por el Profesor Minguet, fue completada por la

ponencia de don Jose Maria Molina Mateos, Secretario de la Asociación Española de Criptología quien nos habló de la Dimensión Jurídica de la Protección Criptológica de la Información, haciendo un estudio interrelacionado de la Criptología y el Derecho, con mención expresa de nuestra Constitución y la LORTAD. Manifestó el referido autor que el uso de la Criptología, como medio de prevención, no ha de aplicarse a ultranza, convencidos de que cuanta más criptología mejor, utilizada de forma abusiva o fraudulenta, puede no solo atentar contra la libertad de información, sino contribuir a la creación de una atmósfera cargada de secretismo.

Los Derechos de Autor y el Uso Legal del Software, fue el título de la Ponencia de don Luis Joyanes Aguilar, Vicedecano de la Facultad de Informática de la Universidad Pontificia de Salamanca en Madrid, quien trató el papel del Estado en la protección de la propiedad intelectual interrelacionando las tecnologías de la información y los derechos civiles, con un minucioso estudio de las implicaciones jurídicas y la regulación del ciberespacio, poniendo énfasis en la propiedad intelectual. El citado autor manifestó que dado que el software es y seguirá siendo uno de los productos estratégicos de la economía mundial, se requiere de los gobiernos nacionales leyes que protejan esos productos ante usos indebidos o fraudulentos, tanto a nivel local como transnacional, además de la necesaria ética profesional.

La problemática de los derechos de autor y los derechos del software fue asímismo tratada en la Mesa Redonda que fue promovida por ALI. Presidió la Mesa, el Ingeniero en Informática y Secretario de ALI, Emilio del Moral, interviniendo D. Carlos de la Iglesia, Director de Computer-World, quien aportó a la Mesa destacados datos sobre el nivel y grado de piratería en el mundo y en nuestro país en particular. D. Jesús Rivero, Catedrático en el Departamento de Organización y Estructura de la Información de la Universidad Politécnica de Madrid y Director de la Secretaría Técnica de ALI, puso de manifiesto una postura moderadamente optimista ante el progresivo descenso de la piratería en España, además del creciente nivel de conciencia social e individual al respecto. Por su parte D. Felipe de Andrés, Director General del Instituto CIBERNOS, aconsejó evitar campañas sensacionalistas que exajeren datos parciales sobre la materia, no obstante, como dijo D. Luis Joyanes, la defensa de la propiedad intelectual, debe iniciarse desde la propia Universidad. El Delegado de ALI en la Agencia de Protección de Datos, también partícipe de esta Mesa Redonda, don Jose Manuel Ferrer, recordó que nuestro ordenamiento otorga protección jurídica a través de la LORTAD, la LPI, el Código Penal..., siendo Doña Amalia

Pelegrín, Abogada del Despacho Anguiano y Asociados, quien reclamó la necesidad de que los Abogados estén al dia en estos temas técnicos.

Don Emilio del Peso Navarro, Abogado e Informático, y D. Miguel A. Ramos González, Doctor en Informática, ambos socios-directores de Informáticos Europeos Expertos, fueron los encargados de desarrollar la apasionante materia de la Auditoría Informática, destacando en un concepto amplio de auditoría informática, los objetivos de colaboración con la auditoría de cuentas, auditoría de los propios sistemas informáticos, y auditoría jurídica de los entornos informáticos. La auditoría en sistemas de información, como función interna, dijo don Miguel Angel ramos, está plenamente justificada en las entidades de cierto volumen, pero tanto en estos casos como en otros, puede estar justificada la auditoría externa, que lejos de ser excluyente, puede muy bien complementarse. Ambos autores trataron y relacionaron el tema de la auditoría con otros aspectos del Derecho Informático, lamentando que la auditoría en los sistemas informáticos, no esté suficientemente implantada en la mayoría de las entidades españolas.

La última de las ponencias de estas intensas jornadas estuvo a cargo de don Carlos Manuel Fernandez Sánchez, Director de Programas Antipiratería de MICROSOFT, y versó sobre los "Medios Eficaces en la Lucha contra la Piratería". Dicho ponente afirmó que la piratería informática es un fenómeno antisocial que perjudica a todos los niveles de la sociedad, tanto al individuo, como a la empresa de tecnologías de la información, al sector empresarial en su conjunto y al Estado. La piratería es una práctica de competencia desleal y un delito, siendo además un ataque a la más elemental ética.

Estas Jornadas fueron clausuradas el sábado 20 de Septiembre, a las 14.00 horas, congratulándonos en nombre de todos los participantes, por el enorme éxito de las mismas, la gran afluencia de congresistas y el enorme interés que todas y cada una de las ponencias y comunicaciones despertó, prometiendo continuar, en nombre de todos y en el mio propio, con esta apasionante labor de estudio e investigación.

VALENTIN CARRASCOSA LOPEZ
Director U.N.E.D. Mérida

PRESENTACION

Jornadas sobre

MARCO LEGAL
Y
DEONTOLOGICO DE LA INFORMATICA

16 a 20 de Septiembre de 1997
Mérida (ESPAÑA)

INSTITUCIONES ORGANIZADORAS

FIADI
(Federación Iberoamericana de Asociaciones de Derecho e Informática)

Centro Regional de Extremadura de la Universidad
Nacional de Educación a Distancia en Mérida

INSTITUCIONES COPATROCINADORAS

Junta de Extremadura

Asamblea de Extremadura

Microsoft

Escuela Universitaria Politécnica de Mérida

OAI
(Organización de Auditores Informáticos)

ALI
(Asociación de Doctores, Licenciados e Ingenieros en Informática)

IEE
(Informáticos Europeos Expertos)

CEJAJ
(Centro de Estudios Jurídicos de la Administración de Justicia)

NEX MEDIA
(Nex Media, Nuevos Medios de Extremadura S.L.)

PROGRAMA

MARTES, 16 DE SEPTIEMBRE

16,30h. "La Regulación Jurídica del fenómeno informático"
Valentín Carrascosa López
Director U.N.E.D. Mérida

18,00h."Tecnologías de la Información: Reflexiones sobre el impacto social y humanístico"
Sebastián Dormido Bencomo
Catedrático. Director Departamento de Informática y Automática de la U.N.E.D.

19,30h."Derecho Comunitario y Nuevas Tecnologías: Libro Verde y directivas de Bases de Datos"
Jorge Páez Mañá
Consejo Superior Investigaciones Científicas

MIÉRCOLES, 17 DE SEPTIEMBRE

09,00h."Internet: Responsabilidades Legales"
Javier Ribas Alejandro
Abogado Espec.. Derecho Informático. Asesor Jurídico SEDISI y BSA.

10,00h."Medios eficaces para la protección de programas"
Javier Ribas Alejandro
Abogado Espec. Derecho Informático. Asesor Jurídico SEDISI y BSA.

12,00h."Contratación Electrónica"
Carlos Barriuso Ruíz
Abogado, especialista en Derecho Informático

16,30h."Delitos Informáticos"

Francisco Hernández Guerrero

Fiscal del Tribunal Superior de Justicia de Granada

18,00h."Delitos Informáticos"

Jose Luís Alvarez de los Ríos

Fiscal de la Audiencia Provincial de Badajoz

19,30h."Responsabilidad Civil en Materia Informática"

Guillermo Orozco Pardo

Profesor Titular Univ. Granada

JUEVES, 18 DE SEPTIEMBRE

9,00h. "La Sociedad de la Información: Oportunidades y Riesgos"

Mª Eugenia Gayo Sta. Cecilia

Profesora Titular U.N.E.D.

10,00h."Protección de Datos Personales en Ficheros de Titularidad Pública"

Eugenio Ull Pont

Profesor Titular U.N.E.D.

12,00h."Contratación Informática"

Eduardo Rodríguez de Castro

Abogado, especialista en Derecho Informático. Profesor U.N.E.D. Mérida

16,30h."Cuestiones eficaces en torno a la libertad informática"

Diego Sánchez Meca

Profesor Titular U.N.E.D.

18,00h."Protección de Datos Personales en Ficheros de Titularidad Privada"

Miguel A. Davara Rodríguez

Director Instituto Informática Jurídica Univ. Comillas

19,30h."La L.O.R.T.A.D. y su futuro"

Manuel Heredero Higueras
Ex-Jefe del Gabinete Jurídico de la Agencia de Protección de Datos. Consultor de Derecho Informático.

VIERNES, 19 DE SEPTIEMBRE

9,00h. "Documento Electrónico"

Jose Mª Alvarez-Cienfuegos Suárez
Magistrado Jefe Gabinete Técnico Tribunal Supremo

10,00h."Criptología"

Jesús Mª Minguet Melián
Profesor Titular U.N.E.D.

12,00h."Criptología"

Jesús Mª Minguet Melián
Profesor Titular U.N.E.D.

16,30h."Derechos de Autor y uso legal del software"
Mesa Redonda A.L.I.

Presidente: Emilio del Moral Serrano.
Secretario de ALI.

Introduce y modera: Jesús Rivero Laguna
Catedrático del Dpto. OEI/UPM.

Ponentes: Jose M. Ferrer Server
Delegado ALI Agencia Proteccion de Datos
Amalia Pelegrín Martínez-Canales
Abogada.

Carlos Díaz de la Iglesia
Director de COMPUTER WORLD.
Luis Joyanes Aguilar
Vicedecano Fac. Informática Universidad Pontificia de Salamanca
Felipe de Andrés Fernández
Dtor. Gral. Instituto CIBERNOS y ESED

18,00h."Aspectos Legales de la Criptología"
Jose Mª Molina Mateos
Secretario Asociación Española de Criptología

19,30h."Teletrabajo"
Emilio Suñé Llinas
Profesor Titular Universidad Complutense

SÁBADO, 20 DE SEPTIEMBRE

09,00h."Auditoría Informática en los entornos informáticos"
Emilio del Peso Navarro
Licenciado en Derecho y en Informática. Socio-Director de Informáticos Europeos Expertos (IEE)

10,00h."Auditoría Informática"
Miguel A. Ramos González
Licenciado en Derecho y en Informática. Socio-Director de Informáticos Europeos Expertos (IEE)

12,00h."Medios eficaces en la lucha contra la piratería"
Carlos Manuel Fernández Sánchez
Director de Programas Antipiratería de Microsoft

ACTAS (VOLUMEN I)

La Regulación Jurídica del fenómeno Informático

VALENTÍN CARRASCOSA LÓPEZ

Director U.N.E.D. Mérida

"No hay razón para negar la realidad del progreso, pero es preciso corregir la noción que cree seguro ese progreso. Más congruente es pensar que no hay ningún progreso seguro, ninguna evolución, sin la amenaza de involución y retroceso....".

ORTEGA Y GASSET

I. Introducción.

Desde hace tiempo, principio de la década de los ochenta, la UNED-EXTREMEÑA, se ha configurado como uno de los foros de reflexión a través del cual se estudian y consideran, con manifiesta humildad, inseguro y titubeante, las necesidades de la interrelación informática y derecho y ayudar con ello en el modelo de sociedad del siglo XXI en el que aparece un mundo que se globaliza, pues si hace algunos años parecía que la "aldea global" era el gran reto del futuro, hoy Internet ha convertido en realidad presente el "hogar global", en la medida en que cada domicilio de los usuarios de la red constituye la terminal de un sistema integrado universal.

Esta globalizacion depende cada vez menos de las geografías, pues, próximo a concluir el siglo XX, la informática y las telecomunicaciones se

presentan, asociadas con el concepto de las autopistas de la información, como determinantes en la construcción de una nueva sociedad, modificando hábitos y costumbres, y cambiando los tradicionales comportamientos y formas de trabajar, de disfrutar del ocio e incluso, de acceder a la formación y la cultura.

Desde los primeros tiempos de la informática, en los años cuarenta, hasta la sofisticación de las redes telemáticas existentes hoy día, se ha recorrido un largo camino en lo que a evolución técnica se refiere, ya que la sociedad moderna no sería posible, en muchos aspectos, sin la presencia del ordenador, que ha llevado a que de los muchos adjetivos con que se ha intentando asignar al momento en que vivimos: la era atómica, la era espacial..... ha llevado a considerar que nos encontramos en la era de la informática.

La era de la informática, es posible, que sea una de las denominaciones que tenga mayor arraigo en el futuro, ya que si la revolución industrial cambió la forma de vida de millones de personas, la aparición del ordenador puede modificar profundamente el mundo de cara al próximo milenio en que se prevé que, en ciertos países, más de la mitad de la población activa tendrá una ocupación que, de una forma u otra, dependerá de la informática.

El ordenador está por todas partes y son pocas las áreas de los negocios, la industria, la ciencia y la educación que no utilizan ampliamente la informática; con ella nos hacen el recibo del agua, el de la luz, controlan nuestras cuentas bancarias y nuestras reservas de dinero pueden ser una serie de números almacenados en los discos magnéticos del ordenador de nuestro banco; el ordenador puede ser un repetidor de lecciones, puede limitarse a comprobar los conocimientos y puede por sí sólo dar verdaderas clases.

En los últimos años, el desarrollo de la tecnología de la información, en especial la amplia difusión de INTERNET, ha tenido una influencia social de tal grado que las prácticas tradicionales de las más diversas disciplinas del conocimiento se han modificado sustancialmente. Tal es el caso de la medicina (asistencia de manera remota al diagnóstico, operación o consulta de un paciente), la ingeniería e incluso el derecho.

Nadie duda, en la década de los noventa, de esos espectaculares avances de las Nuevas Tecnologías de la información y la comunicación y que Internet, esa red de redes que conecta más de dos millones de ordenadores, esta siendo el fenómeno estelar, con más de treinta millones de usuarios, de aquí que

cada día sean más los que consideran que deberían ir acompañadas, igualmente, de una nueva regulación jurídica para evitar que la ofensiva tecnológica no aplaste al hombre aun cuando, por razones de progreso, se vea obligado a cambiar de hábitos y de sus concepciones tradicionales.

Junto a las incuestionables ventajas derivadas de las inmensas posibilidades de conocimiento, actuación y comunicación que permite la navegación por el ciberespacio, que no es otra cosa que un microcosmo digital en el que no existen fronteras, distancias ni autoridad centralizada, Internet ha hecho surgir en los últimos tiempos graves motivos de inquietud (tráfico de imágenes de prostitución infantil, propaganda de bandas terroristas....) que han llevado a millones de ciudadanos a poner de manifiesto los peligros que entrañan determinadas manipulaciones de las nuevas tecnologías.

II. Posición de los Juristas.

Frente a este riesgo de la informática o más concretamente de las Nuevas Tecnologías de la información y la comunicación, los profesionales de ésta, el público en general y especialmente los juristas pueden asumir, al menos, dos actitudes:

1.- Aceptar y someterse al Derecho tal como esta regulado, sin tener en cuenta la discrepancia entre la evolución tecnológica y la reglamentación jurídica.

2.- Desarrollar una nueva legislación adecuada a los cambios que sufre la sociedad, formulando propuestas a fin de que el Derecho asuma nuevas formas que no sólo obstaculicen el uso de las nuevas tecnologías, sino que lo regulen adecuadamente, revisando y adecuando las viejas leyes a las necesidades y situaciones jurídicas que van apareciendo con las nuevas tecnologías.

La solución no puede ser otra que esta última, que a su vez plantea con frecuencia graves problemas político-jurídicos, ya que todo progreso técnico no representa una mejora en la calidad de vida ni un mayor respeto de los derechos individuales, como ya puso de manifiesto ORTEGA Y GASSET, cuando en "La rebelión de las masas", a propósito de comparar primitivismo y técnica, afirma:

"No hay razón para negar la realidad del progreso, pero es preciso corregir la

noción que cree seguro ese progreso. Más congruente es pensar que no hay ningún progreso seguro, ninguna evolución, sin la amenaza de involución y retroceso....."

III. Nueva disciplina: El Derecho Informático.

El intercambio intenso de mercancías más allá de aranceles y costumbres, la simbiosis de las culturas o mejor dicho, su adaptación y asimilación en nuevos contextos, la velocidad con que se transmiten informaciones de toda índole, forman parte de esa idea general a la que conocemos como globalización y que pone de manifiesto que la solucion, jurídica, de estos problemas sea todavía confusa y enrarecida, ya que la rapidez con que suceden los cambios obliga a las personas y a las organizaciones a realizar modificaciones constantes a fin de no perder el contacto ni quedar al margen de este flujo de innovaciones tecnológicas, de aquí que las distintas ramas del derecho se vean afectadas, si bien cada día esta tomando más cuerpo un Derecho de la Informática o Derecho Informático o Derecho de las Nuevas tecnologías, según los autores, ya que razones cualitativas derivadas del papel exponencialmente creciente que juega el ordenador en la sociedad postindustrial hacen emerger esta nueva rama del Derecho, todavía en el umbral de su desarrollo histórico y cuyo contenido no ha sido más que parcialmente definido.

De lo apuntado, podemos deducir, que el ordenador plantea nuevos problemas de tipo jurídico con los que se han de enfrentar los hombres dedicados a la creación, interpretación y aplicación de las leyes: se trata, como hemos dicho, del Derecho Informático, que va adquiriendo carta de naturaleza, aún cuando no está todavía universalmente consagrado como nueva rama del Derecho, aunque si existen numerosas disposiciones legales, una variedad de jurisprudencia y bastantes textos doctrinales al estudio de la materia.

En España la materia no es aún, salvo en contadas excepciones, cada día más numerosas, objeto de asignatura de estudio a nivel universitario, pero sí, es frecuente, en cursos, seminarios y encuentros para intentar clarificar su contenido y también si debe o no constituir una asignatura autónoma, como el Derecho Procesal o el Derecho Mercantil, etc., o por el contrario analizarse y estudiarse en cada una de las disciplinas de la Facultad de Derecho, lo que haría más difícil su sistematización y encontrar especialistas en la materia, a excepción del Derecho Penal donde cada día va tomando cuerpo un Derecho Penal de la informática, pero también es necesario analizar las peculiaridades de los contratos

informáticos, acceso a la información contenida en los bancos de datos, flujo de datos transfronterizos, protección jurídica del software, etc., que hacen prever, como apunta Mario G. Losano, que en el futuro será necesario tratar sistemáticamente el Derecho privado de la informática, el Derecho público de la informática, el Derecho penal de la informática, etc. etc., lo que puede llevar a que la informática sea objeto de estudio simultáneo en las distintas ramas especiales del Derecho a la vez que sería conveniente que se incluyese en los planes académicos alguna asignatura que permitiese un planteamiento interdisciplinario del Derecho de la Informática, tanto en las Facultades de Derecho e Informática como en las Escuelas Universitarias de Informática.

El Derecho Informático, antes o después será una realidad, máxime cuando estamos en el convencimiento de que nos encontramos en un gran cambio en la civilización y por tanto también en el Derecho, y en España, incluso, por mandato imperativo del art. 18.4 de la Constitución, según el cual, la Ley regulará el uso de la Informática.

Con la llegada de la informática se han abierto grandes capítulos en la historia del Derecho y, en España, como hemos dicho, tenemos dos tipos de estudios en los que el Derecho Informático podría incidir directamente. Las Facultades de Derecho e Informática y las Escuelas Universitarias de Informática, que, si quieren preparar a sus titulados para la siguiente generación de desarrollo tecnológico, no les quedará otro remedio que introducir en sus planes de estudios la asignatura de Derecho Informático y estudiar en ella, entre otros, los temas que tienen que ver con la propiedad intelectual de los programas de ordenador, la protección de datos personales, la protección jurídica de las bases de datos, la contratación por medios electrónicos, la transferencia electrónica de datos y fondos, contratos informáticos, el documento electrónico, la prueba, el delito informático, etc.

IV. Nueva Legislación.

Lo apuntado nos ha puesto de manifiesto la necesidad de una nueva legislación adecuada a los cambios que sufre la sociedad y por tanto de una regulación jurídica del fenómeno informático, que, cada vez más, esta siendo estudiado en tesis doctorales.

La regulación jurídica del fenómeno informático no admite demora ya que la incorporación de las denominadas nuevas tecnologías de la

información en nuestra sociedad es una realidad sin retroceso posible. El avance de su implantación en todas nuestras actividades sigue sin parar hacia un futuro prometedor para unos e inc
necesario acompañar los adelantos con una nueva regulación jurídica, que, junto a los sistemas de seguridad (programas de encriptación, los filtros, los cortafuegos, los certificados digitales, los ciberpolicías, ...), representen un principio de esperanza frente a los riesgos y peligros que, sin lugar a duda, comportan las actividades abusivas o ilícitas realizadas a través del ordenador.

Una vez más los hechos - en este caso las nuevas tecnologías - caminan delante del Derecho, entendiendo éste como Derecho positivo, que como regulador de la conducta social del individuo no podía ser, por tanto, ajeno a la importancia decisiva adquirida, en los últimos tiempos, por la informática en la vida cotidiana de los países desarrollados.

De esta forma, el Derecho - como ciencia viva-, se ve influenciado de una manera determinante por la Informática. Así, esta última ha ido calando en el mundo jurídico, no sólo en sus aspectos prácticos, en cuanto facilita la publicación de las leyes, el almacenamiento de datos, la celeridad en los Juzgados...; sino que como faceta de la vida, se presenta como una realidad a tratar por el Derecho. La Informática crea unas relaciones jurídicas que deben ser tuteladas, dada la trascendencia que pueden conllevar. Como podemos observar, la estela de la Informática influye en el Derecho, como en prácticamente todos los aspectos de la vida social.

Pero si el mundo de la Informática, como ya hemos señalado, impregna todas las facetas de la vida humana, no es menos cierto que el desarrollo actual de aquella, su complejidad y la amplia gama de posibilidades que ofrece a través de Internet, crea la necesidad de que sea ahora el Derecho, el que se preocupe de regular las relaciones jurídicas que nacen de la misma.

Si tanto los juristas, como los informáticos, incluso toda persona ajena a éstos ya tan interrelacionados mundos, reconocen sin ningún género de dudas, la posición preeminente que la Informática ha adquirido en la actualidad, no hay, por el contrario, unanimidad en el tratamiento jurídico que a esta materia ha de darse.

Consideramos que cuanto mayor es el avance tecnológico que vamos alcanzando, mayor es la ineficacia o insuficiencia de nuestra normativa

para solventar los problemas jurídicos que van apareciendo. De esta forma la Informática ha creado una parcela con características propias, y con necesidades que nuestras viejas leyes no siempre satisfacen suficientemente.

Muchas veces sucede que cuando tratamos de reconducir estos nuevos hechos a las figuras jurídicas existentes nos encontramos con dificultades. Las viejas instituciones jurídicas que, a través de siglos han ido incorporando nuevas realidades sociales, cuando tienen que hacerlo respecto a estas nuevas tecnologías, en cierto modo, chirrían y las admiten con reserva.

Es fácil comprobar lo mucho que se ha escrito sobre el potencial de las nuevas comunicaciones interactivas en pantalla y de la transición a un mundo multimedia rico en información, existen, igualmente, muchas guías de navegación que explican cómo viajar por Internet, sin embargo, todavía hay mucho que hacer en muchos campos y especialmente en la regulación jurídica del fenómeno informático, clave de la confianza para la existencia y naturaleza de la protección legal sobre la que descansan la nueva contratacion a distancia ya que si el proveedor de servicios no puede confiar en que sus derechos serán protegidos, o si el consumidor no puede confiar en las ofertas del proveedor de servicios, entonces la Sociedad de la Información no será más que un sueño al no conseguir un flujo de comercio significativo y dinámico por falta de protección legal.

V. ¿Leyes con valor universal o autorregulación?.

Son necesarios debates actuales sobre el marco legal, hasta la fecha, el ambiente regulador esta desfasado ya que la regulación jurídica del fenómeno informático no puede circunscribirse a espacios locales o regionales, sino que ante la existencia de redes mundiales - con creciente interactividad - en el sentido de que la autoría se puede producir en un Estado y sus resultados en otro, es imprescindible y urgente que la comunidad internacional se dote de una "Ley Uniforme de la Informática" y de "un Código Deontológico" al respecto, difícil pero necesario si queremos conseguir un mercado funcional global a través de Internet, toda vez que esta dimensión global ha generado hirientes problemas legales, éticos y sociales.

¿Es necesario, por tanto, una normativa universal sobre Internet?.

Interrogantes que van desde el respeto internacional al derecho de autor, el comercio electrónico, el derecho a la intimidad y a la información, aconsejan leyes con valor universal, difícil, por ahora, de conseguirse, por lo que parece que como paso previo, nos encontraremos con la "autorregulación de Internet " y en este sentido las grandes multinacionales Microsoft y Netscape se han comprometido, de mútuo acuerdo, a confeccionar un "código de conducta" (un sistema de autorregulación de Internet) que establezca unas mínimas normas deontológicas en Internet, toda vez que la ética de los negocios forma parte esencial de la empresa contemporánea, por que vender con "honestidad" genera credibilidad en el cliente y amplía eficazmente las redes de mercado.

Establecer un adecuado "código de ética ciberespacial" resulta problemático (porque es un tema sin confines el alcance de la Red y no se puede calcular mínimamente su función manipuladora de conductas y su poder de seducción de voluntades) y unilateral (porque nos movemos con datos estadísticos muy reducidos en sus posibles formas de "perversión ética" en el plano individual y social).

Son tres los campos que tendría que "autocontrolar" ese código ético ciberespacial: garantizar el "secreto" de las comunicaciones, asegurar la correcta "identificación" de los interlocutores y conseguir una auténtica "veracidad" de los mensajes.

Serían cuatro los valores éticos que sirvieran de hitos a perseguir: intimidad, exactitud, propiedad intelectual y acceso. Todos estos valores éticos aluden a un principio regulador, operar como un "filtro de calidad" de los mensajes.

La autorregulación nos lleva a "deberes informáticos de autocontrol", pactados por las empresas, los clientes y las instituciones sociales, para evitar atentados contra el honor y la libertad; para no transgredir derechos de autor; no hacer negocios con tráfico de imágenes pornográficas de niños; para impedir que se den perversamente fórmulas de confección de bombas (con fines terroristas).....He ahí algunos fines derivados de los deberes informáticos de autocontrol, respetando el derecho fundamental de dar y recibir información. La libertad de expresión por Internet no puede estar legalmente "censurada", pero se impone (social y éticamente) que esté "autocontrolada" para que se logre una libertad responsable.

No obstante este intento de autoregulación e incluso de leyes con valor universal, en la actualidad, se observa una fuerte tendencia mundial hacia una liberalización y una desregulación del sector de las telecomunicaciones para afrontar los retos del futuro, sin perjuicio de que, por otra parte, cada día son más el número de leyes que van apareciendo en las legislaciones de varios países para tratar la regulación jurídica del fenómeno informático y evitar con ello que el ciberespacio esté siendo colonizado despiadadamente por todos los gigantes de las telecomunicaciones, que a través de Internet está creando nuevas formas de desigualdad entre "inforricos" e "infopobres", al establecer discriminaciones graves en el acceso y utilización de informaciones y de aquí la conveniencia de que el Derecho Informático, como parte del Derecho que aborda todos los problemas jurídicos que se suscitan como consecuencia de la Informática, se estudie con la independencia y profundidad que exigen las actuales circunstancias.

Si Internet permite a millones de ordenadores comunicarse entre sí y anticipa el futuro de las comunicaciones electrónicas en esa "aldea global" o "ciberespacio" que, en sus inicios, uno de sus mayores alicientes residía en su carácter "acrata", al considerar que actuaba en un espacio absolutamente libre, sin ningún tipo de autoridad o poder que lo regulara o acotara.

El tiempo ha puesto de manifiesto que los grandes beneficiarios de la anarquía de Internet no son los cibernaútas particulares, sino las grandes multinaciones e, incluso los aparatos de control social de los gobiernos.

La conciencia colectiva sobre el respeto de las libertades y de los bienes amenazados por una utilización indebida de los ordenadores y del ciberespacio ponen de manifiesto la necesidad de una autoregulación -con códigos de conducta cuya eficacia se base en la convicción de los usuarios y en su responsabilidad solidaria- y leyes universales y nacionales; lo cierto es que nosotros estamos en un concreto País y éste tiene unas normas, y siguiendo al profesor Efren Borrajo Dacruz, vemos que la informática afecta al Derecho positivo, al menos en los siguientes términos:

a).- En primer lugar, la informática aparece como OBJETO DE REGULACION. Las acciones, procesos y productos informáticos merecen y reciben una atención creciente del legislador. Dan lugar a nuevas y siempre complejas regulaciones.

b).- En segundo lugar, la informática aparece como

INSTRUMENTO AL SERVICIO DEL DERECHO. Es aprovechable en una doble dimensión, a saber: por un lado, en orden a la aplicación del Derecho; por otro lado, en orden a la elaboración y formulación del Derecho. Los bancos de datos jurídicos, los procesos lógicos de análisis del lenguaje y otras muchas técnicas y productos informáticos constituyen medios de trabajo cuya utilización se acrecienta de día en día al servicio del Derecho.

c).- En fin, en tercer lugar, la informática es un factor de transformación social. Afecta, por tanto a la propia realidad socioeconómica que el Derecho regula. Cuestiona las bases mismas de la norma jurídica.

VI. El Derecho Informático en el Ordenamiento Jurídico Español.

Tras este planteamiento general podríamos centralizar lo que entendemos por Derecho Informático y sus principales normas reguladoras del ordenamiento jurídico español.

El Derecho de la Informática, es, para Efren Borrajo, "como un conjunto de normas que, de acuerdo con ciertos principios, regulan las acciones y procesos de la informática y sus productos". Emilio Suñe Llinas concibe el Derecho de la Informática como "el conjunto de normas reguladoras del objeto informático o de los problemas directamente relacionados con la misma".

Ambas definiciones, al igual que cualquier otra que pudiesemos dar o recoger de otros autores, nos llevarían al mismo marco de considerar el Derecho de la Informática como un conjunto de "normas".....; y a éstas, en especial a las españolas, es a las que me voy a referir e intentar resumir en estas líneas, pues cada una de ellas serán expuestas más extensamente por otros ponentes de estas Jornadas, que esquematizaremos, en los siguientes bloques:

- La protección de los datos de carácter personal.

- La protección jurídica de los programas de ordenador.

- Los delitos informáticos.

- La responsabilidad civil en materia informática.

- Informática y proceso: el documento electrónico.

- Los contratos informáticos.

VII. La Protección de los datos de carácter personal.

Dede el año 1970 en que el Estado de Hesse publica la primera Ley de Protección de Datos hasta nuestros días, son numerosos los textos legales que se han ocupado del tema en todo el mundo, y como no podía ser una excepción, igualmente ha sucedido en España, que incluso la propia Constitución española, al igual que la portuguesa y austríaca hace una referencia a la informática y a la protección de las libertades individuales en su art. 18.4 al emplazar al legislador a limitar 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.

Este mandato constitucional se desarrolla, al cumplirse el decimocuarto aniversario de aprobarse la Constitución Española de 1978, con la promulgación de la Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal (LORTAD).

La LORTAD, colma, no obstante llegar tarde, una importantísima laguna legal de nuestro ordenamiento jurídico ampliamente sentido por la opinión pública y que esta ley regulariza al permitir, a los afectados, el derecho de información y acceso a los datos y del derecho de rectificación y cancelación, así como de los principios relativos a la calidad de los datos, a la información sobre su recogida, al consentimiento, a la seguridad y a la cesión de los mismos, en una palabra, a establecer un arsenal de garantías y derechos dentro de un marco normativo, como es la LORTAD que pone fin a las respuestas fragmentarias y marginales para la tutela de la libertad informática de las personas que nuestro ordenamiento jurídico contenía.

La aplicación de la Ley Orgánica 5/1992, a los problemas reales y concretos en esta materia ha puesto de manifiesto la insuficiencia de regulación, en algunos casos, o la ausencia de la misma, en otros, que hace necesario, en un plazo más o menos largo, de una modificación de dicha norma.

La aprobación de la Directiva 95/46/CE y la necesidad de efectuar la transposición de la misma a nuestro Derecho nacional, unido a las Resoluciones del Tribunal Constitucional que pongan fin a los recursos de

inconstitucionalidad formulados contra la Ley Orgánica 5/1992, podrá servir de vehículo necesario para resolver las lagunas e insuficiencias legales detectadas en la LORTAD ya que la situación presente exige una actitud decidida por parte del Poder Legislativo dirigida a efectuar las modificaciones legislativas con la tranquilidad necesaria para resolver del modo más conveniente los problemas que plantea dicha reforma.

Estamos a merced de los ficheros o almacenes de datos. Y la menor "indiscreción" puede producir la ruina del honor, de la familia, de la intimidad e incluso de la economía del ciudadano. De ahí la necesidad de que la regulación jurídica esté bien organizada y que no tenga, en lo posible, lagunas o fallos.

El "Habeas corpus", con todo su inmenso prestigio, no es la vía adecuada para la protección del ciudadano ante ataques informáticos, pero si lo puede ser, con la adecuada regulación, el "Habeas Data" que constituye un cauce procesal para salvaguardar la libertad de la persona en la esfera informática, pues cumple una función paralela al "Habeas Corpus" respecto a la libertad física o de movimiento de la persona.

VIII. La protección de los programas de ordenador.

Hasta 1968 todos los ordenadores eran comercializados de manera indisociada con sus programas, programas que, al nivel de aplicaciones eran adaptados de una manera específica a las necesidades del usuario por el constructor. En ese tiempo se consideraba que al ser los programas de ordenador comercializados con la máquina, su protección se confundía con la del conjunto. En ese sentido, los programas eran tratados como piezas de recambio o artículos análogos.

A partir de 1968, la legislación "antitrus
condujo a una separación progresiva entre máquina y programa abriendo así un mercado particular para estos últimos y a lograr su protección jurídica de una manera autónoma e incrementada incesantemente.

Hoy en día no existe duda alguna acerca de la exigencia de asegurar al programa de ordenador una protección jurídica apropiada, toda vez que los programas en cuanto a su contenido y destino son unos objetos dotados de un valor económico intrínseco: un valor que no depende de la materia que le

es incorporada, sino del factor intelectual integrado en el momento de su creación y del uso de que será objeto; un valor que reside en la información que representa. En este sentido, nos encontramos indiscutiblemente frente a un verdadero bien, ciertamente inmaterial pero susceptible de ser reconocido por el Derecho como otros bienes que, desde hace más de un siglo, han sido objeto de reglamentación legal por la vía de patentes, marcas o derechos de autor.

Hoy día se admite, con caracter general, la protegibilidad de los programas de ordenador como obras de autoría y en esta línea se encuentra la normativa española, es decir, la hoy derogada Ley 16/1993, de 23 de diciembre de incorporación al Derecho español de la Directiva 91/250, de 14 de mayo de 1991, y la actualmente en vigor contenida en el Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el texto refundido de la Ley de Propiedad Intelectual, regularizando, aclarando y armonizando las disposiciones legales vigentes sobre la materia y por tanto de la protección jurídica de los programas de ordenador.

Los programas de ordenador serán protegidos mediante los derechos de autor como obras literarias tal y como se definen en el Convenio de Berna para la protección de obras literarias y artísticas.

Unicamente va a protegerse el programa en cuanto bien inmaterial, independientemente del soporte en el cual se fije el mismo.

El programa de ordenador será protegido únicamente si fuese original, en el sentido de ser una creación intelectual propia de su autor.

IX. Los Delitos Informáticos.

El pasado 4 de julio de 1997 en Bonn, en su discurso inaugural, al comienzo de los dos días de conversaciones en el marco de la Conferencia de Ministros de la UE sobre el tema "Redes de información global- aprovechar sus posibilidades", a la que asistieron Ministros procedentes de 30 países así como representantes de 80 empresas internacionales, acertó el Comisario europeo, Martín Bangemann al definir de modo sencillo el problema central y las vías de solución: "Tanto si se trata de servicios offline como online, lo ilegal siempre será ilegal". O dicho de otro modo: los actos delictivos siguen siendo delitos incluso cuando alguien los comete "navegando por la red de datos".

Es cierto que hemos de preservar el máximo espacio posible de libertad para las redes globales de información y reglamentar sólo aquellos aspectos que sean realmente necesarios pero desde 1969, en que un programador fue condenado en los Estados Unidos por un delito informático, y aquel 1964 en que llego a los Tribunales el primer robo conocido de programas de ordenador, ha pasado mucho tiempo y, sin embargo en la legislación española, hasta el nuevo Código Penal, los delitos contra los elementos "lógicos" (ficheros y programas) encontraban dificultades, en algunos casos insalvables, para ser protegidos penalmente, cosa que no sucede cuando los delitos son contra los elementos físicos del sistema; como cosas muebles que son, reciben el mismo tratamiento que cualquier otra cosa susceptible de apoderamiento, destrucción o inutilización.

Del nuevo Código Penal, aprobado por Ley Orgánica 10/1995, de 23 de noviembre, en vigor desde mayo de 1996, se dice que una de las novedades más atractivas de la Parte Especial es la incorporación del llamado "delito informático". Sin embargo, buceando a lo largo de su artículado nos podemos preguntar ¿Existe, en redalidad, un delito informático, o incluso esta misma expresión ya debería revisarse?, pues todos los delitos pueden cometerse sobre o mediante el ordenador. Así, por ejemplo, se puede matar manipulando el programa del ordenador al que se halla conectado un enfermo en la U.V.I. a fin de que se desconecte automáticamente el respirador en determinado momento; o se puede efectuar una operación de blanqueo de capitales; o se puede realizar apología del terrorismo a través de mensajes enviados por Internet, etc, etc.

Debe reconocerse, la existencia de una realidad criminal, surgida al socaire de las altas tecnologías de la información, que interesa a parcelas bien diversas del Derecho Penal (desde delitos contra la intimidad a las falsedades documentales, desde los delitos económicos hasta otros tan distantes como los delitos contra la seguridad interior y exterior del Estado, por citar algunos ejemplos), realidad criminal frente a la cual las legislaciones tradicionales no estaban preparadas.

Internet ha supuesto un factor de incremento de formas de criminalidad, al potenciar la difusión, virus y abordajes a los sistemas por parte de un número imprevisible e incontrolable de piratas informáticos. Las "autopistas de la información" entrañan también un grave riesgo para la protección de los programas. Así mismo, la facilidad de intercambiar informaciones a distancia puede generar importantes peligros para la proteccion de los datos personales. Internet implica, por tanto el riesgo de un efecto multiplicador de los atentados

contra derechos, bienes e intereses jurídicos.

Para adaptarse a las exigencias de esta nueva expresión de la criminalidad, la mayoría de los ordenamientos de nuestro entorno han experimentado, en los últimos años, importantes reformas de sus leyes penales, siguiendo las recomendaciones emitidas desde distintas instancias y foros internacionales. En España hemos tenido que esperar hasta el nuevo Código Penal para hallar una mayor sensibilidad en materia de criminalidad informática.

De la lectura global del reciente texto se infiere:

1°.-Que para el legislador no existe un delito informático, sino una realidad criminal compleja, vinculada a las nuevas tecnologías de la información, imposible de reconducir a un único tipo legal.

2°.- Que, no obstante, tres han sido las parcelas más directamente afectadas en el intento de aprehender esa realidad criminal:

-Los atentados contra la intimidad (con referencia específica a lo "informático" en el art. 197 del nuevo Código Penal).

-Los atentados contra intereses de contenido "económico" (particularmente a través de los artículos 239, 248.2, 256, 264.2 , 278 y 623.4).

-Las falsedades documentales, remozadas por mor del nuevo concepto de documento que suministra el art. 26 del nuevo Código Penal, comprensivo también del documento electrónico.

3°.-. El nuevo Código Penal contempla la criminalidad informática, no sólo a través de las específicas referencias a lo "informático", sino, además, siempre que el legislador incluye su realización por medios informáticos.

El nuevo Código Penal contempla, entre otras, las siguientes infracciones penales:

- La estafa informática (art. 248.2).

- La utilización ilícita de tarjetas electromagnéticas a los efectos del delito de robo con fuerza (arts. 239 in fine en relación con el art. 238).

- El intrusismo informático- defraudaciones (art.256)

- El sabotaje informático - daños (art. 264 y ss.)

- El espionaje informático (art. 278 y ss.)

- La intimidad (art. 197 y ss.)

- La propiedad intelectual (art. 270 y ss.)

Podríamos seguir concretando otros delitos, como la piratería de programas, etc, pero concluiremos este recorrido en el art. 283, precepto de nuevo cuño, que castiga la manipulación en aparatos automáticos en perjuicio de los consumidores.

Estos y otros preceptos han de jugar un importante papel como instrumento de lucha contra la criminalidad informática, pero el caracter internacional e ilimitado de esas conductas hacen más difícil su descubrimiento, prevención y castigo, ya que incluso en los casos en que puedan ser detectados pueden plantearse conflictos sobre la jurisdicción sancionadora competente.

La criminalidad informática se caracteriza, en suma, por las dificultades que entraña descubrirla, probarla y perseguirla, problemática que se agudiza cuando los diferentes elementos de la cadena se hallan en países distintos y la capacidad de respuesta jurídica se halla fraccionada por las fronteras nacionales.

X. Los Contratos Informáticos.

La contratación actual se ve determinada, por los avances tecnológicos. Sería ridículo imaginar que el mundo jurídico se olvidase de la realidad humana para regular precisamente la convivencia de los hombres.

De esta forma, podemos observar como ciertos contratos han caído en desuso en la actualidad, e incluso existen ciertas figuras jurídicas de tal arcaísmo, que resulta difícil imaginar su posible aplicación práctica.

No es sólo que el objeto de los contratos sea diferente al que

podían tener los romanos, los antiguos moradores de nuestra patria, o nuestros legisladores del siglo XX, sino que estos mismos objetos modifican las características de aquéllos.

Por otra parte, y no menos importante, son los avances técnicos que favorecen, aceleran y en ocasiones, complican, la realidad jurídica del hombre, y más concretamente, sus relaciones contractuales.

Los ordenadores....., están presentes de una u otra forma en todo tipo de contratos, y en muchas ocasiones son, si no determinantes de los mismos sí los caracterizan de tal forma que pueden variar aspectos sustanciales (ley aplicable, juez competente,....etc.).

La Telemática (Ciencia de las Comunicaciones y la Informática), ha minimizado la importancia de la distancia física en la contratación entre personas.

La utilización de los medios electrónicos es una realidad evidente en la actividad negocial, que llega a tener una mayor incidencia en la formulación y cumplimiento de los contratos, sin olvidarnos de la fase precontractual o de preparación de la misma.

Los contratos informáticos - problemas jurídicos relacionados con la adquisición de bienes y servicios informáticos - no sólo deben referirse a equipamiento (hardware), programas (software) y mantenimiento, sino que también afectan a los fabricantes de ordenadores, periféricos, equipos de comunicación, proveedores de suministros consumibles, terminales, vendedores de equipos usados, etc.

La importancia cada día mayor de la actividad informática, su repercusión en la vida económica y los riesgos que ésta representa ponen de manifiesto la importancia y magnitud de los contratos informáticos, que carecen de legislación, jurisprudencia o costumbre; de aquí que debamos acudir al Derecho comparado, si bien hay que actuar con prudencia, meditando cuidadosamente cada caso.

La regla general es que los contratos informáticos sean contratos estándar o de adhesión en los que su característica y desigualdad entre las partes se agrava considerablemente, ya que al desconocer, en la mayoría de los casos, el

cliente la técnica informática no puede establecer juicio sobre el producto o servicio que se le ofrece.

La complejidad no está sólo en la fase contractual, sino que la precede en el estudio de las necesidades del usuario y le sigue en la supervisión del plan de implementación del sistema.

Para que exista el contrato informático es necesario, igual que para cualquier otro tipo de contrato, que se den los tres requisitos del artículo 1.261 del CC.: consentimiento de los contratantes, objeto cierto que sea materia de contrato y causa de la obligación que se establezca.

Igualmente son aplicables a los contratos informáticos las normas contenidas en el C.C. sobre: interpretación, eficacia, rescisión, nulidad, obligaciones de comprador y vendedor, etc.

Podemos igualmente clasificar los contratos informáticos según la materia del acto que se celebre y así nos encontraremos con los de: equipamiento, software, servicios.

Según el negocio jurídico que se celebre nos llevará a contratos de: venta, leasing, locación, horas máquina, prestación de servicios, etc.

De lo apuntado se deduce que la mayoría de nuestras centenarias normas siguen aplicándose a este tipo de contratos que por otra parte dada la especialidad, trascendencia y complejidad de los contratos informáticos requiere una regulación específica de la que carecemos en estos momentos.

Estos y otros son los problemas que puede presentar la contratación electrónica y a los que no podemos dedicarnos por ser materia de otros ponentes que nos lo desarrollaran al propio tiempo que nos pondran de manifiesto lo importante que es conocer ¿cuándo y dónde se concluye el contrato?, autentificación, identidad de los contratantes, fases de la contratación, interpretación, así como las figuras contractuales más representativas: la compraventa informática, contrato de mantenimiento, contrato outsourcing, contrato escrow, contrato llave en mano, contrato sobre bases de datos, etc, etc,.

XI. La Responsabilidad Civil en materia informática.

No se trata nueva doctrina sobre responsabilidad civil. Cuando se habla de responsabilidad en esta materia estamos incursionando siempre en el amplio campo de la doctrina general. Se trata pues, de partir de la disciplina civilista para extraer el "precipitado" básico de las normas de esta naturaleza y aplicarlo, con las debidas correcciones, a un fenómeno tan nuevo como la informática.

El tratamiento particular de los daños generados por la actividad informática se explica en cuanto las soluciones que establece la informática tienen algunos matices diferenciales que apuntan a:

- la complejidad de la materia.
- los particulares vínculos que se establecen entre las partes.
- diverso grado de formación técnica de los sujetos que contratan.
- la diversa posición económica de los contratantes.
- La relevancia que adquiere el periodo precontractual
- las particularidades de la conformidad por entrega, con incidencia en materia de vicios.
- los riesgos que implica el manejo de bancos de datos.

Todo se traduce en el tratamiento diferenciado de los elementos configurativos de la responsabilidad civil en materia informática, donde nos encontramos con daños ocasionados por incumplimientos contractuales (adquisición de equipos, adquisición de programas de ordenador, manejo de bases de datos, etc.) o los generados en responsabilidad extracontractual (aspectos precontractuales, utilización indebida de información nominativa, daños a terceros ajenos a la relación contractual, etc.).

Consideración especial merecería el estudio de la responsabilidad civil en materia de software, o hardware, virus informático, productos defectuosos, responsabilidad por defectos en la actividad telemática (transportador, servidor, usuario,) etc.

XII. Informática y Proceso: Documento Electrónico.

La informática nos lleva a poner de manifiesto la necesidad de un nuevo replanteamiento de los conceptos de prueba, firma, documento original o copia, lugar de los actos y como no el valor probatorio de los comprobantes emitidos por medios electrónicos.

Estos y otros temas, nos llevan a considerar que la materia procesal relacionada con la informática aparece como uno de los campos que con mayor intensidad debe suscitar la atención de juristas y órganos legislativos.

Los hechos, los actos y negocios jurídicos son objeto de afirmación o de negación en el proceso. La cuestión es cómo establecer la prueba en un proceso. La respuesta dependerá de los caracteres particulares de cada tipo de procedimiento - procedimiento inquisitivo o acusatorio - y de los sistemas de prueba - de prueba legal y el de la libre apreciación de la prueba o el mixto.

La LEC en su art. 578 y el CC en su art. 1.215 recogen siete medios de prueba entre los que aparece el documento.

La prueba documental mantiene en nuestros días su tradicional preeminencia y por ello es sin duda la que necesita una más urgente y profunda renovación legislativa que de respuesta a los nuevos planteamientos que la realidad social impone.

En el mundo jurídico el documento, es definido como "el escrito" (art. 596 ss LEC y 1215 y ss CC, si bien en los tiempos modernos y en definiciones, entre otros de, ROUANET Y CARNELUTTI, podemos observar como la característica de escrito no se presenta como sustancial o esencial del documento, abriendo así las puertas a la admisión del documento electrónico, como tal documento.

Las diferencias entre el documento escrito y el documento electrónico, son en principio evidentes, lo que no nos puede llevar a negar el carácter de documento de los segundos, a pesar de que un gran número de autores mantiene que los registros informáticos no son documentos ya que no

están en un soporte papel, no llevan firma y no existe diferencia entre copia y original, pero nuestra opinión se identifica más con aquel sector de la doctrina que considera que los registros informáticos son una forma de escribir y no hay inconveniente para considerar el documento electrónico, como documento escrito, por lo que consideramos que el documento electrónico es un documento en sentido jurídico.

Por documento electrónico debemos entender:

- aquel documento formado POR EL ordenador
(Ejemplo: farmacias)

ó

- aquel documento formado POR MEDIO del ordenador

El documento electrónico se admite como prueba en los sistemas de libre apreciación, pero encuentra muchas más dificultades en los países que han adoptado el criterio de prueba tasada.

En el ordenamiento jurídico español, la prueba debe ser valorada por el Juez, segun su prudente arbitrio, salvo que la ley disponga otra cosa (SISTEMA MIXTO), lo que nos lleva a incluir en el término documento, a efecto probatorios, los documentos electrónicos.

A pesar de que el legislador español se ha olvidado de una necesaria reforma general de la normativa del Código Civil y la Ley de Enjuiciamiento Civil, referente al valor probatorio de los documentos, si se ve reflejada esta progresiva toma de conciencia, en varias normas sectoriales.

- Ley del Patrimonio Histórico (todo soporte)
- Ley de Mercado de Valores (anotación en cuenta)
- Ley I.V.A (factura vía telemática=a originales)
- Ley de Regimen Jurídico de las
  Administraciones Públicas y del
  Procedimiento Común (ar.45 y 59)
    - impulsar medios electrónicos
    - proceso en soporte informático
    - notificaciones

- Ley de Medidas Urgentes de Reforma Procesal
  - añade un apartado 7 al art. 1.429 LEC
- Nuevo Código Penal (art. 26 todo soporte material).

Técnicas de autenticación del documento electrónico

- Código Secreto (P.I.N.) ó Código de Ingreso
  - intransferible y confidencial

- La Criptografía
  sistema de codificación de un texto con una claves

- técnicas basadas en la Biometría.
  - datos físicos o biológicos
    - huellas digitales
    - vasos sanguíneos retina
    - la geometría de la mano
    - las huellas de los labios
    - el reconocimiento de la voz
    - la grafía del individuo

No se puede asegurar de forma absoluta que un programa este exento de errores pero nos atrevemos a decir que esta posible inseguridad existe en la misma medida que en los documentos escritos de puño y letra de los contratantes, en los que conste su firma.

Podemos concluir diciendo que la Comisión de las Naciones Unidas para el Derecho Comercial Internacional emitió una serie de Recomendaciones propugnando la revision de las normas legales y la admisión de las formas de autenticación de los documentos electrónicos.

En el proceso podríamos hacer mención a otros temas relacionados con la informática pero me limitaré a dejar en el aire la siguiente pregunta: ¿Son embargables y secuestrables los ordenadores?. y ¿Los datos

personales y la información que contienen?.

XIII. Conclusiones.

Resulta innegable la enorme influencia que los ordenadores están teniendo en la sociedad de nuestros días.

Los cambios son tan rápidos que la humanidad está perdiendo, en gran medida, su capacidad de asombro.

El peligro real es la posibilidad de que algún hombre o grupos de hombres puedan llegar a controlar a través de los ordenadores y redes a la aldea global.

Es cierto que ninguna tecnología ofrece más potencial, más esperanza en la solución de los problemas que los ordenadores; pero, por otra parte, tampoco hay otra tecnología que plantee más amenazas a las actuaciones de los gobiernos que la propia informática.

La información es materia prima del conocimiento y según Francis Bacon "conocimiento es poder", y el ordenador permite concentrar mucha información que puede ser utilizada de forma correcta o incorrecta según los fines que se persigan.

Para que esa información pueda ser utilizada correctamente necesitamos una regulación jurídica del fenómeno informático pero procurando que éstas preserven el máximo espacio posible de libertad y reglamentar sólo aquellos aspectos que sean realmente necesarios.

La naturaleza internacional de las redes reduce la efectividad de las iniciativas y leyes nacionales y ello se convierte en un fuerte argumento para la cooperación internacional que se está produciendo con retraso.

Es cierto que cada día hay un mayor cúmulo de normas nacionales, supranacionales y autoregulacion del sector, que consideramos es

necesario, hasta cómo para convertir la autoregulación de Internet en leyes con valor universal.

Sin ningún género de duda es necesario desarrollar una nueva legislación adecuada a los cambios que sufre la sociedad como consecuencia de las nuevas tecnologías, pero no intentemos imponer en el mundo virtual las normas que no podemos cumplir en el mundo real.

Tecnologías de la Información: Reflexiones sobre el Impacto Social y Humanístico

SEBASTIÁN DORMIDO BENCOMO

Dpto. de Informática y Automática Facultad de Ciencias, UNED

1. EL CAMBIO TECNOLÓGICO

La Revolución Industrial provocó una furiosa expansión de las capacidades productivas de la humanidad, marcando el comienzo de la era moderna. Ahora, doscientos años después, avanza una nueva revolución que promete intensificar profundamente no sólo la capacidad productiva sino también la potencialidad de la mente humana.

Las nuevas tecnologías de la información están relevando de una forma inexorable a las industrias pesadas y manufactureras como el soporte principal de las economías más desarrolladas del mundo. Pero, a diferencia de la Revolución Industrial, que dependía de recursos finitos, como el petróleo y el hierro, la «revolución de la informática» avivará el suministro inagotable del conocimiento mismo. En todos los países industrializados, y en particular en Estados Unidos, Japón y la CEE, existe una onda de opinión dominante que está penetrando en la sociedad en general. Su característica fundamental es que la materia y la energía pasan a un segundo lugar y la información y el conocimiento se convierten en el nuevo objeto formal de la ciencia y la tecnología, hasta tal punto que economía, cultura y bienestar social dependen cada vez más del nivel alcanzado en el campo de las llamadas altas tecnologías de la información.

Lo distintivo de esta situación es que ahora el conocimiento y los procesos cognitivos (percepción, decisión, planificación, razonamiento, lenguaje y acción) se representan, analizan y sintetizan de la misma forma que se hacía con la materia y la energía en la etapa anterior -aún coexistente-. No hay que perder de vista que el conocimiento computacional se elabora, distribuye y vende como cualquier otro producto, con la diferencia del enorme valor añadido en este caso.

Como muy bien señala Castells, «lo que caracteriza a las nuevas tecnologías es su interdependencia, el hecho de que constituyan un sistema, en el que los avances de cada campo facilitan el progreso en otras áreas de innovación tecnológica sobre la base de la comunicabilidad de la información obtenida y a su traducción en el código específico de cada campo por medio de computadores telecomunicados entre sí».

Sin ánimo de exhaustividad, se analiza a continuación las tecnologías de la información que en nuestra opinión forma el núcleo básico del sistema a que alude Castells. La presentación se hace desde una cierta perspectiva histórica y poniendo el énfasis en su impacto sobre la sociedad actual. En gran parte son reflexiones personales y por lo tanto realizadas sin ningún tipo de dogmatismo que sólo pretenden poner de manifiesto algunos aspectos del problema.

2. LA REVOLUCIÓN INFORMÁTICA

La informática es la ciencia que estudia el tratamiento y almacenamiento de información, utilizando computadores. Es difícil concebir cualquier aspecto de nuestra sociedad, y por tanto de nuestra propia vida, que no se vea de alguna forma afectada por la aparición de los computadores.

Resulta innegable la enorme influencia que los computadores están teniendo en la sociedad de nuestros días. Como muy bien dice el profesor Z. W. Pylyshyn de la Universidad de Stanford, en una época de revolución científica y tecnológica como la nuestra, los cambios rápidos han llegado a asumirse como una condición de la vida misma y esto lleva consigo el que empiece a predominar cierta actitud de apatía hacia la magnitud y proporción del cambio de algunos de nuestros valores fundamentales. La humanidad está perdiendo en gran medida su capacidad de asombro.

Si hiciéramos una lista de las experiencias relacionadas con el computador en las que hemos participado, probablemente quedaríamos asombrados. Los

computadores se usan para preparar las nóminas de las empresas, realizar las reservas de billetes para viajar en avión o tren, mantener actualizadas las cuentas bancarias y llevar un control minucioso de los impuestos sobre la renta. La enseñanza asistida por computador incide en nuestra forma de aprender. La planificación económica de un país sería imposible hoy sin el uso de los computadores. La conmutación de llamadas telefónicas, cuando las líneas están cargadas, es responsabilidad de un computador. Los hospitales y servicios médicos utilizan los computadores para analizar sangre, preparar historias clínicas y hasta proteger nuestras vidas, como elemento indispensable en las unidades de vigilancia intensiva. La llegada del hombre a la luna hubiera sido un sueño quimérico sin la aportación decisiva de los computadores. Estos pocos ejemplos ponen de manifiesto la enorme influencia que estas máquinas están teniendo en la sociedad de nuestros días.

Desde un punto de vista pragmático, el computador se ha incorporado plenamente a la sociedad, produciendo una nueva revolución que denominamos la "revolución informática", con implicaciones que, no por menos explícitas, son menos profundas. El computador se ha convertido en el ejecutor de tareas rutinarias intelectuales, como la máquina de vapor lo fue respecto de las mecánicas. El hombre se ve cada vez más liberado de los procesos no creativos por esta prótesis intelectual que es el computador.

2.1 Algunas consideraciones históricas sobre los computadores

Cuando H. Aiken y sus colaboradores construyeron en 1944 el primer computador digital americano (el Mark IV en la Universidad de Harvard) lo hicieron con miles de tubos de vacío. Esto requería un dispositivo que ocupaba unos 1500 cm^3 y consumía 10 vatios para almacenar un solo bit de información. Si se piensa en el calor emitido por cientos de bombillas de 100 vatios, se puede ver que el mantener fría la máquina era un problema muy importante. Y sin embargo, se trataba de una máquina con muy poca potencia de cálculo comparada con las de hoy día. Como consecuencia de esta situación, quienes hacían predicciones sobre el futuro de los computadores a principio de los años 50, imaginaban un futuro en el que para resolver los problemas de la humanidad se utilizarían computadores gigantes del tamaño de un gran rascacielos, que necesitarían un flujo de agua igual al de las cataratas del Niágara para mantenerse fríos. Esta predicción sobre su tamaño era errónea: las actuales son realmente mucho más pequeñas y más fáciles de enfriar; la razón de esto es el paso de los tubos de vacío a los transitores y a los circuitos integrados.

En los primeros años 60, el tubo de vacío había sido sustituido por un pequeño circuito biestable transistorizado que podía hacer el mismo trabajo consumiendo sólo medio vatio.Los transistores no sólo son más pequeños y utilizan la energía más eficazmente que los tubos de vacío, sino que además son más baratos y más fáciles de producir en masa. La transición a los circuitos integrados (microelectrónica) produjo otro avance considerable. En lugar de utilizar transistores fabricados aisladamente y cablearlos entre sí para formar un circuito, llegó a ser posible grabar todos los componentes y todas las conexiones necesarias para construir el circuito en una sola pastilla de silicio, usando técnicas fotográficas. De repente, los circuitos necesarios para almacenar un bit de información se redujeron a menos de 200 mm^3. Un circuito integrado de los primeros años 60 se podía imprimir con unos 20 componentes. A partir de entonces hemos asistido a un refinamiento rapidísimo de estos circuitos integrados; así, en 1974 contenían más de 20.000 y en la actualidad superan los 64 millones de componentes.

Gordon Moore, cofundador de la empresa norteamericana Intel, de circuitos integrados, ha considerado la velocidad con que se ha efectuado el crecimiento en la complejidad de los circuitos integrados, entendida como número de componentes soportados por aquéllos. Apunta que, partiendo del transistor planar en 1959, dicha complejidad, en promedio, se ha doblado por año. Por tanto, en este momento aparecen como razonables las predicciones de las casas fabricantes de circuitos integrados de que para antes de final de siglo la tecnología habrá evolucionado lo suficiente como para que sea posible disponer, en un solo circuito integrado, de un procesador con longitud de palabra de 128 bits, y una memoria de 500 millones de bits.

La década de los 70 marca un hito importante: la aparición del microprocesador del que se puede decir que está invadiendo de una forma vertiginosa todo el entorno de nuestra vida cotidiana. No obstante, la reducción impresionante del coste de los circuitos de cálculo no implica, lamentablemente, que un sistema completo llegue a ser muy barato, aunque sí que será razonable añadir potencia de cálculo a máquinas y dispositivos que no la tenían antes. Cuando se compra un computador, el coste real de construcción del sistema sólo representa, aproximadamente, la cuarta parte del precio de venta. Las tres cuartas partes restantes corresponden a los estudios de mercado, desarrollo del software, la investigación y los beneficios. De esta cuarta parte del coste total, el procesador cuesta generalmente alrededor de la tercera parte y el resto corresponde a la

memoria y a los dispositivos de entrada y salida. Finalmente, la electrónica real de la unidad central de proceso puede suponer menos de la tercera parte de su coste total. Dicho de otra forma, en los sistemas actuales, la electrónica de la unidad central de proceso cuesta un tercio de un tercio de un cuarto (apoximadamente el 3 por 100) de los costes totales.

Vemos, pues, que el gran impacto de la microelectrónica no consistirá tanto en reducir el coste de los computadores -del tipo de los que existen actualmente-, como en abrir nuevas posibilidades de utilización de la potencia de cálculo. Cuando la multinacional IBM presentó sus primeros computadores comerciales en 1952, un cuidadoso análisis de mercado indicó que con 25 máquinas de aquel tipo se podía satisfacer la demanda durante muchos años, ya que eran pocas las empresas u organismos estatales que utilizaban grandes equipos de operadores de máquinas sumadoras.

Consideremos una de las razones del enorme aumento producido en el uso de los computadores. Cuando se pudo disponer de éstos, el sólo hecho de que una empresa no tuviera que llenar una sala con personas contratadas para utilizar máquinas sumadoras significó que muchos trabajos de tratamiento de la información llegaron a ser factibles de repente.

2.2 ¿Por qué se utilizan los computadores?

Básicamente, un computador es una máquina para procesar datos. Quizás la pregunta que muchos se estén formulando es ésta: ¿por qué el hombre utiliza máquinas? La respuesta es muy sencilla: esencialmente porque las máquinas simplifican el trabajo. Veamos un ejemplo. El ser humano está perfectamente capacitado para realizar los cimientos de una casa de forma manual utilizando una pala; sin embargo, la forma usual de hacerlo hoy día es mediante una pala mecánica. ¿Por qué?. Simplemente porque es más fácil y mucho menos costoso usar la máquina. Pues bien, los computadores se utilizan para procesar datos exactamente por la misma razón.

¿Quiere significar esto que necesariamente todo el procesamiento de datos tiene que ser efectuado por un computador?. Por supuesto que no. ¿Alquilaríamos una pala mecánica para hacer un hoyo en el que plantar un pequeño árbol? Hay ocasiones en las que el trabajo manual es mejor que el mecanizado y esta misma regla se mantiene también en el procesamiento de datos. Es obvio en nuestro ejemplo que el agujero necesitado para los cimientos de una

casa es significativamente diferente del requerido para plantar un pequeño árbol. La cuestión está dónde fijamos la frontera de cuándo la utilización de la máquina se hace ventajosa para nuestros objetivos. Quizás la mejor forma de conseguir una comprensión de exactamente cómo delimitar en un problema dado la línea de separación entre la solución manual y la solución automatizada es mediante un ejemplo. Consideremos una actividad muy común en el procesamiento de datos: el pago de la nómina a los empleados de una empresa. Los pasos que seguir para pagar a un empleado serían:

a)Encontrar el número de horas trabajadas por el empleado en cuestión durante el mes

b)Multiplicar las horas trabajadas por el empleado por el salario convenido por hora de trabajo, lo que nos da el sueldo neto o bruto

c)Añadir los complementos y ayuda familiar si hubiese lugar a ello

d)Determinar las deducciones: impuestos sobre el rendimiento del trabajo personal, tasas de la Seguridad Social, mutualidades, derechos pasivos, etc

e)Restar las deducciones, lo que nos da el sueldo líquido

f)Preparar un cheque.

Esta misma secuencia de pasos se debe repetir para cada empleado. Obviamente esto nos sitúa en este caso en la solución del problema: utilizar una solución automatizada o no dependerá del número de empleados a los que haya que preparar una nómina. Así, pues, el computador puede suministrar una solución a nuestro problema, siempre que se cumplan las dos condiciones siguientes:

1)Podemos describir las tareas a realizar mediante una secuencia perfectamente definida de acciones elementales

2)Esta misma tarea se debe repetir muchas veces

Ambas características de pasos bien definidos y repetidos muchas veces están presentes en la gran mayoría de las aplicaciones comerciales de los computadores. Esta es la motivación fundamental que existe detrás de todas las posibles formas de «automatización»: si la utilización de la máquina es más barata que la del ser humano, la máquina será utilizada. En otras palabras, los computadores se utilizan por razones económicas, ya que nos permiten manejar ciertas funciones a un coste inferior que el que sería posible sin su utilización.

¿Pero únicamente por esto -con ser muy importante utilizamos los computadores?.

Hay algo más: también nos permiten realizar tareas que, sin su concurso, sería imposible que se llevasen a efecto. A lo largo de su historia el ser humano ha confiado fundamentalmente en su cerebro para efectuar los cálculos; en otras palabras, él mismo era el sistema de cálculo (computador). Cuando el tamaño y complejidad de éstos fue aumentando rápidamente, se hicieron obvias dos serias limitaciones:

a)La velocidad a la cual puede realizar cálculos una persona es muy limitada. Una operación elemental típica, como una suma o multiplicación, puede necesitar algunos segundos o minutos. Hoy día problemas que requieren incluso billones de tales operaciones se resuelven de forma rutinaria utilizando los computadores. Tales problemas nunca podrían ser resueltos manualmente en un período razonable de tiempo o a un costo moderado.

b)Los seres humanos somos por naturaleza propensos a cometer equivocaciones, de manera que los cálculos de cierta complejidad realizados a mano son generalmente poco fiables a menos que se tomen precauciones muy serias para eliminar los errores. Como las máquinas no están afectadas por las fuentes usuales de error (distracciones, cansancio, etc.), pueden dar resultados que están, con una gran probabilidad, libres de error.

2.3 Velocidad y precisión: Características esenciales de los computadores

Estas dos características de velocidad y precisión son las que, de forma complementaria, pone el computador al servicio del hombre, para multiplicar su capacidad de hacer aquello que potencialmente, en razón de su inteligencia, es realmente capaz de realizar.

Uno de los más apasionantes logros de la humanidad en los últimos años, la conquista del espacio, no hubiera sido posible sin el concurso de los computadores. Consideremos por ejemplo el número de variables que hay que manejar para intentar colocar un cohete en la luna. La tierra está girando sobre su propio eje y moviéndose en el espacio. El viento es un factor que tener en cuenta y, cuando el cohete se mueve a lo largo de la atmósfera terrestre, su velocidad puede variar de forma significativa. La luna es un blanco móvil. Incluso hay que

tomar en consideración la atracción gravitacional del sol y de los demás planetas. El problema es, pues, de complejidad y velocidad, y el ser humano no puede realmente manejar todas estas variables con suficiente rapidez. El control del tráfico aéreo en un gran aeropuerto es un problema similar. Podemos visualizar cada avión como un punto en el espacio, localizado por sus coordenadas y su dirección de vuelo. Cuando hay sólo unos pocos aviones no se plantea ningún problema. ¿Pero qué sucede si hay 20 aviones esperando instrucciones para el aterrizaje y otros tantos para el despegue? Aunque las decisiones humanas son todavía esenciales en el control del tráfico aéreo, el computador supone una ayuda eficacísima para el controlador aéreo alertándole de situaciones potencialmente peligrosas antes que sea demasiado tarde. Aunque ninguna de estas situaciones es controlada enteramente por el hombre, no hemos de perder de vista que las ecuaciones y estrategias necesarias para realizar un vuelo espacial o el control del tráfico aéreo, sí han sido realizadas por él. El computador no está haciendo realmente nada que no haya sido antes realizado por el ser humano. Lo que sucede es que, debido a sus limitaciones, el hombre no puede efectuar estas tareas con la rapidez que se requiere. La habilidad del computador es, pues, de velocidad y no de inteligencia.

Pero, ¿hasta que punto son veloces los computadores? Fijemos esta cuestión en sus justos términos. Un segundo es un período de tiempo extraordinariamente grande para un computador. En los computadores de hoy día la unidad básica para la medida del tiempo es el nanosegundo (10^{-9} segundos = 0,000000001 segundos). Estamos, por tanto, diciendo que un computador puede realizar ¡1000 millones de sumas en 1 segundo¡. De esta forma podemos darnos cuenta qué cálculos relativamente complejos se pueden ejecutar en un computador en unas pocas milésimas de segundo. ¡Hay tantos nanosegundos en un segundo como segundos en 30 años!.

R.W. Hamming ha tomado otro enfoque para poner de manifiesto la velocidad de los computadores. Consiste en considerar la evolución en el transcurso del tiempo de diversas actividades o hechos en función del estado tecnológico del momento (ver Tabla 1).

Area	Antigüedad	1870	1950	1970
Transporte	65 Km/día	325 Km/día	10^4 Km/día	58.500 Km/día
Expectativa de vida	22 años	45 años	66 años	68 años
Grandes obras	Gran muralla	Canal de Suez	Presa de Fort-Peck	Presa de Mangla
Educación	Ninguna	1 año	6 años	10 años
Potencia explosiva	0.5 Kg TNT	500 Kg TNT	10^6 Ton TNT	10^8 Ton TNT
Energía/persona	0.5 C.V	1.6 C.V	10 C.V	15 C.V
Velocidad de cálculo	0.005	0.005	40	10^7

Tabla 1: Comparación de los avances tecnológicos

De la Tabla 1 se deduce que el aumento en dos áreas específicas: la potencia explosiva y la velocidad de cálculo han sido enormes. Estos dos cambios tecnológicos son de tal magnitud que están modificando a la sociedad misma. La unidad para la energía por persona es un motor de 1 C.V. trabajando 8 h. /día y la de velocidad de cálculo son multiplicaciones/segundo con números de 8 dígitos. Si hubiese habido en los últimos 100 años el mismo aumento en la velocidad del transporte que el que ha existido en la velocidad de cálculo, se podría viajar de Madrid a Los Angeles en 0,002 segundos o ir de la Tierra a la Luna en 0,1 segundo, o al Sol en 6,5 minutos. Esto es ¡más rápido que la velocidad de la luz!.

Es importante observar que grandes cambios en magnitud pueden cambiar, y de hecho así lo hacen, la naturaleza básica de una situación. Esto se

ilustra, por ejemplo si se considera el premio en metálico que recibe un quinielista que ha acertado un pleno. Si recibe 500 pesetas, no representa ningún efecto sobre él (probablemente apostaría más de esa cantidad). Si el premio es de cien veces esta cantidad, es decir, 50.000 pesetas, se llevará una alegría, pero no cambiará en absoluto su situación financiera. Si por el contrario le corresponde cien veces esa cantidad, 5 millones de pesetas, la cosa empieza a cambiar. Ciertamente mejorará su posición financiera; sin embargo, no se libera económicamente de forma total en un futuro inmediato. Este dinero lo puede invertir en la compra de un buen coche o para ayudarle a cambiar de vivienda. Una vez invertido el dinero, volverá a preocuparle otra vez (en la medida que debe preocupar el tener o no tener más o menos cantidad de dinero). Sin embargo, si el premio hubiese sido de mil veces esta cantidad, es decir, 5.000 millones de pesetas (en el supuesto de que se pudiesen dar estos premios), entonces, la naturaleza básica de su situación económica hubiera cambiado. No es posible que se gaste todo el dinero en cosas de tipo personal. Pues bien, el cambio en magnitud en la velocidad de cálculo (y en la potencia explosiva) es mayor que la del ejemplo precedente.

2.4 El computador como máquina que procesa datos y produce información

El computador viene a llenar una necesidad sentida por la humanidad desde siempre: la necesidad de información. El género humano ha precisado siempre de un medio para organizar sus observaciones de una manera sistemática. Los datos por sí mismos carecen de utilidad, deben ser procesados o sintetizados de alguna manera antes de que se hagan significativos. Las sociedades primitivas no distinguían entre los términos «dato» e «información», pero la distinción realmente existía y el sentido de esta distinción simboliza el desarrollo de los sistemas de procesamiento de datos.

Las civilizaciones antiguas nunca oyeron hablar de computadores, pero sus gentes sobrevivían y prosperaban porque eran capaces de sacar conclusiones de sus observaciones. Dicho de otra forma, necesitaban información y la adquirían escudriñando su entorno, lo que era una forma simple de procesamiento de datos. Las primeras sociedades agrarias, por ejemplo, aprendieron a anotar hechos tales como cuándo salía y cuándo se ponía el sol, cuándo hacía frío o calor, cuándo llegaba la época de las lluvias, etc. Estos datos elementales no tuvieron utilidad hasta que fueron sintetizados. Pronto el hombre aprendió a organizar la siembra y la recogida del grano en relación con estos

fenómenos naturales. Los egipcios comprendieron claramente los conceptos esenciales de la astronomía, anotando cuidadosamente las fechas en las que se producían los solsticios de verano e invierno, lo que les llevó a predecir de manera muy precisa cuándo ocurrirían las inundaciones del Nilo.

Estos ejemplos tratan de poner de manifiesto cómo ya desde la antigüedad el ser humano, a partir de unos datos, aparentemente sin utilidad, era capaz de correlacionarlos entre sí para generar una información que le fuera útil según sus necesidades. Si ahora nos resulta clara esta relación entre dato e información, ¿por qué no fue desarrollado el computador mucho antes en nuestra historia?, ¿por qué se dependió durante tanto tiempo de nuestras observaciones personales y de las relativamente simples herramientas de trabajo de que se disponía?. Básicamente por dos razones:

1)Realmente no se necesitó el computador hasta muy recientemente
2)No se poseía la tecnología necesaria para construir un computador.

Consideremos en primer lugar la cuestión de la necesidad. En el siglo XIX, por ejemplo, no existía el automóvil, ni el avión, y en consecuencia no existía una necesidad para un control complejo del tráfico terrestre, ni de regular los vuelos para evitar colisiones aéreas. La mayoría de las universidades eran pequeñas y no se requería procesar la matrícula de por ejemplo 100.000 estudiantes. Los estados eran más pequeños, con pocos ministerios; no había seguridad social, etc. Salvo unas pocas excepciones, las empresas eran pequeñas y fácilmente controladas. Los desarrollos e inventos del hombre tienden a surgir de las necesidades humanas; realmente no inventamos aquello que no necesitamos.

Ahora volvamos nuestra atención a la tecnología. No podemos desarrollar un invento o idea sofisticada a menos que tengamos la tecnología necesaria para hacerlo. Tomemos, por ejemplo, el campo de la aeronáutica. Antes de que el avión se hiciese una máquina de uso común en nuestros días, fue necesaria la tecnología del vuelo; una tecnología personificada en los hermanos Wright en 1903. En 1969, sólo 66 años después, el hombre ha sido capaz de ir a la luna. Este tipo de desarrollo explosivo parece ser más bien la regla en lugar de la excepción. La humanidad tiene una necesidad: a menudo un conjunto de necesidades relacionadas. Entonces, un impacto tecnológico hace posible que se cubra esta necesidad. Aplicaciones de esta tecnología es normal que sugieran nuevas aplicaciones y con frecuencia conducen a una mejora de la tecnología; lo que a su vez implica usos adicionales. Es precisamente con este efecto de

realimentación positiva en forma de espiral creciente como acontecen las cosas en nuestra sociedad moderna orientada tecnológicamente.

3. LOS COMPUTADORES: SU IMPORTANCIA ACTUAL

Los computadores no son infalibles, sino que cometen errores. Aún con esto, en cualquier tarea de tipo repetitivo, su precisión sobrepasa con mucho a la de los seres humanos. Si añadimos a esta precisión su increíble velocidad, tenemos una combinación imbatible. Como resultado de estos factores se deduce que los computadores pueden realizar muchos trabajos a un coste considerablemente inferior que el hombre. Por este motivo se utilizan de forma cada vez más creciente para efectuar tareas repetitivas.

3.1 El mundo de hoy depende de los computadores

Aunque ciertamente cualquier aplicación de los computadores se puede justificar en función de la relación beneficio/coste, el hecho de que muchas funciones modernas hayan sido computarizadas, crea lo que en opinión de muchos expertos es un problema de dependencia del hombre respecto de estas máquinas.

Una historia que se escucha en los círculos de procesamiento de datos es la de aquel empleado que estaba descontento en su empresa y decide dejar su puesto de programador, pero deja detrás de sí un programa que se denomina popularmente «caballo de Troya». Esencialmente un caballo de Troya consiste en un trozo de programa bien enmascarado, que una vez que el empleado ha abandonado su puesto de trabajo, se activa y elimina una base de datos importante para la empresa, y a continuación se autodestruye sin dejar huellas de lo que pudo haber sucedido. El resultado es un caos absoluto cuando la organización intenta recuperar esos datos y descubrir exactamente qué es lo que pudo ocurrir, en un intento de prevenir una posible nueva aparición.

A consecuencia de este tremendo sometimiento de una simple tecnología, hay quienes piensan que hemos generado una situación similar a nuestra dependencia de los productos petrolíferos. El computador se ha convertido pues en el "talón de Aquiles" de muchas de nuestras instituciones modernas. La destrucción o mal funcionamiento de un programa de cálculo puede producir un paro instantáneo en organizaciones que se orientan fundamentalmente sobre el funcionamiento de estas máquinas. Quizá el caso más extremo de dependencia de

los computadores se puede encontrar en el sistema de defensa aérea de los Estados Unidos, el cual dejaría de funcionar sin su concurso.

Debido a nuestra dependencia de los computadores, la fiabilidad de estas máquinas se convierte en una cuestión crítica. Los equipos de cálculo moderno son altamente fiables. En sistemas extremadamente sensibles, tales como el sistema de defensa aéreo o el controlador de módulos espaciales, se refuerza esta fiabilidad duplicando e incluso triplicando los elementos claves. La probabilidad de que dos o tres componentes fallen al mismo tiempo es mucho menor que la probabilidad de que falle solamente uno.

Aún así, el riesgo de fallo del equipo es realmente serio. Baste recordar el todavía reciente apagón de Barcelona durante el pasado mes de agosto. La pérdida de información provocada por este suceso, trajo como consecuencia que algunas empresas tuviesen que parar su actividad un cierto tiempo. La concentración en el computador de gran parte de nuestros recursos de información pone en escena la posibilidad de un accidente potencialmente desastroso.

El riesgo de la pérdida de información y las consecuencias que de ello se derivan desde un punto de vista económico y sociológico no son los únicos problemas atribuibles a la concentración de información en la máquina. Existen también implicaciones psicológicas. Incluso nuestros políticos toman muy en cuenta la consulta que efectúan a votaciones simuladas por un computador antes de tomar determinadas decisiones.

En nuestros sistemas de gobiernos democráticos, un objetivo que se dice explícitamente es el derecho de todas las personas a recibir un mismo trato. Los seres humanos, consciente o inconscientemente, somos subjetivos, y por ello tendemos a fundamentarnos sobre leyes y procedimientos operativos, que están normalizados, estamos en cierta medida orgullosos de nuestro ideal de «un gobierno de leyes y no de hombres». Existe una separación muy sutil entre utilizar leyes y procedimientos más o menos establecidos como un medio para asegurar la administración de justicia, y confiar en estos mismos elementos como un sustituto de la propia decisión humana. Los computadores son extremadamente eficaces para asegurarnos que se realiza adecuadamente toda la burocracia de unos reglamentos. Si admitiéramos que no se necesita una interpretación de todo el papeleo que se ha generado, la máquina podría entonces (y decimos únicamente «podría») tomar la responsabilidad de administrar los reglamentos. Pongámoslo en

otros términos. Si por ejemplo un administrado simplemente «sigue el libro al pie de la letra», su capacidad de decisión se hace repetitiva y altamente predecib

Tales tareas repetitivas y predecibles se pueden programar y asignar a un computador. En otras palabras, una excesiva confianza en la regla y reglamento hace posible la automatización de la función de tomas de decisiones. Esto nos lleva finalmente a analizar ciertas implicaciones que todavía hoy día están en el terreno de la ciencia ficción. ¿Es real la posibilidad de que los computadores tomen en el mundo del mañana el papel del ser humano para tomar todas las decisiones?

3.2 ¿Será el hombre dominado por la máquina?

La posibilidad de que el computador asuma cada vez una mayor participación en la toma de decisiones hace surgir en la mente de muchos observadores una sombra más amenazadora: la de que la máquina domine al hombre y adquiera un poder dictatorial. Podemos considerar a la literatura de ciencia-ficción como una fuente inagotable de ejemplos de este temor. Quizás el ejemplo más conocido es HAL, el computador del libro de A. Clarke "2001: Una odisea en el espacio". HAL tenía virtualmente la responsabilidad completa de la misión que se describía en esta novela y una malfunción de HAL representa un viaje espacial escalofriante. En "La última pregunta" de Asimov, la fuerza mental de un nuevo universo se alberga en un computador que llega a convertirse en Dios. En gran medida, estas historias representan versiones del siglo XX del monstruo Frankenstein, que, como creación propia del hombre, se agiganta y se rebela contra él. Verdaderamente es una tema muy popular e interesante para una novela, pero ¿es real?.

En una palabra, no. Todas estas historias suponen que un computador es, en alguna medida, capaz de tener un pensamiento independiente. Unicamente si admitimos que una máquina puede pensar, podríamos argumentar que potencialmente sería capaz de dominarnos. Este es el defecto básico en todos estos relatos. Es altamente improbable que podamos enseñar a pensar a una máquina. Analicemos brevemente este problema, pues es aquí donde está el nudo gordiano de la cuestion.

¿Qué es exactamente el pensamiento?. Esta pregunta ha traído de cabeza durante siglos a pensadores y filósofos. Es la cuestión clave para determinar si es posible conseguir que una máquina piense; después de todo no podemos probar

que una máquina es capaz de hacer algo que no somos capaces de definir. Una de las primeras definiciones de pensamiento aplicada a los computadores fue el juego del ajedrez. Se razonaba para ello que, como quizás el ajedrez es nuestro juego más cerebral, un computador que se programase para jugar al ajedrez pondría en evidencia que la máquina puede verdaderamente pensar. Hoy día los computadores juegan al ajedrez y cada vez con mejor nivel. ¿Pero la habilidad de jugar al ajedrez implica realmente un pensamiento?. Consideremos que un computador con su tremenda velocidad operativa puede en efecto comparar una posición dada del tablero a miles de estrategias potenciales contenidas en el equivalente de cientos de libros de ajedrez y selecciona en cuestión de minutos el movimiento que tiene la mayor posibilidad de éxito. Esta habilidad de consultar a los expertos puede llevarlo a jugar muy bien al ajedrez, pero ¿es esto pensamiento?. Realmente, no.

Otro experimento, conocido como "test de Turing", propone el uso de tres habitaciones. En dos de estas habitaciones se albergan seres humanos, mientras que un computador ocupa la tercera. A los tres participantes se les indica un determinado tema de conversación y se les permite comunicarse con los otros dos de una forma totalmente libre, a través de un terminal. Después de algunos minutos de conversación, se les pide a los dos seres humanos que identifiquen cuál de los otros dos compañeros era la máquina. Simplemente en razón del cálculo de probabilidades (la misma que al arrojar una moneda al aire para adivinar si es cara o cruz) es de esperar que den la respuesta correcta la mitad de las veces. Si los dos seres humanos no son capaces de hacerlo significativamente mejor, pues identifican al computador la mitad de las veces se podría inferir que éste tenía pensamiento. Incluso si el experimento resultase satisfactorio, ¿se probaría con ello que la máquina puede pensar?. ¿Es la capacidad de mantener una conversación todo lo que se necesita para pensar?. Rotundamente no; existen otros ingredientes.

Los seres humanos tenemos la capacidad de imaginarnos muchas más cosas que una simple ristra de ceros y unos; nuestra memoria, nuestro proceso pensante no es lineal. Por el contrario nuestra mente es multidimensional, es asociativa en el sentido de que una imagen nos permite recordar otras. Podemos imaginar. Podemos planificar. Podemos crear. Tenemos una intuición que desafía toda definición precisa. Todos éstos son componentes del pensamiento. Sin ellos no podemos decir que una máquina verdaderamente piensa.

Un gran número de investigadores están investigando en la actualidad sobre cómo programar los computadores para que presenten un comportamiento en apariencia inteligente. Esta área de investigación se denomina inteligencia artificial. Su objetivo final es crear una máquina inteligente. Sin embargo, estos objetivos no son los del Dr. Frankestein, sino que, en el fondo, lo que les preocupa y motiva es definir exactamente que se entiende por inteligencia.

Hay dos maneras de enfocar el estudio de las relaciones entre la conducta de una máquina y la de los seres vivos. Un grupo de investigadores comienzan su trabajo con la mente humana. Estos científicos analizan de forma exhaustiva la mente, intentando definir de manera precisa qué es lo que acontece cuando pensamos. Su objetivo realmente es copiar la mente humana; el computador en este caso, se utiliza fundamentalmente como una herramienta de trabajo para modelar sus hipótesis. Otro grupo de investigadores empieza con la propia máquina. Intentan modelar sobre la maquina lo que ellos estiman que son los distintos atributos del pensamiento humano, y a continuación compueban la bondad de sus modelos cuando se les compara con la realidad.

En ambos casos, la finalidad es esencialmente la misma; se desea obtener una mejor comprensión de los esquemas que sigue el pensamiento humano. Porque, en definitiva, comprender la naturaleza del pensamiento significa comprender que es lo que hace únicos y superiores sobre la tierra a los seres humanos. Es ésta una zona de apasionantes interrogantes científicos.

Una de las conjeturas más interesantes de la ciencia-ficción defiende la posibilidad de vida basada en el silicio. La vida humana, de hecho, todas las formas de vida en nuestro planeta se basan en un número de compuestos muy complejos formados en torno al átomo de carbono. Se pueden crear compuestos análogos tomando como núcleo al átomo de silicio. Tales compuestos podrían, al menos en teoría, soportar vida. Por supuesto, esto nunca se ha hecho, pero la posibilidad de una vida basada en el silicio es ciertamente intrigante. Desde estos balbuceantes fundamentos científicos, se puede vislumbrar el comienzo de una historia de ciencia-ficción en los términos siguientes: la humanidad al ir creando cada vez circuitos más complejos que tienen como base el silicio, ha comprimido el equivalente a millones de años de evolución basados en el silicio en unas pocas décadas. Rapidamente se alcanza una masa crítica y un computador desarrolla su propia conciencia. Al principio lentamente, luego de forma acelerada esta primera "semilla" despierta en otras máquinas. Mientras tanto, el hombre que depende cada vez más de sus sirvientes electrónicos, no advierte esta nueva y creciente

amenaza a su dominación. Entonces un día, en el espacio de unos pocos microsegundos, el computador se rebela y domina al hombre. La humanidad ha sido suplantada por el siguiente eslabón de la cadena evolutiva. Hay justamente bastante validez científica en esta historia como para permitir sorprender la credibilidad del lector y que este pueda decir "podría ser". ¿Es probable que tal cosa suceda?. Sinceramente, pensamos que no.

Para muchos el computador es la personificación de un nuevo mito. El computador es nuestra creación que controla muchos aspectos de la vida humana. El hombre es responsable de controlar sus creaciones y para controlar debe primeramente comprender. ¿Recuerdan al perverso computador HAL en "2.001 una odisea en el espacio"?. HAL falló, lo cual implicaba unas consecuencias desastrosas, sin embargo el hombre fue todavía capaz de penetrar en la habitación que contenía los circuitos de memoria de la máquina para desactivarlo. Al menos es casi seguro que cualquier computador del futuro incorporará, aunque sea mínimamente, un cierto nivel de control humano. A pesar de nuestra tendencia general de entronizar más y más estas máquinas, la idea de un computador completamente independiente, no sujeto al control directo del hombre, es improbable que gane mucho apoyo.

El peligro real es la posibilidad de que algún hombre o grupos de hombres puedan llegar a controlar el poder político, escondiéndose detrás del mito: la creación del hombre se enfrenta contra el hombre. No sería la primera vez que un grupo de seres humanos usa una combinación de conocimientos y mitología cuasi religiosa para asentar su poder. Hoy día, por ejemplo, no aceptaríamos un líder, cuyo mérito real para detentar el poder fuese, por ejemplo, su capacidad para predecir la llegada de la primavera. Los antiguos egipcios así lo hicieron, pero hoy sabemos que el ciclo de las estaciones está simplemente relacionado con la rotación de la Tierra alrededor del Sol. Quizás, si bastantes de nosotros sabemos que un computador no es ni más ni menos que una máquina, podremos evitar el peligro de caer en las garras de algún apostol de los computadores. Como casi siempre, educación y formación son las claves para controlar el problema.

3.3 Los computadores: Un reto y una esperanza en nuestra sociedad

Los problemas con los que hoy día se enfrenta el mundo occidental: políticos, ecológicos, económicos, urbanísticos, raciales, etc., a pesar de que

algunos de ellos se han originado por la propia tecnología, únicamente se podrán resolver (si ello es posible) mediante nuevas aplicaciones de la ciencia y de la tecnología. En este sentido, ninguna tecnología ofrece más potencial, más esperanza en la solución de estos problemas que los computadores. Pero, por otra parte, tampoco hay otra tecnología que plantee más amenazas a la actuación de los gobiernos que los propios computadores. Esta complementariedad del bien y del mal es común a otros ejemplos de la ciencia y la tecnología. La energía nuclear y la genética molecular son otros dos casos obvios y como con los computadores, nuestro desafío es resistir la amenaza sin perder la confianza.

Un análisis de los efectos de los computadores sobre la sociedad depende del reconocimiento de que la ética en casi todas las circunstancias tiene un cierto sentido relativo y no absoluto o, como se ha dicho, «la ética de un acto es una función del estado del sistema en el momento en que se realiza». El biólogo G. Hardin ha dado un ejemplo sencillo de esto. Hace 150 años, en el oeste americano, uno podía matar un búfalo, cortarle la lengua para prepararse una suculenta comida con ella y abandonar el resto del animal sin que ello fuese considerado punible. Hoy en día, con el búfalo americano en peligro de extinción, este tipo de conducta nos aterraría.

Es importante hacer esta puntualización porque creemos que es esencial analizar la ética de utilizar el computador en la sociedad, en el contexto del mundo tal y como es y no cómo nos gustaría que realmente fuese. De forma general, los últimos 200 años han visto un incremento y desarrollo en la libertad personal de los ciudadanos de países que tenían regímenes democráticos (simultáneamente, por supuesto, ha existido un aumento en la efectividad de los gobiernos de carácter totalitario). Este aumento de libertad ha escondido el hecho de que el potencial para una mayor libertad personal ha ido disminuyendo en el último milenio. En la Edad Media existía muy poca libertad individual excepto para una minoría muy pequeña; sin embargo, al menos en teoría, hubiera sido posible una mayor cantidad de la misma a causa de la relativa falta de interrelación y complejidad dentro de la estructura social. Realmente podemos mirar el aumento de las libertades individuales como dándole al pueblo aquellos bienes -lengua, religión, asociación, etc. que el hombre medieval no tenía, debido a la forma en que su sociedad estaba organizada.

Paralelamente a este aumento de libertades básicas, la mayoría de las cuales se engloban en los países occidentales en sus leyes de tipo administrativo, ha habido, sin embargo, una disminución de la libertad en otros aspectos. Las

personas no somos libres de conducir nuestro coche como nos dé la gana o de quemar cualquier clase de combustible, por citar dos ejemplos. Las leyes administrativas son el precio que pagamos por la complejidad creciente de la vida misma, que se acrecienta en esta fase final del siglo XX. Complejidades urbanísticas, sociales, ecológicas y políticas demandan, si realmente queremos tener un planeta habitable, un cuerpo cada vez más amplio y rígido de leyes administrativas. El resultado inevitable es una restricción gradual de las libertades personales en el supuesto interés de toda la sociedad. La cuestión no es si se debe restringir la libertad sino cuánto y en qué áreas. Entender esto es crucial para fijar la contribución de los computadores en el mundo de hoy y de mañana

Los computadores se pueden utilizar para restringir las libertades personales. De igual manera resulta incuestionable que deberán utilizarse si deseamos controlar mejor que ser controlados por los problemas que acucian a la humanidad. La cuestión importante es decidir cuáles son las aplicaciones apropiadas y cuáles no, y qué se puede hacer para salvaguardar la libertad personal en aquellas que sean necesarias. Por ejemplo, si se desea controlar la explosión de población, puede (decimos «puede») ser necesario tener una información muy precisa y completa sobre el tamaño de las familias, sobre los abortos e incluso tal vez sobre los hábitos contraceptivos de la población. Obtener tales datos se puede considerar una invasión injustificada de la intimidad, pero si se garantiza ésta pueden resultar esenciales. Es imposible hacer un uso razonable de tales datos sin el empleo de los computadores, por lo que éstos tendrán que utilizarse de manera que garanticen la intimidad personal como un presupuesto para asegurar la libertad personal.

3.4 El derecho a la intimidad personal: ¿Representa un peligro el computador?

¿Pero realmente se puede asegurar la intimidad de tales bases de datos?, y si así fuera, ¿compensaría ésto los grandes costos?. Y si no, ¿significa esto que no podemos reunir estos datos, aun cuando sean muy grandes las necesidades de la sociedad?. Estas preguntas intentan únicamente indicar algunos aspectos del alcance general del problema.

Es célebre la frase de Francis Bacon "conocimiento es poder". La información es la materia prima del conocimiento. Si el disponer de información es una fuente de poder, se sigue fácilmente que aquellos que deseen alcanzar algún tipo de poder utilizarán la información para conseguir sus objetivos. Esta

información se puede usar de forma correcta o incorrecta según los fines que se persigan. Realmente esto no es un problema nuevo. Lo que sí resulta novedoso, sin embargo, es la posibilidad de concentrar mucha información en un computador. No es que realmente exista más información, es justamente que el computador nos hace mucho más fácil la tarea de almacenar, procesar, interrelacionar y recuperar la gran cantidad de información que se necesita para mantener en funcionamento nuestra sociedad actual.

La información es esencial a todos los estratos de nuestra sociedad y no podríamos estar a nuestro nivel actual sin ella. Es, pues, importante darse cuenta del valor que en sí mismo posee toda información. En el libro de F.W. Winterbotham, "El ultrasecreto", se cuenta la historia del robo por parte de los británicos, a comienzo de la segunda guerra mundial de un dispositivo alemán de alto secreto para la descodificación de mensajes. Usando este dispositivo, los aliados fueron capaces de descodificar rapidamente comunicaciones secretas de los alemanes, que les daban indicaciones de los planes y estrategias germanas casi tan pronto como éstas se producían. Hay quienes opinan que esta información fue fundamental en la victoria de los aliados.

¿Y qué podemos decir de la información a nivel personal?. Gran parte de nuestra forma de vivir se asienta y controla por la posibilidad de disponer en forma rápida de informaciones personales. Vivimos en una sociedad orientada al crédito, y ¿qué puede ser más importante que nuestro propio margen de crédito?. Un margen de crédito es, pues, pura información que contiene un valor muy significativo para el individuo. Al estar inmersos en una sociedad cada vez más informatizada, se va almacenando cada vez más y más información sobre nuestras vidas en los bancos de datos. Si bien es cierto que sólo los computadores nos pueden liberar de vernos aprisionados por la vorágine de la burocracia, no es menos cierto que aumenta también el número de personas que están muy preocupadas al ver que esta gran masa de datos escapa a su propio control y puede hacer que sus vidas se vean coaccionadas, debido al mal uso que hagan terceras personas de sus registros.

Nadie duda que los computadores y los bancos de datos son elementos esenciales para una gestión eficaz de nuestra sociedad actual, pero también casi todo el mundo piensa que esta eficacia no se debe comprar a un precio tal que incluya las libertades individuales. Aparece así claramente un dilema entre la necesidad real de disponer de información y el derecho de las personas a salvaguardar su intimidad personal. En los países industrializados este problema

ha sido reconocido por sus Parlamentos que han aprobado "leyes sobre la intimidad". El objetivo de dichas leyes es poner límites a los gobiernos, instituciones y empresas para proteger la libertad de las personas, estableciendo barreras a los abusos que de su poder éstos puede hacer para investigar y almacenar información.

Cuando hoy día se habla de información en este sentido, estamos casi por definición hablando de computadores. Los computadores son el almacén moderno de información (o de los datos utilizados para generar esa información). Practicamente no existe hoy día ningún banco de datos independiente de un computador. Desgraciadamente el computador también hace más facil que se pueda hacer un mal uso de la información almacenada. El simple hecho de que toda esta información esté concentrada en un lugar simplifica en gran medida la aparición de un cierto tipo de espionaje electrónico.

¿Es real en nuestra sociedad democrática el riesgo de que se realice un mal uso de determinadas informaciones?. Consideremos por ejemplo, en el mundo de la política, la divulgación de determinadas informaciones negativas de un cierto candidato, o los rumores de que ciertos lideres políticos son capaces de mantener su posición de poder privilegiada en virtud de que conocen ciertas cosas de otros líderes. No hay que inferir de esto, por supuesto, que el disponer de información sea algo íntrinsecamente negativo. Sistemas computarizados nos ayudan a perseguir a los delicuentes, a recuperar tarjetas de crédito y otras propiedades que nos han sido robadas. Únicamente con información pueden gestionarse y controlarse nuestras grandes organizaciones gubernamentales, educativas y empresariales. A nivel más personal, las historias clínicas de cada uno de nosotros son un elemento valiosísimo en cualquier sistema sanitario, y una historia clínica, obviamente, no es nada más que información. Se podría continuar citando todos los ejemplos que sobre el uso de los computadores hemos ido presentando y en todos ellos el punto común es el siguiente: la información es esencial. La eliminación de los bancos de datos no parece ser la solución.

Controlar las ventas de armas, una de las cuestiones más controvertidas estos ultimos años, nos da un ejemplo del uso legítimo de una base de datos en contraste con el mal uso potencial de los mismos datos. Aquéllos que están a favor de dicho control argumentan que una base de datos que mantenga un registro de las ventas de armas limitará su uso con fines delictivos ya que: a) da a los vendedores de armas una fuente centralizada de consultas antes de vender una, b) la policía puede conocer posibles violaciones antes de conceder una

licencia c) se facilita a la policía el poder seguir la pista de un arma sospechosa. Por su parte, los que argumentan en contra, además del hecho real de que hay un derecho constitucional (en los Estados Unidos) que les ampara para comprar armas, expresan su inquietud sobre la posibilidad de que algún futuro Hitler utilice tal lista de propietarios de armas como un mecanismo para eliminar cualquier intento de revolución armada. Ambas posturas son muy dignas de tener en cuenta.

En la actualidad nuestro problema realmente es el de intentar equilibrar las necesidades de la sociedad desde un punto de vista global con los derechos individuales. No se pueden eliminar los sistemas de información computarizada si no es a costa de retroceder hasta el siglo XIX, y a pesar de los problemas reales que se han bosquejado en términos generales, la sociedad no está deseando pagar el precio de un retroceso de este tipo. ¿Qué podemos hacer?. Básicamente podemos conocer el problema.Conocer un problema es el comienzo para tratar de encontrar una solución. Podemos insistir en que nuestros representantes políticos consideren el impacto de cualquier nuevo sistema de información que se propongan. Podemos retirarle nuestro apoyo si sus argumentos para tales sistemas no son sólidos. Podemos rehusar hacer negocios con organizaciones que parezcan dar un mal uso a sus datos. Podemos exigir pruebas convincentes de que cualquier nueva aplicación que se proponga es realmente necesaria. Y podemos, finalmente, insistir para que nuestros gobiernos mejoren la legislación que protege nuestro derecho a la intimidad personal.

3.5 Una nueva forma de delito: El delito informático

Los computadores se utilizan hoy día para procesar la mayor parte de nuestras transacciones bancarias. Las actividades del mercado de valores, el pago de nóminas y los registros de inventarios entre otras cuestiones se realizan y se controlan con estas máquinas. Para una persona con poca o ninguna experiencia en computadores los registros de estas transacciones están tan bien guardados como si estuviesen en la bóveda más inexpugnable. No obstante para el experto en computadores, la información binaria que estas máquinas almacenan en su memoria es muy fácil de manipular. El simple hecho de que hoy día una gran cantidad de dinero se represente nada más que como una ristra de ceros y unos en un computador pone un blanco muy tentador para una nueva clase de delincuente: el delincuente informático.

Vemos así claramente cual es el tipo de trabajo del "caco informatico": tiene que alterar los números almacenados en la memoria del computador de tal manera que él se vaya haciendo cada vez más rico, y de forma que ninguna otra persona note que, a su vez, se va haciendo cada vez más pobre. Analicemos brevemente algunas formas de cómo la gente ha utilizado esta simple idea para su propio aprovechamiento.

Un delito frecuente es el desfalco (manipular los libros de una entidad con objeto de conseguir dinero para uno mismo). Un caso en el que se usó el computador para realizar un desfalco fue el de un cajero jefe que trabajaba en un banco de Nueva York. Su trabajo consistía en utilizar un terminal del computador para examinar los balances de los clientes, efectuar auditorías de los cajeros que estaban a sus órdenes corrigiendo los errores que estos podían cometer. Pero además de efectuar estas funciones, utilizaba el terminal para malversar miles de dólares. Su estrategia era muy simple. Examinando los informes que recibía normalmente del centro de cálculo del Banco, era capaz de detectar un conjunto de cuentas inactivas, es decir, cuentas que en los últimos meses no habían generado ningún tipo de movimiento. Mediante su condición de cajero jefe procedía a transferir unos cientos de dólares de una cuenta inactiva a la suya. Si posteriormente el cliente de la cuenta advertía e la discrepancia y se lo notificaba al Banco, la queja era, por supuesto, dirigida al cajero jefe quien cargaba la culpa al inevitable error humano en el manejo de tantas cuentas. Más tarde hacía una transferencia desde otra cuenta inactiva a la del cliente que había hecho la reclamación por la cantidad que había sustraido. ¿Como se descubrió el desfalco?. Nuestro personaje era un jugador de apuestas que pensaba tomar prestados estos fondos y más tarde reponerlos con sus ganancias. Como sucede muy a menudo, las pérdidas fueron haciéndose cada vez más cuantiosas y tuvo necesidad de aumentar el número de la cuentas inactivas de las que sustraía dinero. La tarea de mantener un control de las transacciones que llevaba a cabo sobre el terminal empezó a consumir un gran porcentaje de su tiempo. Finalmente, fue descubierto. Lo paradójico de esta historia es que fue descubierto por casualidad cuando la policía de Nueva York detuvo a un apostador profesional y a través de éste supo que el cajero, cuyo sueldo era de sólo 40.000 dolares al año, venía apostando semana tras semana unos 30.000 dolares.

Otro caso está relacionado con los errores de redondeo y de truncación de una cantidad. Todos hemos aprendido en la escuela la regla básica para redondear. Supongamos, por ejemplo, que queremos calcular el pago de intereses que corresponde a una cuenta corriente y que queremos dar el resultado con una

cifra decimal. Si el resultado es 237,57 ptas, redondeamos por exceso a 237,6 ptas; Si por el contrario fuera de 237,52 ptas redondearíamos por defecto a 237,5 pesetas. La clave está en el segundo dígito decimal Si es 5 o más redondeamos por exceso y, si no, por defecto. Existe una forma alternativa de realizar esto: la truncación. Utilizando una regla de truncación, 237,57 ptas se convierte en 237,5 ptas; simplemente eliminamos el dígito extra. Con el redondeo, algunas veces aumentamos el número y otras lo disminuimos, consiguiéndose que, en promedio el resultado esté nivelado. Con la truncación, sin embargo, siempre disminuimos el valor.

Esta consideración puede parecer que carece de importancia. ¿Después de todo qué interés puede haber en tener una fracción de unos céntimos?. De forma individual, estamos perfectamente de acuerdo. ¿Pero qué díriamos de una entidad bancaria que maneja cientos de miles de cuentas?. Hubo una vez un programador que reconociendo este hecho intentó sacar un beneficio propio de él. Para ello abrió una cuenta en el banco en el cual estaba escribiendo un programa de cálculo de intereses de las cuentas bancarias. Diseñó el programa para acumular todas las fracciones truncadas de los céntimos de dolar y añadirlos a su propia cuenta al final del programa. Como el Banco calculaba los intereses trimestralmente, cada tres meses se encontraba con unos "beneficios" por este concepto de algunos centenares de dólares. Finalmente, un perspicaz sensor de cuentas descubrió el delito.

Muchas veces parece que los delitos informáticos sólo se llegan a descubrir como consencuencia de algún accidente y no como resultado de las medidas de seguridad que contiene el programa. Por esta causa, muchos especialistas estiman que se pueden haber cometido hasta diez delitos informáticos por cada uno que se descubre. Puede incluso que hayan robos de miles de dólares que aún no han sido descubiertos. Hemos visto como para el profesional en informática es sencillo manipular cientos de miles de dólares simplemente cambiando unas pocas de instrucciones en un programa que le permiten transferir fondos de una cuenta a otra. No es necesario asaltar un Banco y amenazar al cajero con una pistola. De hecho, el acto del hurto informático lleva consigo poco más que una actividad mental.

Lo que es incluso más importante es el hecho de que sólo una pequeña parte de nuestra población es capaz de reconocer que se ha cometido un delito. No existen cuerpos, ni cajas de seguridad asaltadas, ni fotos sacadas por las cámaras del servicio de seguridad del Banco. En su lugar, todo lo que queda para

probar que se ha cometido el delito son unos pocos "1´s" que deberían ser "0´s" y unos pocos "0´s" que deberían ser "1´s". Nada puede ser más fácil y el riesgo es mínimo.

Un programador hábil puede diseñar un programa de manera que no quede ni rastro de una actividad ilegal al destruirse después de unos pocos microsegundos las instrucciones del programa que generaban dicha actividad. ¡Imagínese como detective, intentando probar un delito que tiene lugar en un instante y que luego desaparece sin dejar huellas!. El delito informático es pues muy difícil de detectar.

4. LOS COMPUTADORES: SU IMPACTO SOCIAL

Las tecnologías de la información (electrónica, telecomunicaciones e informática) han creado una profunda interrelación entre el grado de formación de una sociedad y sus cotas de bienestar económico. Existen suficientes evidencias que demuestran que el crecimiento económico y la competitividad de las economías líderes depende muy fundamentalmente del potencial que posean para innovar sus productos y procesos. Esta capacidad se basa en último témino en una elevada cualificación profesional de sus individuos. En una economía que trasciende cada vez más los límites nacionales resulta prioritario que seamos capaces de desarrollar al máximo nuestra formación para tratar de mantener la competitividad con el resto de los países avanzados. La tecnología de forma genérica es pues un mecanismo potente para el crecimiento de la economía y la transformación de la sociedad, y en este sentido tiene que considerarse como una de las fuerzas básicas de la civilización moderna.

4.1 Computadores y empleo

Desde un punto de vista macroscópico el objetivo de la tecnología puede reducirse a una de las dos alternativas siguientes:

1)Efectuar trabajos convencionales con menos esfuerzo y a un coste más reducido

2)Realizar nuevas tareas que hasta la fecha hubieran sido física o económicamente inviables sin la introducción de la nueva tecnología

En el primer caso, la tecnología es un elemento generador de desempleo, reduce la mano de obra que no necesita e intenta optimizar los recursos económicos puestos en juego. Por el contrario,en su segundo aspecto, la tecnología es creadora de puestos de trabajo, y nadie puede cuestionar que es la única forma de conseguir que, por ejemplo, la población actual de un continente como el europeo esté alimentada y tenga unos niveles de trabajo aceptables. Un ejemplo de esta dualidad en la creación-aniquilación de puestos de trabajo, fue la aparición de la máquina de escribir. Ciertamente eliminó el oficio de escribano, pero su número no era ni mucho menos comparable con el de secretarias y mecanógrafas de hoy día. Desde nuestra perspectiva actual nos parecería sin sentido un planteamiento sociológico de tipo pesimista que hubiese objetado la irrupción de la máquina de escribir como un peligro potencial por la eliminación de determinados tipos de trabajo.

El temor de poder ser reemplazado por un computador es muy común y está muy extendido, particularmente entre aquellas personas que realmente no entienden estas máquinas. Hemos estado mostrando los conceptos básicos y algunas aplicaciones de los computadores. ¿Qué tenían en comun todas las aplicaciones en las que los computadores reemplazaban al trabajo humano?. Básicamente cualquier aplicación de los computadores debe consistir en una serie de pasos bien definidos que se repiten muchas veces. Sin el factor "muchas repeticiones" puede resultar económicamente inviable una solución basada en el uso de los computadores.

¿Es repetitivo su trabajo?. La tarea de escribir un libro, por citar un ejemplo, casi con toda certeza no podrá ser efectuada por los computadores, simplemente porque dicha tarea no puede programarse. El término automatización se utiliza para describir la sustitución del hombre por la maquina. Vista de esta forma, cualquier forma de automatización obviamente elimina puestos de trabajo. Si nos preguntasen si los computadores eliminan puestos de trabajo, debemos contestar que, por supuesto, dicha afirmación es cierta. Sin embargo, esto es una verdad a medias, como vamos a tratar de justificar.

Consideremos la máquina de vapor. Cuando se inventó, se temió que originase un gran desempleo, al representar una alternativa de bajo coste frente al esfuerzo muscular del hombre. La máquina de vapor hizo posible la revolución industrial y originó una multitud de nuevos tipos de empleo. El francés Jacquard desarrolló en el siglo XIX un telar automático controlado por una serie de tarjetas perforadas, precursoras de las que posteriormente se utilizarían en los primeros computadores. Esto originó en Francia riadas de protestas por parte de los obreros de la industria textil. Sin embargo, su aparición permitió a esta industria

ofrecer sus productos a unos precios mucho más asequibles, lo que originó un aumento de la demanda y en definitiva un incremento más que un descenso en el empleo. La imprenta eliminó la necesidad de copiar libros a mano, ¿pero tendríamos una industria del libro sin la invención de la imprenta?.

La historia de la tecnología está repleta con ejemplos similares. Al principio, un nuevo impacto tecnológico hace sentir el temor de que se eliminará gran cantidad de empleo. Quizás a muy corto plazo esto sea así, no obstante cuando la innovación comienza a tomar cuerpo se crean nuevos puestos de trabajo para soportar la nueva tecnología. Invariablemente, esta nueva tecnología permitirá realizar tareas que previamente eran imposibles, creando así nuevos puestos de trabajo. Este proceso de avance tecnológico es el elemento clave en el desarrollo de nuestra economía. ¡Sin tecnología, probablemente hoy dia seríamos cazadores como nuestros antepasados!. Los computadores han tenido un impacto análogo. Es evidente que se han eliminado algunos puestos de trabajo. La reducción en el coste fue la justificación original para usar estas máquinas. En una reciente relación de las 50 compañías más grandes de la industria americana el número de personas trabajando directamente en el sector superaba ya el millon y medio de personas.

Sin los computadores no habría habido programa espacial ni la gran mayoría de las actividades de relieve que se han efectuado en los ultimos tiempos. ¿Cuántas personas han conseguido su empleo de forma directa o indirecta a través de este esfuerzo?. La gran demanda de computadores ha creado una tremenda necesidad por una serie de servicios relacionados que han conducido a un crecimiento en la actividad educativa en estos temas, la aparición de sociedades de servicios en estos temas de informática, etc.

Existe otra consideración, muchas veces no tomada en cuenta, del impacto de una innovacion tecnológica sobre el mercado del empleo. ¿Podría haber crecido nuestra economía a su tamaño actual sin ella?. Muchos expertos creen sinceramente que, sin los computadores, hace años la banca que se habría ahogado en sus propios papeles. ¿Podría cualquier empresa moderna haberse desarrollado hasta su estado actual sin que los computadores manejen sus necesidades de procesamiento de datos?.

Podemos decir, pues que, un impacto secundario de la automatización es el crecimiento. Los recursos liberados por automatizar ciertas funciones se pueden invertir en otra parte y la inversion es el mecanismo mediante el cual crece nuestra economia y se crea más empleo. Parece así obligado el argumento de que los computadores han creado más puestos de trabajo de los que realmente han eliminado.

De forma general, las tareas eliminadas por los computadores y otras máquinas automáticas tienden a ser altamente repetitivas y tediosas. Por consiguiente la automatización nos libera del trabajo rutinario permitiendo que nos dediquemos a aquellas tareas más en consonancia con nuestra condición de seres inteligentes. Esto crea un problema con el empleo de los computadores (de hecho, con todas las formas de automatización) y es que tiende a destruir empleos de baja cualificación, mientras, al mismo tiempo crea puestos altamente cualificados. Esta es la cuestión relevante en el momento actual, la automatización tiende a eliminar las tareas de aquellas personas que son más difíciles de reentrenar y adaptar a causa de su baja cualificación. La solución a este problema, como a tantos otros, pasa ineludiblemente por la educación. Una sociedad con una educación integral de todos sus ciudadanos puede mirar el problema con optimismo. Japón ofrece en la actualidad un ejemplo aleccionador sobre este campo. Los masivos programas de automatización en la industria japonesa han sido perfectamente asimilados por sus obreros gracias a unos ambiciosos programas de reciclaje del obrero japonés que le han permitido efectuar, sin ninguna clase de trauma un desplazamiento en su tipo de trabajo.

4.2 El desfase en la formación de los individuos como consecuencia del cambio tecnológico.

Tratemos, pues, de analizar el problema desde la perspectiva de la formación y tomemos para ello otra vez el ejemplo anterior de la aparición de la máquina de escribir. Una persona cuya cualificación básica era la producción de documentos caligráficos sentirá poco consuelo cuando escuche que se produce un aumento de empleo con la introducción de la máquina de escribir. ¿Dónde está, pues, el fondo de la cuestión?.

Básicamente, en la velocidad de transición hacia las nuevas tecnologías y en el desajuste que necesariamente se va a producir cuando tienen que coexistir con aquellos otros medios productivos a los que de una manera inexorable van a desplazar. Cuando las nuevas tecnologías se desarrollan a una velocidad tal que las tareas obsoletas mueren a un ritmo similar al que establece la jubilación de sus operarios, únicamente será suficiente un esfuerzo educativo modesto para mantener el equilibrio profesional. Hoy día las cosas no suceden de esta forma y durante la vida activa de un trabajador se producen cambios sustantivos que afectan tanto al fondo como a la forma de realizar una tarea de forma que ni siquiera un óptimo sistema educativo puede bastar para compensarlo. Este acortamiento del ciclo: desarrollo científico _ innovación tecnológica _ proceso productivo plantea el problema del impacto social que produce un avance tecnológico acelerado y sin un cierto grado de control por parte de todos los

agentes que intervienen en el problema. Parece, pues, razonable analizar con todos los sectores responsables e implicados lo que verdaderamente se puede hacer.

Hay aún un segundo efecto que agrava el primero y es el de la deshumanización que la división y abstracción de las tareas está llevando al lugar de trabajo. Un artesano medieval producía artículos a partir de materias primas que él mismo trataba o que compraba a personas a las que conocía muy bien, y a su vez vendía la mayoría de sus productos a gentes que estaban próximas a su entorno vital. Por el contrario, en la tecnología moderna, la distancia entre suministradores, productores y usuarios está aumentando de forma continuada, y las tecnologías de la información agravan aún más esta tendencia. El lugar de trabajo tiende a ser una rendija estrecha a través de la cual es casi imposible ver el producto completo. En un gran sistema de procesamiento de información ninguna persona, de forma aislada, conoce todos los detalles. A este problema del desajuste de la formación de los individuos, como consecuencia del rápido cambio tecnológico, es al que debe dar respuesta para su solución la propia tecnología. Tiene pues pleno sentido desde estas consideraciones hablar del binomio formación y tecnología.

4.3 Impacto tecnológico en los países en vías de desarrollo

El procesamiento de información una y otra vez pone de manifiesto que la perfección es un concepto idealista, que va bien para los modelos a escala de laboratorio, y es una necesidad para las formalizaciones matemáticas y lógicas, pero resulta inútil en un mundo en el que la imperfección humana es la norma. El computador, considerado como máquina de procesamiento de información de alta velocidad, tiene una propiedad muy reconfortable: nos hace ver los peligros antes de que se produzcan realmente; de manera que es posible observarlos, describirlos, modelarlos y analizarlos cuando aún se está a tiempo de solucionarlos.

Para los países en vías de desarrollo el impacto tecnológico y social es esencialmente el mismo, únicamente que puede ser mucho más fuerte y arriesgado; y tan pronto como los computadores comiencen a multiplicarse, las consecuencias se pueden desarrollar de forma más rápida. Esta aceleración podría no ser tan buena como a primera vista pudiera parecer. El computador no es un amigo natural del desarrollo de los pueblos, y una gran parte de los actuales intentos de aceleración es más que cuestionable. El computador puede convertirse en una herramienta muy útil para los países en vías de desarrollo si se aplica con cuidado y paciencia, con comprensión y disciplina. Cierto tipo de información

puede adelantar el desarrollo y ayudarlo; sin embargo, la mayor parte de la información puede únicamente ser una consecuencia del desarrollo

En otras palabras, es difícil ayudar, y mucho más hacerlo por medio del tratamiento de la información. A las mejoras por las facilidades tecnológicas pueden seguir fácilmente daños irreversibles en la sociedad en la que se inserta. El impacto social y tecnológico del procesamiento de la información se traduce en cambios en los productos y en los métodos de trabajo, de una parte, y en las tareas que realizar y en el grado de satisfacción del trabajador, de otra. Una tecnología y una cooperación adecuada en su gestión entre las organizaciones empresariales y los sindicatos basada en la realidad de la situación del trabajo y la experiencia obtenida por especialistas en informática y sociología permitiría encontrar un camino que, aunque no pueda evitar totalmente ciertas penurias, a largo plazo posibilitaría soluciones aceptables a un costo razonable.

4.4 Computadores y lenguaje

Existe también un impacto que va más allá de los detalles científicos, tecnológicos y sociológicos: el producido sobre la mentalidad y filosofía de todos los pueblos que trabajan o están influidos por el procesamiento de la información. Un análisis en profundidad de esta incidencia está fuera de nuestro alcance. No obstante, seleccionamos algunos aspectos con el fin de caracterizar el problema.

Tomemos el lenguaje como una de las manifestaciones distintivas del ser humano y consideremos las posibles influencias sobre la mentalidad de un ciudadano típico. La investigación científica del lenguaje ha demostrado que no existe una frontera inferior al concepto de lenguaje; la teoría cubre cada nivel desde los sistemas basados en signos extremadamente primitivos hasta las posibilidades más sutiles del lenguaje humano y, por supuesto, todas ellas pueden aparecer en el contexto de los computadores.

La teoría científica del lenguaje distingue entre diversos niveles de importancia creciente: sintaxis, semántica, pragmática etc. La sintaxis es el estudio de la disposición de los símbolos y las palabras; las reglas para construir expresiones bien formadas. El computador es la herramienta ideal para la operación sintáctica de los caracteres, ya que puede verificar la corrección de la entrada recibida y de la salida producida. La semántica es el estudio de las relaciones entre el texto y los objetos designados y descritos por el mismo, es decir, entre la descripción y su realidad. La corrección de la semántica no puede computarse, debe verificarse frente a la realidad, lo cual requiere la mente humana. Por lo tanto, la verificación no puede ser automatizada totalmente, y

habrá siempre un vacío entre cualquier estructura formalizada y la naturaleza viva de la mente humana.

El lenguaje refleja y contiene las infinitas posibilidades del pensamiento humano, mientras que las estructuras formales que son los modelos con los que puede operar el computador claramente son de una naturaleza finita. El sistema es más que la suma de sus partes debido al flujo de información entre los subsistemas. Una palabra es más que la secuencia de sus letras, a causa del significado que se asocia a éstas, y de su relación con otras palabras y con la realidad a la que se refiere. Este universo de relaciones se puede simbolizar mediante una nube que pende de cada elemento del texto y que parece distinta a diferentes personas. El computador no procesa la nube, solamente transforma cadenas de caracteres.

4.5 ¿Hacia un nuevo orden algorítmico?

De la misma forma que podemos convertir ciertas relaciones naturales y artificiales en expresiones matemáticas, también se pueden traducir ciertos aspectos y estructuras de la realidad en modelos formales. Ha costado tres siglos, desde comienzos del Renacimiento, que las matemáticas alcancen el universo de la ciencia, tecnología y economía actual. Estamos justamente comenzando a desarrollar modelos que van más allá de lo que habíamos formalizado desde el Renacimiento, y necesitaremos algo de tiempo para reunir experiencias en estas nuevas áreas, para reconocer y respetar sus limitaciones. El optimismo desmesurado no es útil, tal como ha demostrado el relativo fracaso de los computadores en el proceso de traducción de lenguajes naturales; un fracaso, por otra parte, fuertemente ignorado por los superoptimistas. Pero cualesquiera que sean los problemas que puedan surgir, el objetivo será almacenar un modelo tan perfecto como sea posible en la memoria del computador, porque entonces y sólo entonces se podrá aplicar y disfrutar de todas las posibilidades del procesamiento de información.

Cualquier cosa fuera de este universo orientado hacia el computador no solamente será costoso sino que resultará extraño. ¿No es posible que desarrollemos cierta hostilidad contra aquellos elementos no computarizados?. ¿Una actitud beligerante frente a las excepciones y contra todo aquello que esté más allá del orden algorítmico?. Es concebible que el procesamiento de información intensificará una forma de pensar común, que nos está ya impuesta por la ciencia. Hoy día sentimos que la ciencia puede describir y explicar la realidad completa; lo que la ciencia no explica es o un trabajo no finalizado, o algo irreal, mera imaginación. No es difícil concebir una visión del mundo que siga la misma línea, pero que está aún más restringida por las posibilidades del

computador; para todas las mentalidades, el computador puede cubrir, procesar y controlar cualquier actividad humana; lo que no ha sido programado es un trabajo en curso, y lo que no se puede procesar es o un peligro o un sueño quimérico o una solemne tontería.

Esto no es en absoluto ciencia ficción, es simplemente el paralelismo lógico de la visión derivada de la física por personas que tienen pocas nociones acerca del método fundamental y de las limitaciones del desarrollo científico y tecnológico. Creen en la física como si de una religión se tratara y prefieren estar soportados por esta seguridad pragmática sin riesgos, que es inherente en esta clase de creencia. ¿Por qué no se puede extender este planteamiento al computador, que soporta un subconjunto de la realidad de una seguridad inmensamente superior?. ¿Puede imaginar los detalles de un futuro de esta naturaleza un mundo con casi ningún trabajo ni esfuerzo humano, una jornada laboral muy reducida, vacaciones durante gran parte del año, mientras los computadores hacen cualquier cosa por nosotros y lo que no hacen no es digno de ser hecho?

Realmente no es previsible que lleguemos a esta clase de futuro. El pensamiento algorítmico impuesto y cultivado por el uso de los computadores nos fuerza a mejorar la planificación y la predicción. En el futuro examinaremos mucho más cuidadosamente lo que hemos hecho en el pasado, y de esta forma obtendremos alguna llamada de atención sobre el problema. El primer informe del Club de Roma "Los límites del crecimiento", publicado en 1972 y elaborado por un equipo bajo la dirección de Meadows, produjo un tremendo impacto. La extrapolación del crecimiento de cinco variables: población, producción de alimentos, contaminación, industrialización y agotamiento de los recursos, conducía a resultados catastróficos en el plazo de pocos años. El crecimiento no podía seguir un ritmo exponencial. La única vía de solución es ir más lentamente. Se hace, pues, necesario alcanzar el equilibrio, ya que en caso contrario se produciría agotamiento y posterior hundimiento.

Este informe es un ejemplo sobresaliente de lo que estamos diciendo: no es tan importante cuán correctos sean en el momento de su publicación, ni tan siquiera si las predicciones que arrojan describen el futuro. Lo esencial es que los modelos fueron posibles a través del procesamiento automático de la información, y que los consejos que de los mismos se derivan se escuchen y reciban con la atención que merecen por quien tiene competencias. En este contexto es bueno reflexionar sobre los impactos no esperados que las tecnologías de la información han producido.

En los primeros días de los computadores se podía haber confiado (y muchos lo hicieron) en que por medio de las grandes posibilidades de los computadores, la economía podría llegar a convertirse en una ciencia exacta, como la física y la química. Por supuesto que los grandes economistas no cayeron en la trampa. Así Oscar Morgenstern, coautor con John von Neumann de "Teoría de juegos y conducta económica", ha luchado toda su vida contra esta creencia, particularmente si se basaba en su teoría de juegos. Lo que realmente ha sucedido en los últimos tiempos no ha sido que la economía se transformó en una ciencia exacta, sino que la ciencia de la computación se hizo más inexacta, en el sentido de que la característica de incertidumbre se extiende al diseño de los propios sistemas.

Es necesario planificar durante más tiempo los sistemas, antes de entregarlos, y eso quiere decir que deben responder en un entorno que nadie puede predecir y describir de forma precisa en el momento de su desarrollo. Cuando el sistema que se concible hoy día esté en servicio, podría suceder que fueran erróneas muchas de las hipótesis en las que se basaba. Durante la vida de este sistema pueden incluso cambiar sustancialmente. La naturaleza no mecánica de nuestro entorno actual se hace cada vez más aparente y esto indudablemente tendrá un impacto sobre la sociedad. En particular por lo que respecta al pensamiento algorítmico, nadie negará la elegancia y utilidad del concepto, pero sus limitaciones y dependencias de los hechos fuera de este contexto hay que tenerlo siempre presente. La necesidad de planificar y predecir el futuro a pesar de las muchas incertidumbres nos enseñará que los juicios, más allá de la confirmación científica, son tan importantes en muchos casos hoy día como lo fueron en el pasado. La única forma de vencer a los elementos inciertos es la planificación y la predicción, es esforzarse en dar a nuestras creaciones una flexibilidad máxima para que puedan adaptarse fácilmente a sucesos y tendencias impredecibles o inesperados.

A pesar de todo, bastantes personas no se dejan llevar por la corriente respecto a los nuevos métodos tecnológicos e incluso mantienen un punto de vista crítico sobre sus propios éxitos. Como un ejemplo de esta corriente, se puede citar al renombrado especialista en computadores Joseph Weizenbaum, profesor en el MIT, quien en su libro "Computer power and human reason from judgement to calculation" proporciona una serie de argumentos muy cualificados En realidad, su libro es una excelente descripción de muchos aspectos del impacto de las tecnologías de la información sobre la sociedad. Weizenbaum es crítico pero no pesimista, y es difícil no estar de acuerdo con su tesis fundamental: el computador es una de las más importantes y potentes herramientas que la

tecnología ha puesto en manos de la humanidad. Cualquier herramienta moderna incluye ciertos peligros y debe tener fuertes impactos positivos y negativos sobre la sociedad. El conformar qué tendencia va a ser la dominante a largo plazo está en nuestras manos, en las manos de los gobiernos que elegimos, de los especialistas y de todos los que trabajan en el apasionante campo de las tecnologías de la información y en las manos, en definitiva; de todos los individuos que se benefician y perjudican por el procesamiento automático de la información.

Podemos imaginar un sistema computarizado en el que el ciudadano pueda enviar mucha más información a su gobierno y en el cual, sin embargo, la restricción para cualquier elección humana, la potencia de las interdependencias lógicas y el peso de los hechos objetivos se hagan mucho más transparentes a la sociedad en su conjunto. El ejercicio de un derecho lleva consigo el respeto por la realidad y responsabilidad de la sociedad, virtudes no reconocidas particularmente por las formas presentes de toma de decisiones en las sociedades democráticas, pero que ponen de manifiesto la importancia de un mundo computarizado en el que cualquier tipo de decisión pública por votación debe depender de disponer de la información adecuada, porque, si no, la ejecución automática de la decisión tendrá consecuencias catastróficas. Los sistemas políticos asistidos por computador no han sido todavía intentados. En muchos aspectos aún es demasiado pronto, pero resulta obvio que en el futuro se introducirán esquemas de este tipo.

Tal impacto del procesamiento de la información no significará una era llena de satisfacción y felicidad. Pero, al menos, el hombre será capaz de decidir, utilizando los medios que las nuevas tecnologías de la información pone a su alcance. Nuestro destino permanecerá en nuestras manos, incluso en un entorno tecnológico altamente automatizado, porque el procesamiento de la información nos devolverá otra vez la toma de decisiones.

Un sistema de ciencia y tecnología que se fundamente en la información y en el lenguaje, dos de las propiedades más elevadas de la mente humana, solamente puede tener a largo plazo un impacto general: el retorno de nuestra confianza en la humanidad y en las actitudes morales y éticas del ser humano.

Derecho Comunitario y Nuevas Tecnologías: Libro Verde y Directivas de Bases de Datos

JORGE PÁEZ MAÑÁ

CINDOC-CSIC[1]

1.-Libro Verde sobre los derechos de autor y los derechos afines en la Sociedad de la Información.

En el marco de la política de armonización de las legislaciones de los Estados miembros de la Unión Europea, elaborada con la finalidad de integrar los mercados nacionales en un único mercado de nivel comunitario y facilitar el desarrollo de productos o servicios que requieren, para su rentabilidad, superar las limitaciones provocadas por la existencia de mercados fragmentados de nivel nacional, se inició a mediados del año 1995, con la edición y difusión del Libro Verde sobre los derechos de autor y los derechos afines en la Sociedad de la Información, un amplio debate sobre los aspectos jurídicos relacionados con la

[1] Centro de Información y Documentación Científica, del Consejo Superior de Investigaciones Científicas.

propiedad intelectual afectados por la consolidación de las autopistas de la información.

El Libro Verde, se confeccionó con la finalidad de estudiar la adaptación de las normativas sobre propiedad intelectual a las necesidades generadas por la aparición de nuevos productos y servicios distribuidos por las autopistas de la información, con objeto de lograr una protección jurídica adecuada a dicha variedad y favorecer el desarrollo de infraestructuras telemáticas, cuyo elevado coste no podría justificarse sin el crecimiento sostenido de la citada multiplicidad de productos y servicios.

Su elaboración fue consecuencia de las propuestas del Libro Blanco de la Comisión de la Comunidad Europea sobre "Crecimiento, competitividad y empleo - retos y pistas para entrar en el Siglo XXI", en el que se llamaba la atención sobre la importancia de unir fuerzas y sinergías para alcanzar el objetivo de la construcción de una infraestructura europea de la información, y del informe Bangemann[2] que ponía de manifiesto la necesidad de velar tanto por que la protección de la propiedad intelectual recibiese toda la atención necesaria como por la elevación del grado de protección, con objeto de resolver los problemas de propiedad intelectual planteados con la mundialización y los multimedia. Este informe adoptado por la Comisión y reflejado en la Comunicación "Hacia la Sociedad de la Información en Europa: un programa de acción"[3], proponía, entre otras medidas, una reflexión más especializada sobre la protección de la propiedad intelectual.

Por medio del Libro Verde la Comisión se propuso ahondar en el análisis de la casuística de los derechos de autor y derechos afines, en el contexto del mercado interior de la Unión Europea, en forma integrada con el resto de iniciativas emprendidas por la Unión en ámbitos temáticos coincidentes con dichos derechos, excluyendo del debate tanto los aspectos ya regulados en las Directivas que establecían especificaciones sobre temas relacionados con la

■[2] Informe Bangemann. "Europa y la Sociedad de la Información global - Recomendación al Consejo Europeo", Bruselas, 26 de mayo de 1994.

■[3] Comunicación de la Comisión al Consejo y al Parlamento Europeo, al Comité Económico y Social y al Comité de las Regiones, COM(94)374 final, Bruselas, 19 de julio de 1994.

propiedad intelectual[4] como los referidos a la interoperabilidad de las redes, las patentes y marcas, los diseños y modelos, los conocimientos técnicos, los secretos profesionales y los nuevos servicios audiovisuales.

Con dicho análisis se pretende detectar las previsibles repercusiones que el desarrollo de la Sociedad de la Información provocará sobre la situación actual de los derechos de autor y derechos afines, habida cuenta de la naturaleza de la multiplicidad y variedad de los nuevos servicios generados por la convergencia de los sectores informático, de telecomunicaciones y audiovisual, de la internacionalización del mercado, y de las variaciones en la estructura de la oferta y la demanda en los nuevos sectores generados por la irrupción de las nuevas tecnologías de la información. Asimismo se pretende evaluar el riesgo de que pueda producirse una fragmentación del mercado interior de la Unión Europea como consecuencia de las divergencias existentes entre las regulaciones nacionales y las normas comunitarias tendentes a lograr un mercado interior en el que la libre competencia y circulación de productos y servicios sea realmente efectiva.

El Libro Verde, tras una introducción en la que se reseñan los trabajos previos relacionados con la adaptación de las normativas sobre propiedad intelectual al desarrollo de las nuevas tecnologías de la información[5], analiza las

■[4] Directiva 91/250/CEE, sobre Programas de ordenador; Directiva 92/100/CEE, sobre Derechos de alquiler y préstamo; Directiva 93/83/CEE, sobre Radiodifusión vía satélite y distribución por cable; Directiva 93/98/CEE, sobre Plazo de protección; y Directiva 96/9/CEE, sobre Protección jurídica de las bases de datos, que en el momento de la distribución del Libro Verde se encontraba aun como propuesta de Directiva.

■[5] Libro Verde sobre "Derechos de autor y desafío tecnológico - Problemas de los derechos de autor que requieren una iniciativa inmediata", COM(88) 72 final, de 7 de junio de 1988. Acciones derivadas del Libro Verde - Programa de trabajo de la Comisión en el ámbito de los derechos de autor y derechos afines, COM(90) 584 final, de 17 de enero de 1991. Trabajos de la Comisión Sirinelli, creada por el Ministerio de Cultura francés para estudiar la repercusión de las nuevas tecnologías sobre la protección de la propiedad intelectual. Los informes remitidos por el Ministerio de Industria y Comercio y de la Agencia de Promoción de la Cultura al Gobierno Japonés sobre los problemas de los multimedia en relación con la propiedad intelectual. Los trabajos desarrollados en Estados Unidos por el Grupo de reflexión, creado por iniciativa del Presidente Clinton, para estudio de la política norteamericana en materia de infraestructura nacional de información. Los estudios sobre la repercusión de las nuevas tecnologías sobre los derechos de autor y los derechos afines de la OMPI. El Acuerdo relativo a los aspectos de los derechos de propiedad intelectual relacionados con el comercio (Acuerdo ADPIC), concluido a raíz de las negociaciones de la Ronda de Uruguay. Los estudios previos a la Conferencia

causas origen de los mismos, y las líneas directrices de la Unión Europea sobre la materia centrándose en los siguientes aspectos:

- Las consecuencias derivadas de las ingentes inversiones que se precisan para la creación de la infraestructura internacional básica, para la confección de las autopistas de la información, que permita la creación y gestión de los nuevos productos y servicios suministrados por dicha vía.

- Las repercusiones de la transformación de la tecnología analógica en tecnología digital, dada las facilidades que ésta última ofrece en cuanto a la copia de productos informativos sin merma de calidad.

- El establecimiento del Mercado Único de la información, superando la previa segmentación atomizada del mismo, y la armonización del régimen jurídico aplicable en el mismo para evitar discriminaciones basadas en las diferencias establecidas sobre la propiedad intelectual en los diversos ordenamientos jurídicos.

- La aplicación del los Principios de subsidiariedad e intervención mínima, establecidos como directores de la política de la Unión Europea, por medio de los cuales se pretende armonizar la regulación jurídica de aquellos temas que afecten al establecimiento del Mercado Único.

- La ponderación de los derechos relacionados con la protección de la cultura en aquellos puntos que pudieran friccionar con la defensa de los derechos de propiedad intelectual y los derechos afines.

Una vez analizados los citados aspectos, que inciden en la regulación de la propiedad intelectual derivados del desarrollo de las nuevas tecnologías de la información, y tras el planteamiento de una serie de cuestiones preliminares generales relacionadas con el desarrollo del mercado de la información y su previsible incidencia sobre la protección de los derechos de autor y derechos

Diplomática sobre "Ciertas cuestiones de derecho de autor y de derechos conexos" de la OMPI, que, con posterioridad a la difusión del Libro Verde, se desarrolló en Ginebra, en diciembre de 1996.

afines, el Libro Verde deja abiertos para el debate, los aspectos jurídicos relacionados con los siguientes puntos:

- El derecho territorial aplicable a la explotación de las obras, sopesando la disyuntiva de la utilización o no, como tal, de las normas del país de origen, en las diferentes modalidades de transmisión, con determinadas especificidades; la determinación de la responsabilidad de los partícipes en cada fase de las transmisiones; la armonización de las normas reguladoras de la protección los diferentes derechos integrados en la propiedad intelectual; la ampliación de los derechos reconocidos por el Convenio de Berna; el establecimiento de cláusulas de salvaguarda sobre determinados derechos; y la libertad o limitación de la determinación contractual de los diferentes intereses en juego.

- El agotamiento o la subsistencia de los derechos de propiedad intelectual, en favor de los titulares de los mismos, tras la primera comercialización de los productos objeto de propiedad intelectual, con su consentimiento, en alguno de los Estados miembros de la Unión Europea o en terceros países.

- El derecho de reproducción y sus excepciones, haciendo hincapié en la inclusión o exclusión de la aplicación de dicho derecho a las copias digitalizadas, la incidencia de las nuevas tecnologías en las copias privadas, los efectos de la digitalización de las obras y de su transmisión electrónica, la proliferación de medios y sistemas de reproducción, y el perfeccionamiento de la calidad de las copias.

- El derecho de comunicación o transmisión pública, analizando la delimitación y alcance de los conceptos de transmisión publica y privada en las comunicaciones por la red en función de los sujetos intervinientes, sus relaciones, sus características, etc., y el momento en que deben considerarse como puestas a disposición del público las obras, protegidas por la propiedad intelectual, accesibles por medio de aplicaciones telemáticas.

- La afección de los derechos de autor y derechos afines provocada por la difusión o transmisión digital, punto a punto, de obras o prestaciones objeto de propiedad intelectual, y su posible incardinación, o no, en la protección de los derechos de alquiler y préstamo.

- La conveniencia o inconveniencia de establecer un nuevo derecho exclusivo y diferenciado de radiodifusión digital, independiente del de radiodifusión otorgado a favor de los titulares de los derechos afines, debido a la cada vez mayor trascendencia que, sobre sus derechos de copia, provoca la digitalización de señales y su posterior reproducción, con un nivel óptimo de calidad, por parte de los consumidores, la exigencia de delimitar en forma precisa los medios de difusión de las obras para favorecer los intereses de los citados titulares de derechos afines, y el reforzamiento del derecho de reproducción por medio de la utilización de sistemas técnicos que impidan dicha reproducción.

- La armonización del derecho moral de los autores, las garantías de la protección de la integridad de sus obras y el reconocimiento de su paternidad, dadas las facilidades que la digitalización otorga respecto a la modificación de las mismas, las actuales discrepancias entre la regulación de dicho derecho en los diferentes sistemas jurídicos nacionales e internacionales y la incidencia de las corrientes doctrinales que defienden por un lado el establecimiento de presunciones de renuncia de dichos derechos y por otro la regulación negocial por sectores de los mismos o alternativamente su estipulación contractual en forma individualizada sin cortapisas ni limitaciones legales.

- La gestión de los derechos de autor y derechos afines y la concesión de licencias de ámbito territorial o mundial para obras multimedia, así como la posible extensión de dichas actividades a cualquier otro tipo de obras por parte de las Entidades de gestión, planteando la disyuntiva entre la elección de un sistema centralizado de "ventanilla única", en todo o en parte, o la coexistencia, en el ámbito de la Unión Europea, de sistemas de gestión que compitan libremente entre sí y, por último, la conveniencia o no del establecimiento de códigos de conducta que orienten la conformación del sistema de gestión elegido.

- El incremento de la seguridad jurídica obtenido mediante la utilización de sistemas técnicos de identificación y protección de obras digitalizadas que permitan su marcado y gestión automática; la configuración de la información mínima que deberían introducir dichos sistemas de identificación; la normalización internacional de dichos sistemas; la forma de identificación de las obras de dominio público; y la posibilidad de ejecutar medidas de intervención, en el marco de la Unión Europea, con objeto de hacer obligatoria, de manera armonizada, la utilización de aquellos sistemas de protección previamente aceptados por los sectores industriales.

En síntesis el Libro Verde acomete la adecuación, a los retos y necesidades de la Sociedad de la Información, de las actuales estipulaciones de los derechos de autor y derechos afines existentes en el marco de la Unión Europea, mediante una metodología de dialogo y crítica, abierta a los diferentes sectores implicados, por medio de la cual se pretende lograr un amplio consenso, sobre las futuras regulaciones jurídicas nacionales e internacionales de dichos derechos, que garantice la efectiva protección de los intereses personales y colectivos en juego.

2.-Directiva sobre protección jurídica de las bases de datos.

La Directiva 96/9/CE, del Parlamento Europeo y del Consejo, de 11 de marzo de 1996, sobre la protección jurídica de las bases de datos surge, como consecuencia de la consolidación de la industria de bases de datos como elemento esencial en la actual Sociedad de la información y su previsible afianzamiento, en el futuro, como uno de los más importantes sectores del mercado de servicios de información a nivel mundial, con la finalidad de armonizar las diferencias existentes en la Unión Europea respecto al establecimiento del régimen jurídico aplicable las actividades relacionadas con las bases de datos y de dotar a la industria de bases de datos europea de una suficiente protección jurídica que la permita acceder, en condiciones competitivas, al mercado internacional de información automatizada.

Debe tenerse en cuenta que la industria de bases de datos genera en la actualidad unos ingresos directos próximos a los dos billones de pesetas, de los que la Unión Europea absorbe el 24% del total de la industria mundial (correspondiendo a España aproximadamente el 0,3%), siendo su principal beneficiario los Estados Unidos, con una cuota de mercado próxima al 63%.

En cuanto a la regulación jurídica preexistente se podían observar ostensibles diferencias de cobertura y protección de las bases de datos derivadas de desiguales regulaciones establecidas, respecto de las actividades con ellas relacionadas, en los distintos ordenamientos jurídicos nacionales, regionales e internacionales.

Así en el ámbito internacional, el Convenio de Berna, en su artículo 2.5, incluye entre los objetos de su protección a "*las colecciones de obras literarias o artísticas*

tales como las enciclopedias y antologías que, por la selección o disposición de las materias, constituyan creaciones intelectuales", sin perjuicio de los derechos de los autores de las obras que forman parte de la colección. En dicho Convenio se indica en su artículo 2.1 que "*los términos obras literarias y artísticas comprenden todas las producciones en el campo literario científico y artístico, cualquiera que sea el modo o forma de expresión*".

Por su parte la Convención Universal sobre los derechos de autor, en su artículo 1°, establece el compromiso de los estados contratantes de "*asegurar una protección suficiente y efectiva de los derechos de los autores o de cualesquiera otros titulares de estos derechos sobre las obras literarias, científicas y artísticas*".

Respecto a nuestro país, en el Texto Refundido de la Ley española de Propiedad intelectual, las bases de datos pueden entenderse subsumidas en el artículo 12 que indica que también son objeto de propiedad intelectual "*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*".

Asimismo el artículo 20.2 i) de dicha Ley las cita expresamente al reseñar que son actos de comunicación pública "*el acceso público a bases de datos de ordenador por medio de telecomunicación, cuando éstas incorporen o constituyan obras protegidas*".

Conviene indicar que está actualmente en fase de tramitación la incorporación de la Directiva sobre protección jurídica de las bases de datos, al ordenamiento jurídico español. A estos efectos se ha elaborado ya una propuesta de inclusión de los preceptos de la Directiva en el Texto Refundido de la antedicha Ley de Propiedad intelectual.

Respecto a la observación del mercado Comunitario de información puede constatarse, en el mismo, la existencia de un cierto desequilibrio en cuanto a la evolución de las diversas industrias nacionales de bases de datos, desequilibrio que se acentúa en comparación con las de terceros países ajenos al ámbito de la Unión.

Este desequilibrio se ve acrecentado, con independencia de factores derivados del diferente desarrollo tecnológico, por las divergencias existentes en los ordenamientos jurídicos nacionales respecto a la protección jurídica otorgada a las bases de datos, divergencias que por si mismas distorsionan la libre circulación

de mercancías y servicios de información automatizada insertos en ese sector del mercado internacional.

La citada distorsión se ve asimismo favorecida por la existencia de sustanciales diferencias entre los costes de inversión, tanto humanos como técnicos y económicos, generados por la fabricación de las bases de datos originales y los costes derivados del acceso y copia de bases de datos preexistentes, muy inferiores a los de creación de éstas últimas, lo que provocan graves perjuicios económicos a los fabricantes innovadores cuando se reproducen por terceras personas, sin su autorización, las bases de datos por ellos creadas.

Sin embargo, el crecimiento exponencial de la información exige grandes inversiones en sistemas avanzados de tratamiento de la misma, so pena de quedar, los países que ignoren dicha perspectiva, descolgados de los avances científicos y tecnológicos y postergados a una situación de dependencia tecnológica respecto de los países más avanzados, dependencia que puede ir incrementándose con el tiempo favoreciendo situaciones de desigualdades económico-sociales de difícil resolución.

Respecto a las divergencias en los marcos jurídicos nacionales aplicables a la actividad desarrollada por dicha industria, puede observarse que mientras en diversos países no existe protección alguna a las bases de datos, en el resto la protección jurídica de las mismas difiere ostensiblemente. Así mismo es claramente perceptible la inexistencia de un régimen armonizado sobre competencia desleal que permita cubrir dichas diferencias de protección y la dificultad de recurrir a precisiones jurisprudenciales o doctrinales asumidas en forma generalizada.

Ante dichas circunstancias la Directiva pretende incardinar la protección de las bases de datos originales en el marco de la protección que se otorga a los autores de las creaciones intelectuales, y establecer una serie de medidas complementarias que impidan la extracción y reutilización no autorizadas de las bases de datos que carezcan de dicho requisito de originalidad con la finalidad de proteger la inversión de los fabricantes de dichas bases de datos.

Para ello establece una definición de las bases datos que comprende cualesquiera conjunto de obras, datos u otros elementos independientes, siempre que éstos se encuentren dispuestos en forma sistemática y metódica en una forma

tal que se pueda acceder a ellos individualmente por medios electrónicos o de otra forma.

Sobre las bases de datos así definidas la Directiva establece una serie de preceptos normativos que pretenden armonizar y conformar el marco jurídico aplicable a las mismas poniendo de manifiesto los siguientes aspectos jurídicamente relevantes:

Respecto al contenido de cada uno de los elementos que constituyen el conjunto que conforma el fondo almacenado en la base de datos, indica que éstos podrán acogerse individualmente a dicha protección cuando el grado de originalidad de los mismos sea suficiente para ser considerados como creaciones intelectuales.

En cuanto a la base de datos, globalmente considerada, reseña que ésta podrá acogerse asimismo a dicha protección siempre y cuando la selección de los datos, obras o elemento conformadores del fondo almacenado en la misma, o la disposición de dicho contenido constituya una creación intelectual dotada de un cierto grado de originalidad.

De los productos complementarios y accesorios de la base de datos expone que cada uno de ellos puede acogerse a la citada protección siempre y cuando constituya una creación original.

En los casos en que se reconozca la antedicha originalidad, la protección otorgada al titular de la base de datos respecto al ejercicio de los derechos de explotación, del contenido parcial o global de los elementos almacenados en su fondo o de los productos complementarios y accesorios de la propia base, tendrá una duración de setenta años contados a partir del año siguiente al de su creación y puesta en funcionamiento. A partir del vencimiento de dicho plazo decaerá ésta protección pasando, con la excepción indicada a continuación, a dominio público.

En consideración a la inversión requerida para la producción de las bases de datos, a la facilidad de obtener copias de las mismas, y a las posibilidades que ofrece la tecnología digital de reproducir, adicionar, modificar y reordenar elevados volúmenes de datos, obras o elementos, que permiten elaborar nuevas bases de datos basadas en otras ya creadas a un coste muy inferior, la Directiva instaura, en forma novedosa y ciertamente original, un nuevo derecho

denominado "derecho sui generis de protección de las bases de datos", que pretende proteger a las bases de datos contra esos comportamientos parasitarios.

El establecimiento de este nuevo derecho "sui generis" tuvo su origen en la problemática la situación de la industria de las bases de datos habida cuenta de la siguiente casuística jurídica.

- Una gran parte de bases de datos almacenan en sus fondos datos, obras o elementos cuyos derechos de explotación comercial no son susceptibles de protección por medio de las legislaciones sobre propiedad intelectual (datos económicos oficiales, referencias bibliográficas, jurisprudencia, hechos y noticias de actualidad, etc.).

Y aun en el resto de los casos, en los que sí es posible accederse a dicha protección, los derechos de explotación de dichos fondos corresponden mayoritariamente a personas diferentes de las que ostentan la titularidad de las bases, lo que impide que la reutilización de datos, obras o elementos obtenidos de esas bases por terceras personas, sin autorización, pueda ser considerada como una infracción de los derechos de propiedad intelectual de dichos titulares, ya que carecen de ellos.

- La protección efectivamente otorgada al titular de la base de datos en virtud de los criterios de selección de los datos, obras o elementos que constituyen sus fondos puede ser desvirtuada si se entrecruzan diversas bases de datos dando origen a nuevos conjuntos objetivamente diferentes de los de partida.

Asimismo en los casos en que la selección de obras busque la exhaustividad en un cierto campo temático (obras de un determinado autor, guía de teléfonos, etc.), dicha pretensión excluiría por si misma la originalidad en cuanto a los criterios de selección lo que impediría su protección jurídica.

- La protección legalmente otorgada en virtud de los criterios de ordenación o disposición del contenido, es asimismo fácilmente vulnerable con la aplicación de la tecnología digital, ya que ésta facilita notablemente la reconversión de dicho contenido y su reordenación según otros parámetros, posibilitando de ésta forma la creación de bases de datos con idénticos contenidos sin infringir los derechos de propiedad intelectual, del titular de la base de datos, basados en la originalidad de esos criterios.

- Por último la protección de los elementos complementarios y auxiliares puede igualmente vulnerarse con la inclusión de otros de similares características, dado el escaso coste que esto implica respecto a los derivados de la producción de la base de datos.

Teniendo en cuenta que esta deficiente protección jurídica de las bases de datos debe aplicarse en unas difíciles circunstancias del mercado internacional de la información caracterizado por una creciente competencia en el sector de contenidos, una segmentación del mismo producida por las diferencias entre las legislaciones nacionales aplicables a dicho comercio, y un elevado coste de inversión en medios humanos, materiales y económicos, quedaba patente la necesidad de establecer una nueva regulación aplicable a este específico tipo de obras.

La Unión Europea ha iniciado este camino con la inclusión, en la Directiva sobre la protección jurídica de las bases de datos, de un nuevo derecho "sui generis" de protección de las bases de datos. Este nuevo y original derecho actúa en forma autónoma e independiente del resto de derechos de propiedad intelectual o cualesquiera otros, anteriormente establecidos, utilizados como medio de protección de las bases de datos.

El derecho "sui generis" presenta las siguientes características:

- Se establece sobre las bases de datos que hayan requerido una inversión sustancial, desde el punto de vista cuantitativo o cualitativo, para su creación, producción, verificación o presentación de su contenido y a favor de los titulares de las bases de datos (a los que la directiva cita como fabricantes).

Este requisito responde al objetivo de proteger la inversión del titular de la base de datos por el riesgo asumido con la producción de la misma por lo que no es aplicable a aquellas bases cuya creación y producción no impliquen gastos elevados susceptibles de ser jurídicamente protegidos.

- Otorga a los titulares de las bases de datos, protegidas por el mismo, la potestad de autorizar o prohibir la extracción o reutilización de la totalidad o de una parte sustancial de su contenido. Para la evaluación de dicha sustancialidad debe tenerse en cuenta tanto el volumen como la importancia de la parte extraída o reutilizada.

Así pues los titulares de las bases podrán oponerse a cualquier transferencia permanente o temporal, tanto de la totalidad como de partes sustanciales del fondo almacenado en las mismas, a otro soporte, con independencia del medio utilizado o la forma en que se realice, siempre que dicha transferencia no cuente con su preceptiva autorización.

Asimismo podrán oponerse a cualquier forma de puesta a disposición del publico de la totalidad o de partes sustanciales del contenido de sus bases, mediante la distribución de copias, alquiler, transmisión en línea, etc., que se produzca sin su expresa autorización.

En todo caso conviene tener en cuenta, especialmente en el caso de bases de datos en soporte CD-ROM o similares, que la primera venta de una copia de las bases de datos en el ámbito de la Unión Europea, por su titular o con su consentimiento, extinguirá el derecho de distribución mediante venta, ostentado hasta dicho momento por dicho titular, sobre las ventas sucesivas que puedan realizarse de la citada copia en cualquier país de la Unión Europea.

- Exige de los usuarios legítimos de las bases protegidas que, en los casos de realizar extracciones o reutilizaciones, repetidas o sistemáticas, de partes no sustanciales de las bases de datos, que supongan actos contrarios a la normal explotación de las mismas o que causen perjuicios injustificados a los intereses legítimos de los titulares de las bases, obtengan una previa autorización de dichos titulares.

De esta forma se pretende evitar que la acumulación de actos, aparentemente inocuos para los titulares de la bases de datos, acaben provocando una desvalorización de la utilidad de la mismas o una merma de los beneficios que previsiblemente podrían obtenerse sin esta pseudo-competencia desleal.

- Permite la transmisión o cesión de este derecho sobre las bases de datos a sucesivos titulares mediante cualquiera de las formas aceptadas en Derecho.

Esta vinculación del derecho sui generis a la titularidad de la base de datos facilita una mayor disponibilidad y seguridad en el trafico comercial por el que, a lo largo de su vida útil, puede transitar la base de datos.

- Se aplica en forma independiente de cualesquiera otras protecciones jurídicas a las que puedan acogerse las bases de datos y sin perjuicio de los

derechos existentes sobre su contenido, poniendo de manifiesto la autonomía de este derecho por las específicas causas que lo originan.

Dado el especial objetivo del derecho sui generis, la Directiva establece un plazo inicial de duración de su protección de 15 años, que se contabilizan a partir del inicio del año siguiente al de finalización del proceso de producción de la base. A estos efectos debe considerarse como finalizado dicho proceso en el momento en que la base se encuentre en condiciones de ser utilizada por los potenciales usuarios de la misma.

En los casos en que las bases de datos objeto de la protección de este derecho sean puestas a disposición del público, incorporándose de esta forma al trafico mercantil, el plazo de 15 años de protección se reinicia nuevamente, siempre y cuando la puesta a disposición del público se produzca antes de la expiración del plazo de protección inicialmente concedido.

Habida cuenta de la dinamicidad y permanente actualización de las bases de datos, lo que implica nuevas inversiones materiales, económicas y personales, la Directiva establece que el derecho "sui generis" puede ampliar el ámbito temporal de su aplicación, mediante renovaciones periódicas del plazo de protección, en aquellas bases de datos en las que se produzcan modificaciones sustanciales, evaluadas cualitativa o cuantitativamente, de su contenido o acumulaciones de adiciones, supresiones o modificaciones que impliquen nuevos y elevados gastos. Los nuevos y sucesivos plazos de protección, de 15 años, deberán contabilizarse a partir del momento en que se consideren producidas dichas trascendentes modificaciones.

Si bien la Directiva abarca en forma necesariamente global los aspectos jurídicos relacionados con las bases de datos, hay que tener en cuenta que en las mismas confluyen la casi totalidad de derechos, tanto morales como patrimoniales, contemplados en las leyes sobre propiedad intelectual, debiéndose en la mayoría de los casos aplicar criterios de analogía, pero siendo necesario, en el resto, establecer delimitaciones tipificadas dada su especificidad. Respecto a las singularidades concretas de las bases de datos, que deberían haberse puesto de manifiesto en la Directiva, podemos poner de manifiesto las siguientes:

- Respecto a la definición de base de datos convendría haber precisado sobre si su unicidad implica el almacenamiento de la misma en un único soporte o si por el contrario se admite que la base pueda encontrarse en diferentes soportes,

ubicados en distintos puntos de la red, y por ende sometidos a dispares ordenamientos jurídicos.

Asimismo, según la actual evolución, debería haberse determinado si ha de considerarse como una única base de datos los diferentes conjuntos de información suministrados por un mismo titular, que cubren campos y finalidades diversas, ubicados conjuntamente en un punto determinado de la red y gestionados, conjunta o individualmente, por el mismo sistema.

Cabe por ende analizar la casuística generada por la superposición de los dos criterios antedichos dada la previsible evolución de los servicios de información que permiten la creación virtual de bases de datos constituidas artificialmente con partes de bases de datos preexistentes para trabajar sobre ellas como un único producto.

Hubiera convenido, a estos efectos, introducir en el concepto de bases de datos un criterio de homogeneidad en cuanto a su objeto y finalidad a fin de diferenciar bases de datos diseñadas para diferentes aplicaciones y de unir bases de datos descentralizadas que bajo la titularidad de un mismo sujeto puedan interconectarse para cumplir con un objetivo común.

Igualmente habría sido conveniente reconocer explícitamente la dinamicidad de las bases de datos, evitando asemejar las mismas a las colecciones u obras estáticas, lo que permitiría eludir la ligazón establecida en la Directiva entre los plazos de protección y los actos de creación o modificación sustancial y facilitar el reconociendo de que cada nueva incorporación de obras a la base inicia individualizadamente el nacimiento del plazo de protección para estas últimas. De esta forma los plazos de protección se establecerían para cada unidad independiente de las bases a tenor del momento de su incorporación a las mismas.

- Es interesante la precisión de la Directiva en cuanto a la diferente protección jurídica otorgada a las obras almacenadas de la otorgada a la obra compuesta constitutiva de la base de datos, y asimismo la diferenciación de esta última respecto de la otorgada a los elementos complementarios o accesorios de la base de datos.

Dada la protección jurídica sobre la selección cabría interpretar que las bases de datos que almacenaran obras obtenidas de unas previas selecciones (artículos de revistas publicados según criterios de selección de los consejos de

redacción, etc.) deberían obtener la previa autorización de los titulares de dichas preselecciones directamente o a través de las entidades de gestión correspondientes.

- Respecto a los problemas derivados de la autoría, en primer lugar convendría determinar las partes de los ordenamientos jurídicos aplicable a las actividades relacionadas con los procesos relacionados con la creación, producción y distribución de las bases de datos para, para una vez obtenidos los preceptos aplicables a las mismas, poder deducir las consecuencias jurídicas derivadas de su ejecución.

El marco jurídico de referencia, en que deben circunscribirse dichos procesos, está delimitado por las leyes y reglamentaciones nacionales sobre propiedad intelectual y por los Convenios internacionales sobre dicha materia, en especial por el Convenio de Berna para la protección de las obras literarias y artísticas, y la Convención Universal de Ginebra sobre los derechos de autor.

Partiendo de lo estipulado en los diferentes corpus jurídicos, nacionales e internacionales, hay que recalcar el reconocimiento en los mismos de la existencia de un nexo de unión entre las obras objeto de propiedad intelectual y sus creadores.

En dichos corpus se exige que para que una obra pueda quedar incluida en el ámbito de protección de las legislaciones sobre propiedad intelectual, ésta deberá haber sido producida en virtud de una actividad intelectual genuina, y por ende original, de sus creadores, que reciben la consideración de autores de la misma.

Los autores, por tanto, deberán ser necesariamente personas naturales ó físicas, ya que solamente dichos sujetos pueden realizar una actividad intelectual susceptible, en virtud de su propia e íntima idiosincrasia, de crear obras originales que reflejen sus personales conocimientos, ideas, sueños, elucubraciones o sentimientos.

Si bien algunas legislaciones permiten otorgar la condición de autor, en determinados casos, a las personas jurídicas, esta seudoautoría debe entenderse únicamente como una forma de reconocimiento de que los derechos de explotación de las obras, publicadas bajo el nombre de dichas personas jurídicas, corresponden "ab initio" a las mismas, en virtud del precepto legal que regula

dichos supuestos, debiendo rechazarse cualquier otra interpretación que desvirtúe el vínculo establecido entre la obra y su creador.

En múltiples casos la autoría de las obras corresponde a un conjunto o grupo de autores que en forma autónoma o coordinada dan vida a las mismas, estando constituidas éstas por la suma global de sus aportaciones. En estos supuestos reciben todos ellos la condición de coautores de las obras creadas en virtud de dicha colaboración. Este tipo de obras, denominadas según los casos obras en colaboración u obras colectivas, conforman la mayoría de las bases de datos.

Es posible asimismo establecer una clara relación entre las bases de datos y las obras compuestas, consideradas estas últimas como aquellas que incorporan obras preexistentes sin la colaboración de sus autores. En la mayoría de las legislaciones sobre propiedad intelectual se establece que los autores de las obras compuestas deberán respetar los derechos de los autores de las obras incorporadas y obtener, en forma previa a su inclusión, su necesaria autorización, diferenciando y delimitando los derechos de los autores de las primeras, respecto al global de la obra, de los de las segundas, respecto a las partes individualizadas de las mismas de las que son creadores.

La autoría de las bases de datos genera una serie de derechos morales que presentan unas características especiales que la Directiva debería haber recogido o al menos reseñado mediante el correspondiente reenvío a las legislaciones nacionales o normas internacionales, entre las que cabe citar las siguientes:

El derecho de los autores de las bases de datos a exigir el reconocimiento de su autoría, y en consecuencia su potestad para imponer o prohibir que en la divulgación de las mismas se incluya su nombre o seudónimo (en un fichero especial dedicado al efecto, que pudiera ser consultado por los usuarios). Este derecho se considera en la mayoría de legislaciones como imprescriptible, irrenunciable, e inalienable.

La adecuación de los de derechos morales relacionados con la difusión, modificación, integridad o retirada del comercio de las bases de datos, ya que, dada la finalidad divulgativa y la necesaria dinamicidad de las mismas, éstos deben quedar subsumidos entre los derechos patrimoniales integrados en la potestad de disposición del titular de la base de datos.

- Respecto al titular de los derechos de la base de datos, la Directiva debería haber concretado más los aspectos relacionados con dicha titularidad indicando que se considerará como tal titular a la persona o grupo de personas físicas o jurídicas que adquieran los derechos de propiedad sobre la misma pudiendo usarla, disponer de la misma, poseerla o enajenarla, así como proceder a su explotación o reivindicar su dominio en la forma que consideren más oportuna, sin más límites que los establecidos en las leyes, recalcando los siguientes aspectos:

En consideración a la actividad intelectual desarrollada por los autores de la selección o disposición del contenido de la base de datos, durante el proceso de su creación, éstos ostentarán ab initio la titularidad de la misma.

La titularidad de la base de datos, creada como obra en colaboración, que sea resultado unitario de la contribución de varios autores corresponderá conjuntamente a todos ellos, tal y como indica la Directiva.

La titularidad de la base de datos, creada como obra colectiva (constituida por la reunión de aportaciones de diferentes autores cuya contribución personal se funde en una creación única y autónoma, para la cual haya sido concebida), que sea resultado de la iniciativa y coordinación de una persona física o jurídica que asume el riesgo de efectuar las inversiones necesarias para su elaboración corresponderá, salvo pacto en contrario, a dicha persona física o jurídica. Los autores partícipes en la obra colectiva no podrán oponerse a que ésta se divulgue bajo el nombre de su titular.

La titularidad de la base de datos creada en virtud de una relación laboral será ostentada por el empleador o el empleado a tenor de lo pactado en el contrato. A falta de pacto escrito, se presumirá que la titularidad ha sido enteramente y en exclusiva transmitida al empresario.

Corresponde a los titulares de las bases de datos, siempre y cuando éstas constituyan obras consideradas como objetos de propiedad intelectual, el ejercicio exclusivo de los derechos de explotación en cualquier forma y lugar, y en especial los derechos de reproducción, distribución, comunicación pública y transformación, que no podrán ser ejecutados sin su autorización salvo en los casos expresamente previstos en la legislación sobre propiedad intelectual.

Estos derechos pueden ser enajenados o transmitidos en forma total o parcial a sucesivos titulares, inter vivos o mortis causa, en cualesquiera de las formas admitidas en Derecho, ostentando los nuevos titulares los derechos así obtenidos.

El titular de la base de datos debe tener muy presente que, en la producción de las bases de datos que incorporen obras preexistentes, objetos asimismo de propiedad intelectual, sin la colaboración de los autores de estas últimas, deberá contar con su autorización en forma previa a la inclusión en la base de datos de dichas obras.

El ejercicio de los derechos de explotación, por el titular de este tipo de bases, deberá ejercerse sin perjuicio de los derechos de los autores o titulares de las obras incorporadas, siendo compatibles e independientes los derechos sobre las bases de datos y los derechos sobre las obras incorporadas a las mismas.

Asimismo cabría hacer una apreciación sobre la diferente titularidad de los derechos de explotación y los derechos morales, que podrían estar detentados por diferentes titulares sin menoscabo de la protección jurídica de la propia base, definiendo con precisión los conceptos de autor de la base, productor de la base, distribuidor de la base y titular de los derechos de explotación de la base, que según los casos podría coincidir o no con alguno de los anteriores. A efecto de las repercusiones legales generadas por la producción de bases de datos nominativas también hubiera sido conveniente precisar el concepto de responsable de la base de datos.

- En cuanto a la incorporación, a las bases de datos referenciales, de obras de terceras personas, esta circunstancia obliga al respeto del derecho de cita de las mismas, debiéndose indicar su fuente y, en los casos en que junto a la referencia se añada un resumen, si este resumen ha sido realizado por el autor de la obra incorporada o por un tercero.

Asimismo los usuarios de una base de datos que obtengan una información susceptible de aprovechamiento en beneficio propio deberán citar la fuente de procedencia de la información utilizada (la base de datos, junto con el nombre de su titular), que por ende disfrutará del derecho de cita correspondiente a la información original o derivada que suministre por medio de la base de datos.

- Al titular de la base de datos la Directiva debería haberle otorgado los derechos a actualizarla, modificarla, integrarla en otra o disgregarla en diversas bases, así como la potestad de cambiar su finalidad sin consentimiento de sus autores, sin que ninguno de estos actos supusiera una vulneración del derecho de los autores a la integridad de sus obras, siempre y cuando dichos cambios estuvieran plenamente justificados por la necesaria dinamicidad de las bases de datos y no perjudicaran sus derechos morales, así como el derecho a oponerse a la retirada de la obra del comercio de la base, cuando así lo solicitase alguno de sus autores, si esto le supusiese un injustificado perjuicio a sus intereses.

- En cuanto al derecho sui generis, en la Directiva se debería haber limitado las extracciones y reutilizaciones de una parte "no considerable" de las bases cuando éstas pudieran constituir una parte "si considerable" de la reutilización; analizado la casuística del cambio de la finalidad de la utilización de los datos obtenidos, cuando la finalidad de la utilización de las extracciones difiera ostensiblemente de la finalidad de la base de procedencia (utilización como corpus lingüístico, utilizado para el estudio y análisis de frases, de la extracción obtenida de una base de datos legislativa a texto completo suministrada para información jurídica); y contemplado la casuística generada por la posibilidad de introducir las bases de datos en sistemas expertos.

Por último cabría interrogarse sobre la efectividad del derecho sui generis en el futuro, habida cuenta de que, con los previsibles avances tecnológicos, los costes de producción de las bases de datos se irán reduciendo, lo que haría decaer este derecho basado exclusivamente en su grado de onerosidad.

En conclusión, la Directiva cumple el objetivo primordial de toda norma jurídica en cuanto a la sensibilización y conformación de la conciencia social sobre los riesgos derivados de la evolución tecnológica en el campo que abarcan sus preceptos, aporta un novedoso grado de originalidad que es de agradecer, establece una protección jurídica a un sector necesitado de la misma, marca unas directrices en consonancia con el nuevo orden económico mundial y abre el camino a un debate, en el que no debe faltar la crítica constructiva, sobre la forma de resolver los nuevos problemas planteados con la consolidación de las modernas tecnologías de la información, la universalización de los mercados, y el flujo internacional de productos y servicios informativos a través de denominadas autopistas de la información.

Internet: Responsabilidades Legales

JAVIER RIBAS ALEJANDRO

Abogado especialista en Derecho Informático. Asesor Jurídico de SEDISI y BSA.

INTRODUCCION

El ciberespacio es un mundo virtual en el que los defectos, miserias y malos hábitos del ser humano se reproducen con la misma fidelidad que las virtudes. El efecto de aldea global generado por el entramado de redes y la proliferación de nodos en todo el planeta ayuda a la difusión inmediata de los mensajes y permite el acceso a cualquier información introducida en la red. A las reconocidas ventajas que ello supone se unen las distorsiones y los malos usos que pueden tener lugar en el sistema y que confirman una vez más que el mal no está en el medio utilizado sino en la persona que lo utiliza.

Actualmente se está produciendo un intenso debate respecto a la necesidad de prevenir y sancionar estos malos usos en la red de redes Internet y el objetivo de este artículo es localizar las distorsiones más habituales que se producen y resumir los argumentos que se han dado a favor de una legislación que regule el uso de la red y los criterios contrarios a esa regulación.

1. ARGUMENTOS A FAVOR DE LA REGULACIÓN

Los partidarios de la regulación se apoyan en la tesis de que las redes de telecomunicaciones como Internet han generado un submundo en el que los delitos son difíciles de perseguir debido a la propia naturaleza del entorno y a la

falta de tipificación de las modalidades de comisión y de los medios empleados. Entre los delitos, infracciones administrativas y malos usos que se pueden llevar a cabo en la llamada infraestructura de la información, destacan, sin ánimo de clasificarlos, los siguientes:

1.1 Delitos tradicionalmente denominados informáticos

A pesar de que el concepto de delito informático engloba tanto los delitos cometidos contra el sistema como los delitos cometidos mediante el uso de sistemas informáticos, cuando hablamos del ciberespacio como un mundo virtual distinto a la "vida real", me refiero al delito informático como aquél que está íntimamente ligado a la informática o a los bienes jurídicos que históricamente se han relacionado con las tecnologías de la información: datos, programas, documentos electrónicos, dinero electrónico, información, etc..

Incluyo también dentro de este apartado los actos que sólo constituirían una infracción administrativa o la vulneración de un derecho no tutelado por la jurisdicción penal, pero que en algunos países pueden llegar a ser delito.

Dentro de este tipo de delitos o infracciones podríamos destacar:

Acceso no autorizado: La corriente reguladora sostiene que el uso ilegítimo de passwords y la entrada en un sistema informático sin la autorización del propietario debe quedar tipificado como un delito, puesto que el bien jurídico que acostumbra a protegerse con la contraseña es lo suficientemente importante para que el daño producido sea grave.

Destrucción de datos: Los daños causados en la red mediante la introducción de virus, bombas lógicas y demás actos de sabotaje informático no disponen en algunos países de preceptos que permitan su persecución.

Infracción de los derechos de autor: La interpretación de los conceptos de copia, distribución, cesión y comunicación pública de los programas de ordenador utilizando la red provoca diferencias de criterio a nivel jurisprudencial. No existe una opinión uniforme sobre la responsabilidad del propietario de un servicio on-line o de un sysop respecto a las copias ilegales introducidas en el sistema. Mientras un tribunal condenó a un sysop porque en su BBS había imágenes scaneadas de la revista Playboy, en el caso LaMacchia, el administrador del sistema fue hallado no responsable de las copias de programas que albergaba su BBS. El recurso de los propietarios de sistemas on-line y BBS ha sido incluir una advertencia o una cláusula contractual que los exonera de responsabilidad frente a

un "upload" de un programa o fichero que infrinja los derechos de autor de terceros.

Infracción del copyright de bases de datos: No existe una protección uniforme de las bases de datos en los países que tienen acceso a Internet. El sistema de protección más habitual es el contractual: el propietario del sistema permite que los usuarios hagan "downloads" de los ficheros contenidos en el sistema, pero prohibe el replicado de la base de datos o la copia masiva de información.

Interceptación de e-mail: En este caso se propone una ampliación de los preceptos que castigan la violación de correspondencia, y la interceptación de telecomunicaciones, de forma que la lectura de un mensaje electrónico ajeno revista la misma gravedad.

Estafas electrónicas: La proliferación de las compras telemáticas permite que aumenten también los casos de estafa. Se trataría en este caso de una dinámica comisiva que cumpliría todos los requisitos del delito de estafa, ya que además del engaño y el "animus defraudandi" existiría un engaño a la persona que compra. No obstante seguiría existiendo una laguna legal en aquellos países cuya legislación no prevea los casos en los que la operación se hace engañando al ordenador.

Transferencias de fondos: Este es el típico caso en el que no se produce engaño a una persona determinada sino a un sistema informático. A pesar de que en algunas legislaciones y en sentencias aisladas se ha asimilado el uso de passwords y tarjetas electrónicas falsificadas al empleo de llaves falsas, calificando dicha conducta como robo, existe todavía una falta de uniformidad en la materia.

1.2 Delitos convencionales

Al hablar de delitos convencionales me refiero a todos aquellos que tradicionalmente se han venido dando en la "vida real" sin el empleo de medios informáticos y que con la irrupción de las autopistas de la información se han reproducido también en el ciberespacio. También en este caso incluyo en este apartado actos que no son propiamente delitos sino infracciones administrativas o ilícitos civiles. No obstante, teniendo en cuenta el carácter global de Internet, alguna de las conductas reseñadas pueden constituir un delito en unos países y en otros no.

Espionaje: Se ha dado casos de acceso no autorizado a sistemas informáticos gubernamentales e interceptación de correo electrónico del servicio secreto, entre otros actos que podrían ser calificados de espionaje si el destinatario final de esa información fuese un gobierno u organización extranjera. Entre los casos más famosos podemos citar el acceso al sistema informático del Pentágono y la divulgación a través de Internet de los mensajes remitidos por el servicio secreto norteamericano durante la crisis nuclear en Corea del Norte en 1994, respecto a campos de pruebas de misiles. Aunque no parece que en este caso haya existido en realidad un acto de espionaje, se ha evidenciado una vez más la vulnerabilidad de los sistemas de seguridad gubernamentales.

Espionaje industrial: También se han dado casos de accesos no autorizados a sistemas informáticos de grandes compañías, usurpando diseños industriales, fórmulas, sistemas de fabricación y know how estratégico que posteriormente ha sido aprovechado en empresas competidoras o ha sido objeto de una divulgación no autorizada.

Terrorismo: La existencia de hosts que ocultan la identidad del remitente, convirtiendo el mensaje en anónimo ha podido ser aprovechado por grupos terroristas para remitirse consignas y planes de actuación a nivel internacional. De hecho, se han detectado mensajes con instrucciones para la fabricación de material explosivo.

Narcotráfico: Tanto el FBI como el Fiscal General de los EEUU han alertado sobre la necesidad de medidas que permitan interceptar y descifrar los mensajes encriptados que utilizan los narcotraficantes para ponerse en contacto con los cárteles. También se ha detectado el uso de la red para la transmisión de fórmulas para la fabricación de estupefacientes, para el blanqueo de dinero y para la coordinación de entregas y recogidas. El notable avance de las técnicas de encriptación permite el envío de mensajes que, a pesar de ser interceptados, pueden resultar indescifrables para los investigadores policiales. Debe tenerse en cuenta que sólo en 1994 los jueces americanos concedieron 1.154 órdenes de vigilancia electrónica, de las cuales un importante número tuvieron resultado negativo a causa de la utilización de técnicas de encriptación avanzadas. Por ello, tanto el FBI como los fiscales americanos reclaman que todos los programas de encriptación generen puertas traseras que permitan a los investigadores acceder al contenido del mensaje.

Otros delitos: Las mismas ventajas que encuentran en Internet los narcotraficantes pueden ser aprovechadas para la planificación de otros delitos como tráfico de armas, proselitismo de sectas, propaganda de grupos extremistas,

y cualquier otro delito que pueda ser trasladado de la vida real al ciberespacio o al revés.

1.3 Mal uso: cybertorts

Usos comerciales no éticos: Algunas empresas no han podido escapar a la tentación de aprovechar la red para hacer una oferta a gran escala de sus productos, llevando a cabo "mailings electrónicos" al colectivo de usuarios de un gateway, un nodo o un territorio determinado. Ello, aunque no constituye una infracción, es mal recibido por los usuarios de Internet, poco acostumbrados, hasta fechas recientes, a un uso comercial de la red.

Actos parasitarios: Algunos usuarios incapaces de integrarse en grupos de discusión o foros de debate on- line, se dedican a obstaculizar las comunicaciones ajenas, interrumpiendo conversaciones de forma repetida, enviando mensajes con insultos personales, etc. Aunque la mayoría de estas conductas están previstas por los suministradores de servicios on-line, resolviendo el contrato con los reincidentes, existen algunos partidarios de que se establezcan normas para sancionar estos actos.

Obscenidades: Más adelante veremos la polémica generada por el proyecto de ley del senador Exon en EEUU respecto a una Communications Decency Act.

1.4 Efectos transfronterizos

Otro de los aspectos sobre los que se reclama una regulación es el de la competencia jurisdiccional en el caso de actos realizados en un país determinado pero que, debido a la extensión de la red, tienen sus efectos en otro país. Aunque el derecho internacional da solución a este tipo de conflictos, existen diversos criterios respecto a la determinación del lugar en el que se ha producido la infracción.

Así como en una radiodifusión vía satélite existe una conducta activa de emisión, sujeta a unas normas especiales, la introducción de una obra infractora en un host conectado a Internet. ¿debe entenderse también como un acto de difusión o comunicación pública?

La conducta activa o pasiva del presunto infractor es determinante para apreciar la existencia de la infracción y la competencia jurisdiccional. Si hacemos una comparación de las autopistas de la información con las autopistas de asfalto, deberíamos reconocer que no es lo mismo enviar camiones de reparto a todos los países y ciudades con vías de acceso, que tener una tienda abierta al lado de la autopista.

Un ejemplo de conducta pasiva sería el caso de Phil Zimmermann, investigado por exportar tecnología de doble uso a otros países. Zimmerman se limitó a introducir su programa de encriptación de clave pública PGP (Pretty Good Privacy) en hosts que se hallaban dentro del territorio de los EEUU, pero al estar estos hosts conectados a Internet, todos los países conectados a la red pudieron obtener una copia del programa. Zimmermann recibió numerosos mensajes de felicitación y agradecimiento desde países con embargo comercial y tecnológico. Este caso ha acabado siendo un exponente de la lucha entre el poder intervencionista del Estado y el derecho a la intimidad de la persona, como más adelante veremos.

Un ejemplo de conducta activa sería remitir una recopilación de imágenes pornográficas scaneadas a los mailbox de un país en que dicho tráfico estuviese prohibido.

2. ARGUMENTOS EN CONTRA DE LA REGULACION

Frente a la corriente reguladora se levantan los partidarios de que ciertas áreas queden libres del intervencionismo o proteccionismo estatal. Entre los argumentos más utilizados figuran el derecho a la intimidad y la libertad de expresión.

2.1 Derecho a la intimidad

Uno de los derechos más defendidos en los países en los que ha habido una gran implantación de los sistemas informáticos en la gestión de los datos de los ciudadanos por parte de la Administración, ha sido el derecho de la persona a que su intimidad no sea vulnerada por un abuso de estos medios. La protección de este derecho ha generado preceptos de rango constitucional en muchos países. En España, el artículo 18 CE garantiza el secreto de las comunicaciones y abre la posibilidad de que la Ley limite 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. Del desarrollo de este precepto ha surgido hasta ahora la LORTAD como instrumento destinado a evitar que mediante el tratamiento automatizado de los datos se llegue a obtener el perfil de una persona, sus aficiones y sus hábitos. Con ello se reconoce que el uso de las tecnologías de la información permite una rapidez en la manipulación de datos que era impensable con el empleo de medios manuales o analógicos. En la discusión de la LORTAD se llegó a establecer la comparación de que los sistemas manuales equivalían a pescar con caña y los informáticos a pescar con red.

La misma frase se ha repetido al hablar sobre el poder del Estado al investigar las transmisiones efectuadas en la infraestructura de la información, y concretamente al interceptar y leer el e-mail. En la declaración de Phill Zimmermann ante el Subcomité de Política Económica, Comercio y Medio Ambiente de la Cámara de Representantes de los EEUU, puede leerse: "En el pasado, si el Gobierno quería violar la intimidad de los ciudadanos corrientes, tenía que gastar sus recursos en interceptar, abrir al vapor y leer el correo y escuchar, grabar y transcribir las conversaciones telefónicas. Eso era como pescar con caña, de uno en uno. Por el contrario, los mensajes de e-mail son más fáciles de interceptar y se pueden scanear a gran escala, buscando palabras interesantes. Esto es como pescar con red, existiendo una diferencia orwelliana cuantitativa y cualitativa para la salud de la democracia".

Con argumentos similares se está defendiendo la idea de que si los avances tecnológicos han creado un ciberespacio en el que cualquiera puede expresarse y comunicarse sin temor a ser oído por otros, el poder del Estado no debería ampliarse hasta poder controlar este nuevo mundo.

Por de pronto, el servicio secreto norteamericano ya ha sido condenado por introducirse sin mandamiento judicial en la BBS Esteve Jackson Games y leer el e-mail en ella depositado. El servicio secreto ha tenido que pagar una indemnización de 50.000 dólares al propietario de la BBS y 1.000 dólares a cada usuario de la misma, por haber vulnerado su intimidad.

2.2 Libertad de expresión

Pocas propuestas de ley han generado tanta discusión en Internet como la Communications Decency Act. Los detractores de este proyecto sostienen que no sólo prohibiría conversaciones públicas de contenido "obsceno, lascivo, sucio o indecente" sino incluso las de ámbito privado entre dos personas, con la posibilidad de sancionar al proveedor del servicio on-line. Los usuarios de

Internet americanos se niegan a tener que hablar constantemente como si estuviesen en un entierro. La aplicación de esta ley, además de ser un importante obstáculo para la libertad de expresión, exigiría una enorme inversión en la monitorización y vigilancia del sistema y generaría constantes intromisiones en la intimidad de los ciudadanos. Durante el mes de abril y mayo de 1995, ha habido un importante movimiento para conseguir firmas de oposición a este proyecto. La dirección donde debían enviarse los mensajes era s314-petition@netcom.com.

2.3 Libertad de acceso a la información

Una corriente de usuarios de la red considera que el derecho a la información está por encima de otros derechos como la propiedad intelectual, la propiedad de los datos el secreto que se da al know how. Los partidarios de esta idea consideran que cualquier tipo de obra introducida en la red debería pertenecer al dominio público, y solicitan la inaplicabilidad de los derechos de autor y la supresión de fronteras en el ciberespacio para permitir el libre flujo de la información en todo el planeta.

3.AUTOREGULACION: CODIGOS DE CONDUCTA Y CIBERPOLICIAS

Códigos de conducta: Por el momento, y a falta de una legislación específica, en Internet existen unos códigos de ética cuyo incumplimiento está castigado con la censura popular, lo cual acaba siendo, en algunos casos, más eficaz que una norma de derecho positivo. Es posible que un usuario se marque unas pautas de conducta de acuerdo con unas leyes, pero la distancia o la ausencia de control de los órganos de vigilancia pueden hacer que esas pautas se relajen. No obstante, si sabemos que podemos ser juzgados por nuestros compañeros de la red y somos conscientes de que de nuestro comportamiento en los debates on-line y en la emisión y recepción de mensajes dependerá la opinión que tengan de nosotros y la calificación de novato, informal o persona non grata que podamos recibir, actualizaremos nuestras pautas de conducta día a día.

Ello hace que la tónica normal en Internet sea de respeto entre los usuarios de la red, siendo los demás casos la excepción.

Sistemas de seguridad informática: Las propios sistemas de control de cada host garantizan un umbral de seguridad aceptable, aunque no impiden que

los archivos que circulan por la red puedan contener algún virus. Y en muchos casos pueden ser neutralizados por un programa generador de passwords.

Ciberpolicías: Tanto NSA, FIRST Forum of Incident Response and Security Teams y CERT Computer Emergency Response Team tienen equipos de especialistas dedicados a la localización de hackers, defensa frente a sabotajes e intervención en caso de siniestros informáticos. Por otra parte, algunas policías como el FBI y Scotland Yard disponen de unidades especiales para investigar la comisión de delitos a través de la red.

4. SITUACION ACTUAL Y PROPUESTAS LEGISLATIVAS

El Código Penal de 1995 contiene muchas referencias a los delitos informáticos y a los derivados del uso de las telecomunicaciones, entre las que podemos destacar las siguientes:

- Delitos contra la intimidad y el secreto de las comunicaciones
- Estafas electrónicas.
- Infracción de los derechos de propiedad intelectual
- Delito de daños
- Revelación de secretos contenidos en documentos o soportes informáticos.
- Falsedad en documento electrónico
- Fabricación o tenencia de útiles e instrumentos específicamente destinados a la comisión de delitos.
- Sustracción, destrucción, inutilización u ocultación de documentos electrónicos por parte de un funcionario público cuya custodia le esté encomendada por razón de su cargo.

Por otra parte, algunas leyes como por ejemplo la LORTAD, incluyen en su articulado referencias a la seguridad informática de las bases de datos.

Pero en general, los españoles estamos algo desprotegidos frente a la nueva categoría de delitos que hemos comentado en este artículo.

Proyectos de ley de EEUU: Después del atentado de Oklahoma, el gobierno norteamericano ha empezado a estudiar formas de investigación y prevención antiterrorista. Ante la sospecha de que en la organización del atentado se utilizara la red Internet para el envío de mensajes encriptados, la propuesta de

ley antiterrorista de los senadores Dole y Hatch incluyen la ampliación de las facultades del FBI en materia de vigilancia electrónica y rastreo de la red.

Otro proyecto de la Casa Blanca modifica las leyes que regulan la intimidad y la intervención de las telecomunicaciones (Privacy Act y Wiretap Act) para poder interceptar y desencriptar mensajes electrónicos enviados o recibidos por sospechosos o presuntos terroristas, con plena eficacia procesal como prueba documental incluso cuando dichas evidencias hayan sido obtenidas sin el correspondiente mandamiento judicial.

Este proyecto también prevé la asignación de una partida presupuestaria para que el Fiscal General pueda solicitar a compañías telefónicas, electrónicas y de seguridad informática el diseño de tecnologías de intervención de las telecomunicaciones.

Todo ello va acompañado de un intenso debate sobre las posibilidades de desencriptación y la posible vulneración del derecho a la intimidad, al que antes he hecho referencia.

GATT - Ronda de Uruguay: En los últimos acuerdos del GATT se hacen referencias al nuevo entorno económico y tecnológico y a la necesidad de acuerdos globales en materia de Propiedad Industrial e Intelectual, pero no se analizan a fondo ni se resuelven los problemas que se han mencionado en este artículo.

Reuniones del G7 respecto a la Global Infraestructure Information: Las conclusiones del G7 en sus últimas reuniones han supuesto un enorme esfuerzo de síntesis para resumir en unos puntos básicos las actuales necesidades en materia normativa, frente al reto de la sociedad de la información. A continuación se enumeran algunas de las conclusiones más significativas:

a) La necesidad de analizar el alcance del derecho de información frente a la seguridad de la información.
b) La conveniencia o no de seguir limitando la cobertura del copyright a la expresión, en un contexto en el que la expresión es a veces menos importante que la propia información.
c) La necesidad de modificar los conceptos tradicionales del derecho de autor.
d) La necesidad de proteger las herramientas de navegación en el nuevo contexto digital.

e) La necesidad de analizar el impacto en el derecho de autor de nuevos conceptos como "almacenamiento temporal", "browsing" y "cita digital".
f) La necesidad de que el uso de las tecnologías de la información también es importante para los países en vías de desarrollo.

Libro Verde: La Comisión Europea ha editado un Libro Verde sobre los derechos de autor y los derechos conexos en la sociedad de la información.

Entre las propuestas que contiene este texto cabe destacar:

a)La existencia de ventanillas únicas para contratar telemáticamente los derechos necesarios para crear obras multimedia, facilitando así la localización de los titulares y el pago de los royalties correspondientes a las imágenes, textos, sonidos y videos utilizados.

b)La determinación del derecho aplicable en los casos de infracciones transfronterizas a través de la infraestructura de la información.

c)La armonización del derecho de los estados miembro para proteger de manera uniforme los derechos de las obras multimedia y de las bases de datos que se hallen en la infraestructura de la información.

d)La necesidad de redefinir del concepto de reproducción por medios digitales, planteando la cuestión de si la digitalización de una obra y la copia privada deberán ser objeto de autorización por parte del titular o no.

e)La necesidad de definir el concepto de transmisión digital de una obra en el seno de la infraestructura de la información con el fin de determinar si constituye un nuevo acto que precisa autorización del autor o si, por el contrario, está integrado en otros derechos como el de cesión, distribución o comunicación pública.

f)La conveniencia o no de regular las medidas de protección, seguridad informática, passwords y encriptación.

Contratación Electrónica

CARLOS BARRIUSO RUIZ

Doctor en Derecho- Abogado Especialista en Derecho Informático
e-mail: carlosbar@icam.es

1. INTRODUCCION

En la "CONTRATACIÓN ELECTRÓNICA" contemplamos las distintas fases de formación del consentimiento y el flujo informático de decisión, estudiando la parte de voluntad latente que encierran, que se manifiesta con vinculación jurídica cuando se activa el sistema, y por quien lo activa, en función de los distintos grados de electronificación e informatización , pero siempre reservando la decisión como atributo perteneciente en exclusiva a la inteligencia, voluntad y personalidad Humana.

El contrato electrónico más puro se daría proporcionalmente a la mayor cantidad de fases electronificadas e informatizadas incluido el cumplimiento (telecumplimiento), cuando el objeto contractual sea susceptible de transformación en bits, y el pago se haga por medio de anotaciones en cuenta u otros medios digitales.

Así en el mercado de valores, el procesamiento de la información de indicadores económicos, permite hacer previsiones del comportamiento de la bolsa, que ayudan a decisiones cuya expresión puede monitorizarse. La ley 24/88 del mercado de valores fue puntera en la contemplación de redes informáticas en la negociación bursátil por la comisión Nacional.

2. VALIDEZ

Consideramos perfectamente válida la "contratación electrónica", a la luz de nuestro Código Civil , que existirá jurídicamente desde que una o varias personas consientan sin error, libre y conscientemente, en obligarse entre ellas, a darse alguna cosa o prestarse algún servicio licito, por medios electrónicos en base al art. 1.254 del Código Civil y en virtud de la autonomía de la voluntad, expresada en el artículo 1.255 del Código Civil.

Las situaciones no previstas se regularán, por vía paccionada como en el caso de EDI con los acuerdos de intercambio, y códigos de conducta.

3. PERFECCIÓN

Un "animus contrahendi" "in ídem placitum consensus" expresado por medios y sobre soportes electrónicos, o realizado con ayuda de programas o elaboradores electrónicos, perfeccionara el contrato electrónico, siempre que concurran las condiciones esenciales para la validez de los mismos determinadas en el art. 1.261 del Código Civil y respeten las limitaciones y restricciones legales.

La oferta instrumentada electrónicamente aunque sea "ad incertam personam", es válida y el contrato se perfeccionará con la sola aceptación, cuyos "facta concludentia", serían, siguiendo la teoría civilista de la "recepción" y no la mercantilista de la "emisión", cuando el ofertante reciba el correo electrónico o el signo electrónico en su buzón o dispositivo electrónico, ya que se da un conocimiento efectivo potencial. art. 1.262 C.C.(correspondencia), Desde entonces, nacería la obligación del ofertante de proceder a la venta y al cumplimiento.

El Convenio de Viena de 11-4-80 al que España se adhirió el 17 de Julio de 1990 en su art. 23 establece también la aceptación de la oferta como perfección del contrato.

La datación del e-mail registrara el momento de la contratación, y con ello se determinara si esta en plazo la oferta.

El comprador podrá instrumentalizar en la red, también electrónicamente una "petición de ofertas" , para aceptar la mas conveniente.

4. FORMA

En cuanto a la forma del contrato electrónico, la consideramos también valida, amparado en la libertad de forma plasmada en el artículo 1.278 del Código Civil, (artículo 51 del Código de Comercio para los contratos mercantiles), fruto del carácter espiritualista heredado del Ordenamiento de Alcalá, pero este concepto quiebra en aquellos contratos en que la ley exige una forma constitutiva o sustancial; en aquellos que siendo potestativa de las partes, la exigen o acuerdan "ad probationem" ; en aquellos otros cuya fuerza ejecutiva está condicionada a la forma; o cuando se necesita o se requiere inscripción en registros públicos. En estos casos la intervención del legislador es obligada, para que el documento electrónico pueda acceder a estas categorías.

Así el testamento ológrafo 688 C.C. ; La donación de Inmuebles art. 633. C.C.; Las señaladas en El art. 1.279 y 1.280 del C.C. cuando los contratantes se compelen a ello; El Seguro, (art. 5 L. Contrato de Seguro) ;Letras de Cambio, Cheque ; Sociedades cooperativas , asociaciones, fundaciones; Censo enfiteutico (art. 1628) ;Las del art. 52 Código de Comercio ;Capitulaciones; Las Ventas de Bienes Muebles a plazos .

Con respecto a estas ultimas diremos que el proyecto de Ley sobre Ventas de Bienes Muebles a Plazos, aprobado el 11 de Abril de 1997 por el gobierno, y pendiente de su aprobación por el Parlamento, que sustituirá a la ley de 1965, ha perdido la oportunidad de incluir alguna referencia a la formalización del contrato electrónicamente, con lo cual se les veda la vía electrónica, ya que se exige a estos contratos para que tengan fuerza ejecutiva su constancia en escritura publica o póliza intervenida por un corredor de comercio, lo mismo que a los contratos sobre leasing o arrendamiento financiero. Lo mismo que en las pólizas de crédito que deben estar intervenidas por fedatario publico, o fedatario mercantil para poder entablar la demanda ejecutiva. Y lo mismo que la Hipoteca (1.880 -C.C. que la somete a la Ley hipotecaria) para cuya validez se necesita Inscripción en el Registro de la Propiedad (art. 1875 C.C.).

La ley de Ordenación del comercio minorista 7/1996 , no impone forma determinada para los contratos de compraventa, realizados a distancia fuera de las señaladas por el código civil de comercio o por otras leyes especiales (art. 11).

Pero sus artículos 47, 11.2 , exigen llenar la forma escrita, y aunque no sea con carácter esencial esta prescripción y por tanto civilmente el contrato no quedaría

viciado , la propia ley contempla multa de 500.001 a 2.500.000,- de pesetas (art. 68-2) para los casos de incumplimiento.

Llama la atención que esta forma escrita no se asimile a alguna forma electrónica máxime cuando la venta a distancia se apoya en medios electrónicos esencialmente, como si hace la Directiva 97/7.

La Directiva 97/7 relativa a la protección de los consumidores en materia de contratos a distancia publicada el pasado 4 de Junio, que luego comentaremos, tampoco impone una forma especifica para la venta a distancia fuera de la indicación de facilitar información escrita sobre el derecho de resolución , y las condiciones de rescisión, dirección geográfica, y los servicios posventa .

5. PRUEBA

Por otro lado jurídicamente es necesario constatar la voluntad declarada por medios electrónicos, reconociendo la validez de los caracteres del documento electrónico con un grado suficiente de eficacia. La criptología proporciona hoy el elemento básico para realizarlo, y en especial la Firma Electrónica, que permite articular las pruebas que determinan la integridad, autoría, y autentificación del documento.

Se hace pues necesario equiparar legalmente la firma electrónica a todos los efectos con la manuscrita , incluso dotarla de algún valor probatorio mas, ya que permite la integridad y autentificación del documento, cosa que no permite la analógica . Nuestro código civil se refiere a la firma, en los artículos - 688 testamento ológrafo; -Art. 1.223 escritura defectuosa , -Art. 1.225 Valor del documento privado suscrito. -Art. 1.226 obligación firmada impone a declarar sobre su autenticidad. Todos los cuales deberían tener su correlativo electrónico.

La firma electrónica responde ante el sistema informático por algo "que se tiene" en exclusiva como es la tarjeta con chip que realiza el algoritmo de encriptación con el software necesario; por algo que "se sabe" en exclusiva como es la clave privada del criptosistema de clave publica RSA. Puede complementarse con características biométricas es decir por algo "que se es" intrínsecamente.

El art. 45 de la Ley 30/1992 de régimen jurídico de las Administraciones Publicas y del Procedimiento administrativo Común incorporó el empleo y aplicación de los medios electrónicos en la actuación administrativa, de cara a los ciudadanos.

Para su regulación , el Real decreto 263/1996 de 16 de Febrero, indica que deberán adoptarse las medidas técnicas que garanticen la identificación y la autenticidad de la voluntad declarada, pero no hace ninguna regulación legal de la Firma electrónica.

El articulo 6 del Acuerdo EDI de la Comisión de las Comunidades Europeas , que determina la necesidad de garantía de origen del documento electrónico , tampoco regula la firma electrónica.

Que tampoco contempla la Directiva 97/7 CE, ni la ley 7/1996 al hablar de contratos a distancia .

La futura ley General de las Telecomunicaciones, parece ser, será quien regulara las Técnicas Criptográficas.

Aunque la política criptológica en algunos países se regula en Leyes de comercio como EE.UU. aunque antes tuviera tratamiento legal de munición, que aun conserva Francia.

En cualquier caso la OCDE, propugna activamente el desarrollo de políticas criptográficas y la no obstrucción a su establecimiento.

Algunos Estados de EE.UU. y Alemania ya han elaborado las primeras leyes sobre firmas electrónicas. Aunque en Alemania este en suspenso por un recurso de competencias legales planteado recientemente.

Y aunque jurisprudencialmente (STS .5-2-1988, ponente Ruiz Vadillo) , en base a que las relaciones de medios probatorios legales no son exhaustivas , se admita la aportación a juicio del documento electrónico, con tal que sea autentico, su obtención haya sido licita, y se observe el principio de contradicción, se hace necesario dotarle de las condiciones necesarias para su irrefutabilidad.

6. REDES

Las redes con formatos y estándares de comunicación TCP/IP, en especial Internet y en general las nuevas tecnologías :

-como objeto del derecho producirán una regulación especifica nueva.

Esta regulación jurídico positiva compromete en parte, y este es nuestro cometido , a la teoría general de los contratos y obligaciones; y a su cumplimiento con dinero electrónico así como a la valoración de la prueba de este nuevo hecho, donde la extensión de la red, determina el posible ámbito territorial de formación de la voluntad contractual.

-como instrumento del Derecho posibilitara la contratación electrónica independientemente de la ubicación de las partes y por tanto el nacimiento de derechos y obligaciones en una nueva dimensión, con una representación no solo textual o alfanumérica sino visual, pictórica, audible, etc. que hace que nos movamos a través de sonidos , imágenes, texturas , colores en definitiva información multimedia, hipermedia y realidad virtual, alejada de las presentaciones tradicionales o analógicas

7. SEGURIDAD

Pero toda esta infraestructura, es un eslabón sensible a errores y a la manipulación en la contratación, por lo que los datos de carácter personal y patrimonial, quedan expuestos. Para evitar esto, se van imponiendo políticas de seguridad, basadas en cortafuegos, autoridades certificadoras, y criptología, sin que exista todavía un estándar.

8. RESPONSABILIDAD

La contratación electrónica, implica, por otra parte una serie de contratos y servicios interpuestos , como alta en Telefónica , alta en Los " proveedores de acceso", alta en "servidores" o host que proporcionen los bienes o servicios en la red , nodos , router, etc, que determinaran las posibles responsabilidades jurídicas de cada uno.

9. ADAPTACIÓN NORMATIVA

El Código Civil por su depurada elaboración, ha resistido los embates del tiempo y las innovaciones tecnológicas, si acaso ahora con las nuevas tecnologías, en algún extremo concreto, necesite la intervención del legislador.

Nos referimos fundamentalmente a la :

-La firma electrónica y su equiparación con la manuscrita
-A la consideración de original y copia (todo son clónicos)

-A la forma desmaterializada ; que nos lleva a la conclusión de que el soporte de la contratación electrónica tendrá que ser digital.

-A la forma constitutiva y ad probationem

-Al "Acta publica" electrónica , y los protocolos notariales en soporte electrónico .

-A la regulación de la valoración de la prueba de medios electrónicos informáticos o telemáticos.

-A las terceras partes confiables ; autoridades certificadoras. En la idea de una red de confianza basada en una estructura jerárquica de certificación.

-A la esencialidad del mensaje donde las condiciones generales deben quedar perfectamente definidas sin romper el equilibrio entre las partes.

-El poder liberatorio del dinero electrónico .

10. LUGAR Y LEGISLACION APLICABLE

El lugar del contrato será donde se hizo la oferta a tenor del 1.262 del Código Civil, y siguiendo normas de Derecho Internacional Privado , la "lex rei sitae" del articulo 10 del Código Civil en sus cuatro primeros números .

Importante por cuanto con estas nuevas tecnologías , es perfectamente viable que se contrate desde el avión , buque , ferrocarril o automóvil quedando sometidos entonces a la ley del lugar de abanderamiento , matricula o registro y siendo por carretera en el lugar donde se hallen.

Del mismo modo la norma de derecho internacional privado "locus regit actum" recogida en el art. 11, contempla en la nueva redacción excepciones como el sometimiento a la ley que rige el contenido, a la ley personal del disponente en actos unilaterales y a la ley común de los otorgantes ,o al lugar donde radiquen los inmuebles.

No obstante, lo habitual, en la contratación electrónica, será el sometimiento expreso a una legislación y jurisdicción determinada. (art. 10-5 del código civil) (art. 57 Ley de Enjuiciamiento Civil).

En el art. 63 de la L.E.C. se dan reglas para los otros casos.

En el plano internacional fuera de nuestro Código Civil, el convenio de Roma de 19 de Junio de 1980 , en defecto de pacto rige la relación o "vínculos mas estrechos" , para la determinación de la legislación aplicable;

El Convenio de Bruselas art. 5 determina como tribunal competente el del lugar en que debiere ser cumplida la obligación, etc.

11. EFECTO TRANSNACIONAL, ALDEA GLOBAL

Pero la eficacia normativa , en un plano global determinado por Internet, es muy discutible . Constituyendo el efecto "aldea global", o efectos transnacionales, que provocan la aparición de paraísos informáticos, que demandan urgentemente una solución legal.

La directiva 97/7/CEE , sobre protección de los usuarios en materia de contratos a distancia en su art., 12.2 indica que "Los Estados miembros adoptaran las medidas necesarias para que el consumidor no quede privado de la protección que otorga la presente directiva por la elección de un país tercero como Derecho aplicable al contrato, cuando el contrato presente un vinculo estrecho con el territorio de uno o mas estados miembros" . Introduce una protección contra la exclusión voluntaria a la ley aplicable al contrato , e INSTA el desarrollo(C21), de procedimientos fiables EXTRAJUDICIALES eficaz para la tramitación de RECLAMACIONES TRANSFRONTERIZAS, en línea con el "Plan de acción sobre el acceso de los consumidores a la justicia y la solución de litigios en materia de consumo en el mercado interior" publicado por la comisión el 14 de Febrero de 1996.

Se deja para estudio posterior la viabilidad de la cuestión de las RECLAMACIONES en la venta a distancia se de. (ART. 17), sin indicar ningún procedimiento .

Independiente de la cuestión de la nulidad del contrato que conllevaría esta conducta por contraria al orden publico según el art. 6.2 del Código Civil o por realizarse en fraude de ley Art. 6.3. o 12.4 C.C. El hecho es que, el efecto seria difícilmente perseguible, por no decir imposible en un contrato celebrado y cumplido en país distinto por voluntad de las partes.

Como por ejemplo:

-La venta de la publicación electrónica de la biografía de Miterrand por su medico desde un servidor de Internet fuera de Francia para eludir la prohibición de publicación, que fue un éxito.

-La compra en Internet de fármacos prohibidos, como la hormona melantonina o sematropina de crecimiento o de cualquier clase sin receta. Publicado el 15-5-1997 por el diario "Cinco Días" y recogido por el diario "El País" 16-5-1977.

-O como en España ,El 26 de Mayo de 1997 , que Sanidad ha incautado dos productos milagro (Friatroy contra el SIDA y el cáncer y Life Plus reguladora de la glucosa y colesterol) que se producían en un laboratorio en Ibiza y vendían desde Miami (EE.UU.) a través de Internet . Los anuncios de venta en Internet, contravenían la normativa sobre sanidad y publicidad de medicamentos Española, así como la ley 25/1990 de 20 de Diciembre del Medicamento que impediría la venta a distancia (venta indirecta) . Así mismo la directiva 92/28/CEE del Consejo de 1 de Marzo de 1992, relativa a la publicidad de los medicamentos para uso humano (DO nº. L113, de 30-4-1992) que prevé prohibiciones en materia de medicamentos. etc.

-O el caso, publicado en el país el 9 de Junio de 1997 de la secta religiosa con sede en Suiza denominada "Rael" que oferta a través de Internet para cualquier país del mundo , la venta del servicio de clonación para parejas estériles humanas. Donde La clonación la realizaría la empresa Valiant Venture Ltd. con sede en las Bahamas EE.UU.

Muchos países no disponen de leyes propias sobre aspectos ligados a la biomedicina . Así el pasado 11 de Marzo de 1997 la asamblea del Consejo de Europa instó al comité de Ministros para que el futuro protocolo sobre la protección del embrión humano prohiba la clonación humana y el 4 de Abril de 1997 en Oviedo una quincena de países firmo el Convenio Internacional sobre Derechos humanos y Biomedicina , destinado a proteger a las personas contra posibles abusos en las distintas aplicaciones biológicas y medicas , al cual podrán sumarse el resto de los cuarenta países del Consejo de Europa y otros ; el reciente Proyecto de Directiva del Parlamento Europeo (Julio 97) sobre productos obtenidos a partir de seres vivos , excluye la posibilidad de clonación reproductiva de seres vivos. Pero CON QUE SOLO HAYA UN PAIS que no asuma la regulación internacional, permitirá una actividad o contratación ilegal a través de Internet con efectos en los demás países.

Como soluciones, se piensa en un derecho Global, pero no es fácil. Así se ha demostrado en el caso de la protección de los derechos de autor, donde no solo las industrias sino los diferentes gobiernos están divididos, como patentizo la conferencia de Ginebra. Así mientras Estados Unidos primer exportador de propiedad intelectual apoya la protección de derechos de autor , los países en vías de desarrollo, accesibles a través de Internet, no tienen el menor interés en defender copyrights extranjeros.

Otra solución puede venir de dentro de la propia técnica surgiendo así otro modo de regular, que la industria impondrá, ante las dificultades de encontrar una solución legal.

Así se esta ensayado con distintos fines la introducción de "Chip,s" en las obras multimedia; o para controlar la información como : el Chip V ; o los de cifrado como el EES. KES.Capstone ; o el chip Clipper; o el "software" especializado como los PICS (Plataforma para la Selección de Contenido) que permite a cada usuario crear su propia lista de contenidos con accesos codificados. Pero en estos casos se necesita cooperación y en el caso de acciones ilícitas se trabaja desde el anonimato, perjudicando seriamente la parte de negocio legal de la red.

A nosotros nos preocupan soluciones de este tipo , fuera de un control legal. Pero como decimos , existe escepticismo en las soluciones legales, dentro de Internet con la afirmación de que no se pueden poner "puertas al campo"

Así la "Ley de reforma de las comunicaciones" (ley de decencia, para prohibir pornografía) que el presidente Bill Clinton firmo con un bolígrafo electrónico sobre una pantalla de cristal liquido el 8 de Febrero de 1996, en un dialogo interactivo con el ordenador de la Biblioteca del Congreso, hoy esta recurrida por la Asociación de Derechos Civiles de América , por el atentado que supone a la "libertad de expresión" como así mismo ha sido objeto de una enmienda la prohibición de dar información sobre el aborto, por cuanto este esta legalizado y reconocido. Provocando reacciones solidarias.

Hasta ahora Internet parecía despertar sentimientos de cooperación, nosotros nos preguntábamos si ¿seria el espíritu caballeroso que anima a los pioneros?, o si ¿verdaderamente se estaría creando un espacio común altruista a respetar por todos? .

En este sentido, Pérez Luño (1996) " ve que las redes de telecomunicaciones pueden producir un movimiento solidario basado en la respuesta a

las utilizaciones indebidas en la red, y así mismo la solución a problemas de uso de la red puede producir reglas consuetudinarias alejadas de la dimensión coactiva de las normas estatales y mas próximas a su acatamiento por convicción," (Colom y Van Bolhuis 1995).

No obstante creemos que la solución está en establecer con prontitud normas positivas de regulación de la contratación electrónica , desde una óptica comunitaria y global, pero con respeto a la diversidad de culturas e intereses nacionales .

La economía ya ha alcanzado un nivel de globalización muy importante. La comunidad científica también. Esperemos que pronto lo consiga la regulación jurídica y así evitaremos que la red albergue esos "paraísos informáticos" en donde se pueda burlar las regulaciones legales a través del "servidor" instalado en un ámbito no sujeto a esa legislación restrictiva y poder sancionar estas acciones transfronterizas.

12. COMENTARIO DIRECTIVA 97/7

La reciente Directiva 97/7 de 20 de Mayo 1997 RELATIVA A LA PROTECCION DE LOS CONSUMIDORES EN MATERIA DE CONTRATOS A DISTANCIA (DOCE L 144/19 de 4 de 6- 1997) constituye la primera regulación que afronta la venta a distancia con carácter especifico y donde se menciona expresamente el correo electrónico y por tanto una forma de contratación electrónica, aunque sin contemplar las herramientas de ultima generación, ni las cuestiones fundamentales de la contratación electrónica. Mas preocupada por las técnicas telefónicas y bajo catalogo.

-La Directiva, DEFINE los contratos negociados a distancia (c9) en el (art. 2): como los que se celebran utilizando técnicas de comunicación a distancia sin presencia física simultánea, entre un proveedor y un consumidor sobre bienes o servicios en el marco de un sistema de ventas o prestación de servicios organizado por el proveedor .

-Destaca la indicación de "sin presencia física simultánea", también recogida en nuestra ley 7/96, art. 38 , ya que alguna reciente sentencia considera que la conversación por teléfono se asimila a presencia, concepto que algunos autores de origen informático, quieren también ampliar , a nuestro entender erróneamente, a la simultaneidad y contemplación que determina la video-conferencia.

La presencia o ausencia entendemos se debe referir siempre a la parte corporal orgánica, que es lo que caracteriza estos contratos.

La Directiva (art. 3) EXCLUYE de esta consideración los contratos sobre:
-servicios financieros;
-distribuidores automáticos
-con operadores de telecomunicaciones para utilizar teléfonos públicos
-los referentes a Bienes Inmuebles excepto el arriendo;
-subastas.

y Excluye parcialmente de la aplicación de los artcs. 4, 5, 6, apt1-7 sobre información y derecho de resolución) , los -productos alimenticios ;-bienes de consumo corriente y los de alojamiento, transporte y esparcimiento.

-Nos parece correcta la no exclusión de estos últimos productos del resto del ámbito de la directiva , pues su formalización sigue siendo mediante técnicas a distancia, lo que nuestra ley erróneamente no recoge, pero que en cambio amplia la exclusión a los productos a medida.

-Lógicamente esta excluido también el comercio al mayor, (business to business) y otras modalidades de comercio , ya que lo que se pretende con la directiva es la protección de los consumidores finales, sobre todo contra envío de mercancía o prestación de servicios no encargados y contra métodos agresivos de venta.

COMO CUESTIONES A DESTACAR ESTÁN :

- El DERECHO DE RESOLUCIÓN, en un plazo mínimo de siete días a contar desde la recepción, sin penalidad ((c14), (art. 6) y art. 44).
Sin perjuicio de los derechos ya existentes, frente a productos y servicios deteriorados, o que no correspondan a la descripción de la oferta.

-La falta de contacto real con el producto o servicio a la hora de contratar, fundamenta este derecho de rescisión.

--La ley 26/1984 de 19 de Julio para la Defensa de los Consumidores y Usuarios Art. 10.1.c , al contemplar la venta por correo , considera como cláusula no abusiva el derecho de resolución, lo que entendemos extrapolable al contrato a distancia.

Tiene EXCEPCIONES este derecho como (ART. 6-3 d): el acuerdo, las fluctuaciones de coeficientes, los encargos, o los que puedan ser copiados -como los programas-, o pierdan la actualidad, o las lotería y apuestas.

-Estas excepciones serán efectivas "salvo pacto en contrario" .

Otro capitulo Muy Importante en la "Venta a Distancia" es la INFORMACION .

-Aunque estas técnicas a distancia pueden favorecer la exhaustividad en la INFORMACION frente a los métodos analógicos, lo cierto es que la ausencia corporal de la persona y del bien exige garantizar un mínimo de información, por la falta de la información añadida que proporciona la inmediatez física.

Hay obligación de informar al consumidor del derecho de resolución: (art. 5 -1 de la directiva) y (art. 47-c) ; de la directiva y de los Códigos de Conducta existentes, art. 16.

Además, con carácter previo, se informará (art. 4) , mediante cualquier medio, en forma clara y sujeta a la buena fe y respeto a los menores (incapaces) de la: a) Identidad del proveedor (domicilio si hay pago adelantado). b) Características esenciales del bien o servicio. c) Precio. d) Gastos de entrega. e) Modalidades de pago, entrega o ejecución. f) Derecho de resolución. g) Coste de utilización de la técnica de comunicación. h) Plazo de validez de la oferta y i) duración mínima.

- La obligación de indicación del coste de la técnica de comunicación, es acertada , en contra de nuestra Ley de Ordenación del comercio minorista que dispensa de ello cuando "es evidente", y que tampoco indica la duración mínima del contrato cuando sea necesario.

Por ultimo hay obligación de (art. 5) confirmar, por escrito, la información referente a la identidad; al derecho de resolución; a la dirección geográfica; al servicio posventa y a las garantías comerciales.

-Nos parece correcto que se permita su cumplimiento no solo por escrito sino con técnicas digitales, al expresar ..."mediante cualquier soporte duradero" como puede ser un CD ROM. Lo que no contempla nuestra L.O.C.M. que la exige por escrito solamente.

-La exigencia de expresar la dirección del establecimiento debería completarse con la del domicilio social , la del e-mail y la del "Web site" , pues puede darse el caso en Internet, que no se tenga establecimiento, como los vendedores "on line" .. Nuestra ley (en el art. 47) , no así la Directiva (art. 4 y 5) , determina que se de también la dirección del domicilio social del proveedor.

-Para garantizar el cumplimiento de las obligaciones en este tipo de contratos , se exige la información sobre el servicio pos venta y garantías comerciales . En cambio nuestra ley no lo hace , fuera de la consideración general de seis meses y la necesidad de establecer un servicio técnico, expresada en el art. 12.

-Toda exigencia de la mayor cantidad de información , es deseable , por la "esencialidad" de los mensajes, en la contratación electrónica ,que provoca, que las condiciones generales, no llegue a conocerse, o sea impuesta por el proveedor.

En este sentido La ley de consumidores 26/1984 en su articulo 10 determina que las cláusulas de carácter general, deben ser claras .

Para la publicidad y marcado habrá que tener en cuenta también el Decreto 2.807/72 de 15-9-72 y la Ley de Consumidores 26/1984, artículos : 10 ; 11; 13 ; 15 y 22

-Estamos de acuerdo en acrecentar la buena fe en estas transacciones y proteger a los menores, incapaces.

-El incumplimiento de estos requisitos de información y documentación serán sancionados por vía del art. 64-h, 65-1.ñ y art. 68 de nuestra ley .

-La potencia de las técnicas multimedia (realidad virtual) exige una prevención especifica frente a la posibilidad de que puede inducir a contratar por la confianza en ella depositada mediante publicidad que puede considerarse engañosa. A lo que habrá que tener presente la Directiva 84/450 CEE sobre publicidad engañosa y concordantes.

En este sentido aunque en un caso de documentación escrita (analógica) la reciente sentencia del TS sala 1 de 8 de Noviembre de 1996 ha condenado a la entrega de lo anunciado en folletos de propaganda. Lo que puede predicarse para la información en Internet, quedando para ejecución de sentencia la determinación de la prestación sustitutoria de no poderse llevar a efecto la prestación especifica.

Para los Ficheros con fines de publicidad usados en esta contratación también se tendrá en cuenta el (Art. 29),de la LORTAD 5/1992 que restringe la fuente del dato a los accesibles al publico o facilitados por el interesado.

-En cuanto a la INTIMIDAD

-La directiva reconoce la defensa de la intimidad y La protección a la vida privada según los artcs. 8 y 10 del Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales de 4 11-50. señalando que los que no deseen ser contactados puedan ser protegidos de forma eficaz .

-Hoy las empresas están renovando las formas en que se dirigen al mercado, con un nivel de eficacia y procesamiento de la información impensable hace muy poco.

El procesado de esta información y los perfiles consecuentes deben atenerse a la normativa existente, permitiendo el derecho de control efectivo, por el consumidor de la información que le concierne y de la que quiera recibir.

En el sentido del -Art. 18.4 C.E. -Art. 1 y Titulo III de la LORTAD ; y el R.D. 1.332 /2O en su desarrollo. Con la salvedades del art. 7 - y las matizaciones del art. 15 de La Directiva 95/46/CE de 24-10-95 de tratamiento de datos personales , que permite la decisión que se haya adoptado en el marco de la celebración o ejecución de un contrato a instancia de la parte .

El Art. 39.3 de nuestra Ley OCM 7/1996, aunque considera el nombre apellidos y domicilio de las personas que figuran en el censo electoral como datos accesibles al publico en los términos de la LORTAD 5/1992 , hay que considerar el Padrón como fichero de titularidad publica art. 3.b. Regulado por la ley 4/1996 de 10 de Enero, y debe considerarse confidencial .

El censo electoral participa de esta confidencialidad , así el art. 41 -2 de la Ley Orgánica 5/1985 de 19 de Junio , del Régimen Electoral General determina que queda prohibida cualquier información particularizada sobre los datos personales contenidos en el censo electoral , lo que ha provocado que este 39.3 de Nuestra Ley OCM esté recurrido en el T. Supremo por el expresado conflicto con la ley electoral respecto al carácter que se da a esta información.

Del art. 10 de la Directiva se deduce la prohibición de publicidad por fax , por correo electrónico o telefonía automática, no pedida, al imponer la necesidad de autorización previa .

El PLAZO máximo DE EJECUCIÓN del contrato se establece en treinta días, (art. 7) (art. 43). Si se agota el producto, se devolverán las cantidades si no se ha especificado un cumplimiento sustitutorio.

-La difícil comprobación por el usuario de la disponibilidad o no del producto , deja en manos del comerciante el cumplimiento con un producto u otro alternativo si así se ha previsto, pues el art. 11-3,a no prevé en este caso la inversión de la carga de la prueba.

Piénsese que el alcance de la oferta en Internet por su carácter global puede tener una respuesta altísima que tiene que ser previsto en la oferta .

Fomenta la vía paccionada de CODIGOS DE CONDUCTA, (C18)para la protección de los consumidores en el sentido de la Recomendación 92/295/CEE relativa a códigos de conducta

LEGITIMA (art. 11) a Organismos públicos y Organizaciones de Consumidores o profesionales con interés legitimo a velar por la aplicación de la Directiva.

INSTA el desarrollo(C21), de procedimientos fiables EXTRAJUDICIALES eficaz para la tramitación de RECLAMACIONES TRANSFRONTERIZAS, en línea con el "Plan de acción sobre el acceso de los consumidores a la justicia y la solución de litigios en materia de consumo en el mercado interior" publicado por la comisión el 14 de Febrero de 1996.

Tiene presente la problemática de los EFECTOS TRANSNACIONALES art. 12-2 y paraísos informáticos, considerando (c22) que existe el riesgo de que la protección d la presente directiva , puede desaparecer .."...designando como ley aplicable al contrato el Derecho de un país tercero, cuando presente vínculos con uno o mas Estados miembros;" que por tanto es conveniente establecer disposiciones encaminadas a evitar dicho riesgo.

Contempla las PROHIBICIONES DE COMERCIALIZACION de determinados productos y servicios, especialmente en materia de medicamentos.

A tener en cuenta la Directiva 92/28/CEE del Consejo, de 31 de Marzo de 1992, relativa a la publicidad de medicamentos para uso humano.

Permite la anulación de un PAGO cuando se haya efectuado mediante la utilización fraudulenta de la tarjeta.(art. 8)

--Pero desconoce el resto de los distintos tipos de pago con dinero electrónico.

-Es acertado proteger la utilización del nº. de tarjeta del cliente, sin el consentimiento del usuario.

En cualquier caso, la reclamación se hará sobre los oportunos justificantes de compra, no sobre el estado de la cuenta bancaria del titular.

Penalmente , el art. 239 de Ley 0rganica 10/1995 del Código equipara las tarjetas magnéticas o perforadas a llaves falsas.

-La sustracción de la tarjeta y uso fraudulento por un tercero, civilmente podría tipificar una culpa concurrente y exigir por mitad la responsabilidad, por un lado del titular de la tarjeta al no comunicar su robo o perdida y por otro del establecimiento que la carga sin comprobar la firma.

Para ello se tendrá en cuenta que la reclamación se hará sobre los oportunos justificantes de compra, sin que otro tipo de anotaciones en cuenta sin el correspondiente reflejo documental tenga virtualidad al efecto de la reclamación.

Penalmente , el art. 239 de Ley 0rganica 10/1995 del Código equipara las tarjetas magnéticas o perforadas a llaves falsas.

No hay obligación de devolver El SUMINISTRO NO SOLICITADO (art. 9), la aceptación tácita no se permite.

-Contemplado en nuestra ley en el art. 41 Ley 7/1996.

-En este caso se preserva al usuario de la coacción que puede significarle el enviarle un producto sin que se haya pedido . Constituiría una donación a efectos

jurídico-civiles , aunque en algunos casos no se perfeccione si hay devolución y no aceptación .

En caso de error evidente del envío, se guardara, un mes, a disposición del vendedor. Teniendo que ser indemnizado en un 10 por ciento del valor de venta, o hacerlo suyo en caso contrario.

Reconoce en el considerando 22 la dificultad de dominar la técnica necesaria para este tipo de contratación a distancia, recomendando que la CARGA DE LA PRUEBA de la información previa pueda recaer sobre el proveedor.

IMPORTANTE es que el 113-b permite adoptar medidas para que el proveedor y operador de la comunicación , cuando puedan hacerlo , cesen las practicas contrarias a la Directiva.

Son (art. 12) IRRENUNCIABLES estos derechos .
Se da tres años como máximo, para la APLICACION (art. 15).

La cuestión de las RECLAMACIONES en la venta a distancia se dejan a estudio de su viabilidad . (ART. 17), sin indicar ningún procedimiento .

Ni la DIRECTIVA ni la ley contempla garantías del cumplimiento mediante FIANZA O un resarcimiento económico. Entendemos que considera suficiente el derecho de desistimiento para los casos en que no se corresponda el producto con las expectativas despertadas, pero en caso de incumplimiento de la obligación el perjuicio para el proveedor recaerá en la perdida de su fama o confianza.

No contempla el caso de que el proveedor pueda ser directamente el fabricante, lo que en estas ventas telemáticas, es muy factible. Nuestra ley sí contempla la venta directa.

La Directiva tampoco indica la necesidad de estar autorizados e inscritos para estas ventas, lo que se indica en nuestra ley de competencia de la Comunidad Autónoma, y cuando el ámbito sea Nacional del Ministerio de Comercio y Turismo. Pero hasta tanto se habilite un registro, habrá que estar a la norma del procedimiento administrativo común Ley 30/1992 de 26-11 y al Real Decreto 1778/1994 .

13. EPILOGO

Las leyes autonómicas y nuestra ley 7/1996 de 15 de Enero de ORDENACION DEL COMERCIO MINORISTA cuando se transponga la Directiva deberán reformarse y adaptarse , y entonces podría contemplarse mas específicamente la contratación electrónica .

Como así se hizo en la Orden de 22 de Marzo de 1996 aplicando lo ya contemplado en la ley del IVA 37/92 , y RD 80/96 que la modifica, con la factura electrónica, y su registro electrónico, importante decreto por cuanto legaliza el EDI.

Sin que quepa EXAGERARSE LA SEGURIDAD JURIDICA, en estas ventas que por lo general serán ínfimas, debe mantenerse la buena fe y la confianza en el sistema.

Señalamos, para terminar, la desigualdad social y dependencia creciente en la contratación electrónica, a tener o no acceso a estas nuevas tecnologías y a su correcto funcionamiento.

La avería telefónica el 10 de Octubre de 1966, en la red UNO al implantarse un nuevo software dejando sin servicio en España a bancos y cajas e interrumpiendo el mercado interbancario; O el caso del incendio de la sede Central del Credit Lyonnais en Francia dejando sin sistemas informáticos e inoperante a la institución financiera, nos da buena prueba de ello.

Se impone la sensibilización del jurista ante los progresos técnicos, en orden a regular esta nueva situación.

Y aunque sin compartir la total obsolescencia de la cultura alfabética que predica Bill Gates, sí debemos darnos cuenta de que algunas soluciones válidas para una cultura analógica no son extrapolables a una cultura digital.

Responsabilidad Civil en Materia de Informática

GUILLERMO OROZCO PARDO

Profesor Titular del Departamento de Derecho Civil.
Universidad de Granada

RESPONSABILIDAD CIVIL EN MATERIA INFORMATICA.

El presente trabajo, que supone una relectura sobre un trabajo nuestro precedente, tiene como objeto principal el de analizar la aplicación de los principios generales que inspiran al Derecho de Daños al campo de la informática en lo referido a las actividades de riesgo que en el seno de la misma se realizan. Es por ello que hemos considerado más adecuado dividirlo en dos partes. Una primera que tiene por objeto establecer el contenido y significado de los conceptos y figuras jurídicas más relevantes aplicables al campo de estudio, a la luz de las corrientes doctrinales, legales y jurisprudenciales más modernas.

En la segunda parte, hacemos una aplicación directa de las mismas a las tres actividades de riesgo más importantes a nuestro juicio: contratación de bienes informáticos, prestación de servicios y tratamiento automatizado de datos personales. Sólo aludimos a la disciplina contractual de estas materias en la medida en que ello ha sido necesario para nuestro estudio, pues la contratación de bienes y servicios forma parte de otro bloque temático del presente Curso, distinto al que nos da sede

Por otra parte, hemos de hacer constar que la perspectiva desde la cual se plantean estas líneas es la de proponer criterios de solución a los múltiples problemas que el tema puede plantear, en razón de ello hemos eludido el entrar en la exposición de una casuística dentro de la cual seguramente hubiésemos dejado muchos supuestos por destacar. Para ello partimos desde nuestra condición de jurista por lo que forzosamente el nivel técnico de la exposición no estará a la altura de muchos lectores, si bien nuestra intención es incidir en la dimensión cultural y ética de la informática como medio al servicio de la persona y no como un simple avance tecnológico. Esa coordinación ética entre los hombres que es el Derecho debe servir de punto de partida para extraer los principios necesarios a fin de que un avance tan decisivo como este sirva realmente a la sociedad para su mejora y desarrollo y no se convierta en un instrumento de poder de un sector científica y tecnológicamente más preparado para su utilización. Por otra parte, hoy más que nunca se hace necesario dotar al técnico de un código ético para regir la utilización y finalidad de su actividad y poner a disposición del ciudadano unos medios legales que le permitan obtener, cuando no impedir, la reparación de los daños en sus bienes y derechos que una utilización inadecuada de la informática pueda inferirle. Esa es la intención que persiguen estas líneas.

PRIMERA PARTE

I- INTRODUCCIÓN:

La amplitud de conceptos que sugiere el título que preside estas líneas hace que, ineludiblemente, iniciemos nuestra exposición poniendo de manifiesto que nuestro objetivo fundamental no es agotar la materia sino plantear o sugerir unas líneas de investigación y análisis que se deducen de la aplicación de la disciplina de la responsabilidad civil, contractual y extracontractual, al campo de las relaciones jurídicas que se plantean por medio de ese instrumento capital de nuestro tiempo que es la informática. Superado ya el tópico de su comparación con la imprenta, hoy debemos atender a unos fenómenos nuevos que se nos están presentando a todos, juristas o no, que generan una problemática a la que debemos dar una solución en base a esquemas legales surgidos en una época en la que la informática aún no existía.

Básicamente, la cuestión que nosotros vamos estudiar está referida a los daños que se infrinjan a la personas como consecuencia de la prestación de servicios o de la utilización de los medios informáticos. Se trata, de

un lado, de analizar la responsabilidad del profesional informático, en cuanto sujeto técnicamente capacitado para actuar en el campo de la prestación de servicios de esta naturaleza; y de otro de atender a las consecuencias que la fabricación y comercialización de "hardware" y "software" pueden ocasionar al usuario que los adquiere o utiliza por cualquier titulo legítimo. Finalmente, analizaremos la problemática de la responsabilidad de los titulares de los ficheros de tratamiento automatizado de datos de carácter personal.

Se trata pues, de partir de la base de la disciplina civilistica para extraer el "precipitado" básico de las normas de esta naturaleza y aplicarlo, con las debidas correcciones, a un fenómeno tan nuevo como la informática. Las relaciones entre informática y Derecho son múltiples y variadas y, de hecho, han originado que en los más modernos planes de estudios de las Facultades de Derecho se vaya abriendo, tímidamente, paso una nueva disciplina llamada "Derecho de la Informática o Derecho Informático" que atiende al estudio sistematizado de las relaciones jurídicas que surgen en este campo y a sus consecuencias.

Ello implica cuestiones de muy diversa índole: relaciones contractuales, protección de datos, propiedad intelectual e industrial de sus productos, delitos informáticos, etc... que plantean un desafío que hoy el derecho no llega a responder adecuadamente. Es mucho más que adaptarse a la nueva tecnología, supone un cambio de estructuras mentales a la hora de abordar tales temas, pero sin abandonar el principio base de toda disciplina jurídica: la protección y promoción de los valores de la persona; con ello se llegaría a una suerte de "humanismo tecnológico" imprescindible en una sociedad como la actual que cada vez más demanda la defensa del "mandato ético de la norma" frente a la vulneración o incumplimiento de la misma.[1]

Ciertamente, la influencia de la evolución tecnológica sobre las estructuras socioeconómicas ha ocasionado unas importantes consecuencias en las

■[1]Vid. Pérez Luño, A.E.:" Derechos Humanos, Estado de Derecho y Constitución".Madrid, 3ª ed. y " Manual de Informática y Derecho". Ariel, Barcelona, 1996; Davara Rodríguez:"Derecho Informático".Aranzadi, Pamplona, 1993; Frosini:" Cibernética, Derecho y sociedad". Madrid, 1982 y Diez Picazo:" Derecho y masificación social. Tecnología y Derecho privado.(Dos esbozos)". Cívitas, Madrid, 1979

mismas. Además ha supuesto la aparición de una complicada problemática que el Derecho no puede resolver fácilmente de acuerdo a las categorías y métodos tradicionales. Hoy cobran cada vez mas peso especifico en una sociedad, y en su economía, las llamadas nuevas tecnologías; así la informática ha supuesto que la información y su tratamiento sean un sector fundamental de manera que la dependencia tecnológica en este campo es también económica y política. Esta tecnología dirigida a la captación, tratamiento y almacenamiento de la información, se ha vuelto capital para cualquier país. Pero además, el trafico jurídico económico de la información y los productos informáticos ha cobrado una gran importancia de manera que los países "punteros" en la investigación y desarrollo de los mismos ocuparan el "primer mundo" del siglo venidero.[2]

Así mismo, es de destacar un fenómeno que la informática aporta y que parte de una idea que procede ya del siglo XIX: la vinculación entre máquina y función ya no es unívoca, es decir, la precedente ligadura de una máquina para cada función se rompe pues el ordenador se convierte en la máquina susceptible de desarrollar múltiples funciones diferentes con solo cambiar la antigua tarjeta perforada. De ahí surge la idea del software como conjunto de instrucciones que programan a la máquina para que desempeñe una tarea o función diferente según el caso. En consecuencia, software y objetivo se van identificando, siendo así que la frustración del fin perseguido puede deberse, más que al fallo de la máquina, a la inadecuada elección del programa que le instruya para realizar la función tendiente a lograrlo.

Por otra parte, tales fenómenos han producido unas consecuencias "nocivas" que el Derecho debe evitar o, cuando menos, sancionar según criterios de justicia. Surge así la necesidad de elaborar nuevas categorías científicas y dogmáticas que den respuesta a estas necesidades pues, aunque no lo parezca, no hay nada más práctico que una sólida construcción teórica. Es preciso disponer de todo un sistema que racionalice y unifique el tratamiento científico de esa diversidad de relaciones jurídicas que la informática viene originando: creación y producción de programas y equipos, prestación de servicios, trafico jurídico comercial, daños, responsabilidad, delitos informáticos, adquisición, tratamiento y transmisión de información automatizada, etc... forman un cúmulo de cuestiones que no pueden ser resueltas parcial y sectorialmente, sino que

■[2] Vid. Breton:" História y crítica de la informática". Trad.V.Villoria, Madrid, 1989.

precisan de un tratamiento unificado. Debe elaborarse una disciplina que conjunte las distintas normas que regulan estos fenómenos desde la unidad de conceptos, criterios, método y fuentes, y esta sería el Derecho Informático en el que se estudia todo el conjunto de principios y normas de carácter jurídico que regulan los distintos supuestos que la relación informática y Derecho origina.

Dentro de esta tarea debe encuadrarse nuestro trabajo que se inicia con una primera parte destinada a fijar el contenido y alcance de los conceptos básicos que se dan cita en el mismo: profesión, daño, responsabilidad, etc... son términos que el jurista conoce y domina, pero, supuesto que no todos nuestros destinatarios lo son, habremos de comenzar por fijar esos presupuestos básicos. Seguidamente, pondremos de manifiesto las líneas fundamentales de las cuestiones más relevantes que la conjunción de responsabilidad e informática plantea. Es decir, la responsabilidad del profesional, independiente o laboral, que presta sus servicios como tal; la del fabricante y comercializador de productos informáticos, sea como consecuencia del incumplimiento de su deber contractual o por una causa ajena al mismo. Finalmente, hemos de atender a la actividad de riesgo que supone el tratamiento automatizado de datos y sus consecuencias a efectos de responsabilidad.

No pretendemos realizar aquí y ahora un "tratado" de la cuestión sino de analizar los supuestos más importantes a partir de las categorías generales del Derecho Civil para aclarar conceptos y suscitar un debate científico y práctico de aquellas cuestiones problemáticas mas relevantes, a nuestro juicio, y de aventurar una solución por vía de aplicar unos principios legales, jurisprudenciales y doctrinales que se consideran más adecuados a falta de respuestas normativas específicas.

II- CONCEPTOS BÁSICOS:

Vamos a exponer aquí los conceptos que de una forma sustancial deben quedar fijados a efectos de poder aplicarlos posteriormente a los distintos problemas que surgen dentro de nuestra exposición. No tratamos de acotar ahora en toda su extensión términos tales como responsabilidad objetiva o subjetiva, sea contractual o extracontractual, pues ello supone una tarea muy superior a nuestros objetivos y posibilidades.

Conceptos tales como responsabilidad, objetiva y subjetiva, daños y perjuicios, y otros que aquí utilizamos, han de quedar fijados en su

contenido de la manera más clara posible para poder aplicarlos posteriormente al campo de la informática.

1- La Responsabilidad civil en su concepción actual.

Tradicionalmente, se vino ligando la idea de responsabilidad con la de culpa en la medida en que se entendía que sólo se había de responder de aquél daño conscientemente causado y que fuere imputable a un sujeto culpable, ello conformaría la llamada responsabilidad subjetiva o por culpa que se basa en el reproche culpabilístico a una conducta.

Paulatinamente, se ha ido evolucionando hacia una responsabilidad objetiva que hace abstracción de conceptos subjetivos, pues se basa en el resultado y la actividad: toda actividad que genere un riesgo y, por tanto, sea susceptible de producir un daño, debe contar con la consiguiente obligación de responder si éste se produce.

Actualmente, la doctrina más moderna defiende la idea de un único concepto de responsabilidad que se identifica con la idea de tener que cumplir una obligación o de compartir las consecuencias de esa obligación. Son los principios que inspiran una época en la que la tecnología, la contratación en masa, etc... han excedido con mucho los estrechos márgenes legales impuestos por el Código Civil, en razón de ello han de ser la doctrina y la jurisprudencia quienes desarrollen y modifiquen ese moderno Derecho de Daños, tal y como se deduce de la sentencia del Tribunal Supremo de 10 de julio de 1943, " precursora " de la tendencia objetivadora en nuestro foro.

El Derecho debe dar respuestas adecuadas a ese ineludible necesidad de seguridad que los ciudadanos demandan y ello ha llevado a consagrar nuevos principios en este campo, a tenor de ello han perdido peso específico elementos tales como la culpa, la causalidad, etc... en aras del principio pro dannato. En razón de ello, se afirma que " ya no hay que reparar porque existió antes una conducta reprobable, sino que hay que reparar a secas; que no se trata tanto de moralizar las conductas de los eventuales autores de los daños, como de asegurar las indemnizaciones a la víctimas...la indemnización adquiere el aspecto de un verdadero imperativo social".

Efectivamente, la solidaridad social impone la necesidad de asegurar la indemnización antes que discernir los fundamentos subjetivos de la misma y ello se debe a que "se ha perdido aquella concepción mágica o teológica de la mano de Dios para ver por todas partes las manos de los hombres. No hay, pues, razón sólida que aconseje la resignación".[3]

Pero es que además cada vez se dan más supuestos en los que concurren conductas de varios sujetos, sin que pueda determinarse con claridad siempre quién fue el responsable directo del daño, en razón de ello se ha consagrado un sistema de solidaridad para tales casos pues no cabe hacer una imputación adecuada. Así el empresario responde por los actos de su trabajador, la Administración por la de sus funcionarios, la sociedad por sus socios, independientemente de que quepa repetir después contra ellos, pues lo prioritario es asegurar la reparación. Por tanto, existen personas por quienes se ha de responder, según el imperativo del artículo 1903 CC y posteriormente cabe repetir contra ellas, conforme al 1904 CC. No se trata tanto de una culpa compartida ("in vigilando - in eligendo") cuanto de la necesidad de que la víctima no soporte sola las consecuencias del daño causado. Es por ello que la jurisprudencia se dirige contra todos los autores posibles: existe una pluralidad de obligaciones, cada una de ellas soportada por un sujeto diferente, pero con objeto idéntico, pues en todas ellas existe una misma obligación.[4]

No obstante, ello no debe llevarnos a consecuencias extremas, pues acentuar el rigor de estos principios llevaría ineludiblemente a que nadie pudiera o quisiera realizar aquellas actividades susceptibles de un riesgo tal que hace desaparecer el beneficio previsible o la motivación para actuar (v.gr. la cirugía cardiovascular, la atención en la UCI, etc...) Para "equilibrar" esta situación se consagra la teoría de la concurrencia de culpas o de causas, pues son supuestos en los que esta obligación de responder mitiga o desaparece al mediar la conducta de la víctima. Se debe resarcir todo evento dañoso en el que no aparezca clara la razón por la cual la víctima deba soportarlo sola.

■[3] Vid. Diez Picazo:" La responsabilidad civil hoy ".ADC 1979

■[4] Vid. Rogel Vide:" La responsabilidad civil extracontractual en Derecho español".Madrid, 1977

Esta situación nos ha llevado a una sociedad de seguros en la medida de todo el que realiza una actividad susceptible de crear un riesgo viene obligado a cubrir esa eventualidad mediante un seguro correspondiente: transporte, uso de automóviles, medicina, etc... son actividades que implican un mayor índice de factores de riesgo, en razón de ello la Ley o el propio sujeto aseguran esa eventualidad y su cobertura merced al oportuno contrato.

Haciendo una simplificación esquemática, podemos decir que para que se pueda hablar de responsabilidad es preciso que concurran tres presupuestos:

A- Un acto u omisión ilícitos: se trata de una conducta voluntaria por parte del sujeto que transgrede el mandato imperativo consagrado por la Ley: no dañar a nadie. Puede consistir en una conducta positiva, llevar a cabo un comportamiento, o bien omitir una actuación debida. No existe en el campo civil un "catálogo" de tipificación de conductas como sucede en el Derecho Penal, sino que se parte de ese tipo ideal de conducta diligente que se espera de un ciudadano medio. Así lo consagra la STS de 11/2/93 cuando afirma que la antijuridicidad no penal se funda en la transgresión del mandato genérico "alterum non laedere", sin que sea precisa la infracción de una norma jurídica concreta.

No obstante, el Derecho consagra determinadas circunstancias en las cuales se elimina el presupuesto de antijuridicidad que eximen al autor del acto: la legítima defensa, el estado de necesidad y el ejercicio del propio derecho, cuando este no se haga de una forma abusiva.

B- El daño: supone una perdida o lesión que sufre un sujeto como consecuencia de el acto lesivo. Como veremos posteriormente, consiste en un menoscabo de diversa índole que afecta a bienes personales o patrimoniales del sujeto.

C- El nexo causal: entre el daño y la acción debe haber un vínculo de causalidad en la medida en que esta ha sido la causa que origina la lesión o menoscabo. A veces hay varias causas que concurren a la producción del daño y en otros casos hay que discernir cual de ellas es la que lo ha ocasionado. En este tema existen dos posiciones: una teoría de la "equivalencia" según la cual se considera causa del daño toda acción que contribuye al resultado lesivo de suerte que, sin ella, no se habría producido. La teoría de "causalidad adecuada" defiende que el vínculo entre ambos ha de ser suficiente y adecuado de manera que la causa sea apta para

producir aquél daño que se le atribuye. Como dice la STS de 23/9/91 el resultado ha de ser una consecuencia natural, adecuada y suficiente de la acción.

Esta doctrina de la causalidad adecuada o eficiente es la que aplica nuestra jurisprudencia, tal y como nos recuerdan las sentencias del Tribunal Supremo de 30/12/95 y 3/5/97, pero, como dice esta última, " siempre termina afirmando que opta decididamente por soluciones y criterios que le permitan valorar en cada caso si el acto antecedente que se presenta como causa tiene virtualidad suficiente para que del mismo se derive, como consecuencia necesaria, el efecto dañoso producido y que la determinación del nexo causal debe inspirarse en la valoración de las condiciones o circunstancias que el buen sentido señale en cada caso como índice de responsabilidad, dentro del infinito encadenamiento de causas y efectos, con abstracción de todo exclusivismo doctrinal, pues, como se viene repitiendo con reiteración, si bien el art. 1902 descansa en un principio básico culpabilista, no es permitido desconocer que la diligencia requerida comprende no sólo las prevenciones y cuidados reglamentarios, sino además todos los que la prudencia imponga para prevenir el evento dañoso, con inversión de la carga de la prueba y presunción de conducta culposa en el agente, así como la aplicación, dentro de unas prudentes pautas, de la responsabilidad basada en el riesgo, aunque sin erigirla en fundamento único de la obligación de resarcir". Con ello se pone de manifiesto esa línea objetivizadora de la responsabilidad que trasciende el mero fundamento culpabilista, pero sin llegar al extremo de dotarla de una "rigidez" que pudiera llevar a consecuencias injustas. La clave, pues, no está solamente en la conducta típica definida por el "standard jurídico" de la diligencia debida, tal y como nos recuerda la sentencia antes citada cuando afirma:"... todo lo cual permite entender que para responsabilizar una conducta, no sólo ha de atenderse a esa diligencia exigible según las circunstancias personales, de tiempo y lugar, sino, además, al sector del tráfico o entorno físico y social donde se proyecta la conducta para determinar si el agente obró con el cuidado, atención y perseverancia apropiados y con la reflexión necesaria para evadir el perjuicio".

Por tanto, quiere decir el Supremo que cuando consta la conducta omisiva del sujeto, unida a la inversión de la carga de la prueba. a la presunción de culpabilidad y a la teoría del riesgo, surge la obligación reparadora.

Este nexo se "rompe" cuando interviene un elemento externo que puede ser el caso fortuito o fuerza mayor, entendidos como eventos imprevisibles o inevitables no imputables al sujeto, la acción de un tercero y la

conducta del propio perjudicado, si bien estas dos últimas han de ser valoradas para conocer cual es su grado participación en el evento dañoso.[5]

D- La culpa: supone una mayor o menor consciencia de inobservancia del deber de actuar con la diligencia exigible adecuada al caso. Se habla de dolo cuando el sujeto prevé la posibilidad de producir el daño y tiene intención de causarlo. Hay culpa cuando se omite la diligencia debida y se produce un daño no querido pero previsible.

Toda vez que concurren estos elementos surge la obligación de reparar el daño ya sea específicamente, la misma cosa o bien dañado, o por su valor económico; tal y como afirma la STS de 6/5/97 la indemnización debe tender a restaurar el estado anterior al evento dañoso, comprendiendo las reparaciones y las pérdidas de ingresos, si bien estos límites pueden "infringirse" en ciertos casos (v.gr. razones de urgencia SAP Málaga, Sec. 6ª, de 30/12/96). Para ello se atiende al acuerdo de las partes o al criterio de los Tribunales, pero sin entrar a valorar el grado de culpabilidad del sujeto, pues hoy se ha producido la objetivación de este fenómeno.

Veamos a continuación, siquiera brevemente, los tipos de responsabilidad civil que serían aplicables al objeto de nuestro estudio.

2- Responsabilidad civil contractual y extracontractual.

Tradicionalmente se ha venido distinguiendo entre débito y responsabilidad entendido aquél como el deber de cumplir la prestación convenida por el contrato y ésta como la obligación de resarcir las consecuencias del incumplimiento soportando el deudor ese poder de agresión conferido al acreedor para obtener el resarcimiento. Por ello algunos autores plantean el hecho de que fuera del contrato no hay responsabilidad, sino un deber jurídico de resarcir sancionado por la Ley para cada caso. Para ellos la responsabilidad contractual es un medio de garantía para el acreedor que funciona después del incumplimiento contractual, mientras que el acto ilícito produce el deber de reparar el daño por imperativo legal y, por tanto, sería una obligación legal. No

[5] Vid. Díaz de Lezcano, I.:" El caso fortuito y la fuerza mayor en el Código civil". S. Cruz de Tenerife, 1990

obstante, la doctrina actual ha elaborado una categoría intermedia que sería la conducta social típica que basándose en el contrato entronca con la obligación legal y que se deduce de algunos preceptos del Código Civil como luego veremos.

A tal efecto, hemos de tener en cuenta que la realidad social de nuestros días, merced a la evolución tecnológica, presenta multitud de supuestos no incardinables fácilmente en las dos categorías arriba enunciadas. Así nos lo recuerda la SAP Granada, Sec. 3ª, de 11/3/97 cuando afirma que "la temática reparadora de este litigio no se puede incardinar en uno solo de los dos clásicos campos de la culpa - contractual y extracontractual - entendidos como contrapuestos, sino que el fenómeno es más complejo y al igual que ocurre en el acontecer cotidiano de la vida presente, donde el devenir fáctico se anticipa a toda regulación jurídica, de ahí que un principio básico en nuestro ordenamiento es la interpretación de las normas conforme a la realidad social del tiempo en que han de ser aplicadas - art. 3.1 C.C. - es incuestionable que el Juzgador ante el dato objetivo del perjuicio sufrido, tenga que admitir la intercambiabilidad de los principios que inspiran la culpa y sin llegar a una objetivación de la responsabilidad en el orden civil, los conceptos de solidaridad, inversión de la carga de la prueba, adopción de las más mínimas precauciones, riesgo creado, etc... sean comunes a la culpa contractual y extracontractual, al igual que la regulación derivada de los artículos 1103, 1104,1106 y 1107 del Código no sea de exclusiva aplicabilidad a la culpa convencional, sino que abarca a las obligaciones que nacen en acto ilícito.... pues la parca regulación del Código civil impone integrar las lagunas existentes mediante la aplicación analógica de los preceptos relativos a las obligaciones en general, dado que, aún existiendo indiscutibles y claras diferencias entre la responsabilidad contractual y extracontractual, no pueden negarse también las grandes semejanzas que posibilitan esa aplicación analógica que ciertamente evitará, en el caso del art.1103, resultados contrarios a la equidad ".(Cfr. STS 20/6/89)

A - <u>La responsabilidad contractual</u>:

Lo cierto es que, como dice DE ANGEL, ésta surge cuando se incumple el deber de conducta impuesto por el contrato, pero para valorar ese incumplimiento no sólo cabe atenerse a las cláusulas expresas del convenio, sino a todo aquello que, según su naturaleza, a tenor del artículo 1258 CC sean consecuencias derivadas del mismo merced a la buena fe, el uso y la Ley. Esa buena fe no implica sólo honradez y rectitud, sino también crédito, confianza, fidelidad y lealtad en cuanto actitudes exigibles a las partes a la hora de la

ejecución del contrato. Ello quiere decir que ambos han de colaborar cumpliendo todas aquellas obligaciones que sean precisas para lograr el cumplimiento adecuado y satisfactorio del contrato y sus fines.(STS 9/12/63)[6]

Aquí la buena fe actúa como un modulo objetivo que sirve para amortiguar el rigor de las normas, incluido el "ordenamiento contractual", indicar a las partes la conducta que han de observar y servir de límite para evitar un ejercicio abusivo del propio derecho y la utilización del dolo.(STS 8/4/88) Por ello la jurisprudencia sostiene que incide especialmente en el modo de obrar en la ejecución y cumplimiento del contrato, dando a éste cumplida efectividad para lograr los fines propuestos, " por lo que deben estimarse comprendidas en las estipulaciones contractuales aquellas obligaciones que constituyan su lógico y necesario cumplimiento".(STS 9/12/63)

Como afirma la SAP de Valencia, Sec. 8ª, de 10/5/97 " en el cumplimiento de los contratos ha de emplearse la diligencia exigible ordinariamente, aún sin pacto al respecto", pues el artículo 1258 C.c. así lo impone por ser consecuencias que, conforme a la naturaleza del contrato, se derivan de la buena fe, el uso y la Ley.

La SAP de Palencia de 17/5/97 define la negligencia contractual como aquella derivada del artículo 1104 del Código civil en los siguientes términos:" debe ser entendida la actitud culposa en la realización de un contrato... como aquella acción u omisión realizada de forma voluntaria, libre y sin malicia por una de las partes contratantes, de la que se deriva daño o lesión a otra parte contratante, teniendo la característica la acción u omisión de que pudo ser evitada".

En aplicación de esta doctrina la STS de 15/7/85 mantiene que se atenta contra la buena fe y se incumple el contrato cuando no se entrega en el edificio construido la instalación de ascensores, que son instrumentos necesarios para el uso y disfrute de los pisos comprados aunque en las escrituras no se aluda al ascensor, pero todos los datos concomitantes acreditan que estaba prevista su construcción, así como en la propia construcción hecha , dotada de hueco para tal aparato elevador," por lo que su instalación no es consecuencia del contrato sino

[6] Vid.:" La Responsabilidad Civil". Deusto, 1989

contenido del mismo". De esto se deduce que el contratante que cumple su prestación (por ejemplo, paga el precio) ha de recibir todos aquellos elementos accesorios al principal que adquiere para poder lograr el fin propuesto en su adquisición cuando este venga previsto en el contrato. Cuando se adquiera el equipo informático para su aplicación a fin determinado y acordado por las partes, el comprador debe recibir todo aquello que sea preciso par que ese equipo despliegue la aplicación necesaria para ello. Tal sería el caso de la empresa que requiere al proveedor los aparatos y programas necesarios par informatizar la contabilidad y gestión de su actividad.

Esto quiere decir que la buena fe no sólo esta referida a un modo de ser o estar en el seno de las relaciones jurídicas, sino que es además un modulo objetivo de valoración de conductas y un medio de integración del contrato en la medida en que incorporan al mismo estipulaciones no previstas expresamente, pero que se han de considerar integrantes de este según los parámetros establecidos por el artículo 1258 CC. En este sentido, dice GETE ALONSO que en el contrato sobre bienes informáticos el proveedor tiene que cumplir unos deberes que no se agot n con la entrega sino que además tiene el deber de consejo e información. La información implica el poner en conocimiento de la otra parte la naturaleza y características del bien, su adaptabilidad, posibles fallos y carencias, errores, alcance, riesgos, así como precauciones a adoptar y actividades a desarrollar.[7]

El consejo conlleva una ayuda partiendo del análisis de las posibilidades y necesidades del cliente para determinar cuales son los equipos y medios más adecuados, incluso cuando el cliente pretenda un equipo inadecuado debe ser aconsejado, salvo que le acompañe un especialista o auditor en informática que le haya trazado un plan específico de informatización. Obviar este deber, o utilizar una publicidad engañosa que exagera propiedades, atribuye funciones que no posee, u oculta fallos o carencias del producto, sería incumplir el contrato por aplicación del artículo 1598 CC pues se trata de responsabilidad contractual, no extracontractual, y del artículo 8.1 de la Ley 26/84 de Consumidores y Usuarios que dispone:

■[7]Vid." La contratación en materia informática".La Ley,1992

" 1. La oferta, promoción y publicidad de los productos, actividades o servicios, se ajustarán a su naturaleza, características, condiciones, utilidad o finalidad, sin perjuicio de lo establecido en las disposiciones sobre publicidad. Su contenido, las prestaciones propias de cada producto o servicio, y las condiciones y garantías ofrecidas, serán exigibles por los consumidores o usuarios, aún cuando no figuren expresamente en el contrato celebrado o en el documento o comprobante recibido.

2. No obstante lo dispuesto en el apartado anterior, si el contrato celebrado contuviese cláusulas más beneficiosas, éstas prevalecerán sobre el contenido de la oferta, promoción o publicidad.

3. La oferta, promoción y publicidad falsa o engañosa de productos, actividades o servicios, será perseguida y sancionada como fraude..." [8]

En base a este precepto afirma la SAP de Toledo, Sec.1ª, de 3/10/94, que en determinados casos los documentos publicitarios vinculan a quien los utiliza como medio de instrumentalizar la oferta del producto. En este caso la Sala deduce el incumplimiento de contrato de compraventa de un bien inmueble, pues la venta se realizó sobre plano, por medio de un documento privado en el que se describían las condiciones del inmueble y mediante el suministro a la compradora de ciertos documentos precontractuales en los que se indicaban las calidades de los materiales que se habían de emplear en la construcción. Pues bien, según afirma la sentencia citada "esos documentos, de los que normalmente se valen las empresas inmobiliarias para hacer publicidad de las viviendas que construyen y de este modo atraer posibles compradores, vinculan contractualmente a aquellas, en el sentido de que el comprador de la vivienda está legalmente facultado para exigir de la inmobiliaria que la vivienda se adecue fielmente a las condiciones, características y prestaciones ofertadas en la publicidad ".

El respaldo legal se encuentra en el precepto antes citado y en el hecho de que el otro contratante entra dentro del concepto amplio de consumidor

[8] Estas conductas entrarían en los supuestos de publicidad ilícita que se recogen en los artículos 3 y siguientes, en concreto la engañosa de los art.4 y 5, de la Ley 34/1988 de 11 de noviemmbre, General de Publicidad.

del artículo 1.2 de la precitada Ley. [9] En consecuencia, si el producto o servicio no alcanza las calidades ofertadas en la publicidad (prestaciones, utilidad o finalidad, contenido, características, condiciones y garantías) se entiende que hay incumplimiento esencial y acarrea la estimación de la pretensión resolutoria ejercitada por la otra parte. A tal efecto, debemos recordar que el Tribunal Supremo ha dejado muy claro que la resolución del contrato sinalagmático por incumplimiento tiende a cancelar desde un principio los efectos de lo convenido, colocando a los intervinientes en la misma situación en que se hallarían si el pacto no se hubiera celebrado, efecto que opera ex tunc y que conlleva la obligación de restituir por cada parte lo que haya recibido de la otra por razón del vinculo obligacional; todo ello sin perjuicio de los terceros de buena fe.

En esta misma línea, pero con una base argumental más amplia, se pronuncia la STS 1ª de 8/11/1996 pues, en un caso similar, afirma que " bien por la vinculación a la oferta, ya por la Ley General de Protección de Consumidores y Usuarios, sea por los artículos generales sobre obligaciones y contratos.... no se podía prescindir de los treinta y cinco folletos de propaganda aportados a los autos.... ya que se trata de documentos que contienen actividad publicitaria, con intención de atraer a los clientes constituyendo una clara oferta, de forma que al no entenderlo así se infringen los artículos 57 del C. de comercio, el principio de buena fe y el artículo 1283 del C.civil debiendo tal publicidad integrar los contratos, pues para que no fuese así tenía que excluirse expresamente de los mismos el contenido de los folletos, sin que para tal consideración fuere necesario apreciar engaño o fraude, extremos que no requiere el artículo 8 de la Ley de Consumidores ". (Cfr. STS 21/11/63; 16/10/67; 28/11/85 y 24/2/88 y 22/7/94, entre otras).

Y como nos recuerda la SAP de Toledo " pero además de la restitución de las prestaciones objeto del contrato, el artículo 1124 C.c. reconoce a la parte que insta la resolución la posibilidad de solicitar la indemnización de los daños y perjuicios que se le han ocasionado como consecuencia del

[9] No obstante, para la compraventa y arrendamiento de viviendas hemos de reseñar el artículo 3.2 del R.D. 515/1989 de 21 de abril, sobre protección de consumidores en cuanto a la información a suministrar en dichos casos, que sanciona expresamente el carácter vinculante de los contenidos de los documentos de oferta, promoción o publicidad que " serán exigibles aún cuando no figuren **expresamente** en el contrato celebrado".

incumplimiento de la contraparte", así como los gastos en que incurriera con ocasión de la celebración del contrato, en palabras de la sentencia, " todos los gastos que tengan su causa determinante y directa en la realización de la compraventa, o sea los gastos que la compradora no hubiera realizado de no haber adquirido la vivienda".

La gravedad de las consecuencias de ese incumplimiento es tal que la parte que oferta el bien o servicio informático ha de fijar con mucha claridad los extremos de "calidad" arriba indicados. Para que lo sea así el usuario tiene el deber de colaborar poniendo a la otra parte en pleno conocimiento de sus posibilidades, circunstancias y necesidades así como de los objetivos y fines que persigue con el producto o servicio. Esta es la base imprescindible para que la otra parte pueda informarle y aconsejarle adecuadamente sobre cual es el producto o servicio que le interesa. Además de conocer previamente la realidad de estos datos apuntados, el usuario debe adquirir los conocimientos o el personal competente y cualificado para poder utilizar de forma adecuada el producto objeto del contrato. La otra parte no puede responder por una mala utilización producto fruto del desconocimiento, el descuido o el uso inadecuado; en definitiva, el incumplimiento de la diligencia exigible a esta parte.

El cumplimiento de tales deberes es imprescindible por cuanto es la base para determinar adecuadamente el objeto del contrato es decir, el tipo de bien o servicio de que se trata, sean piezas sueltas, equipos completos, programas, sistemas, aplicaciones o cualquier otra prestación principal o accesoria, pues sólo así podrá fijarse exactamente cuales el objeto sobre el que las partes han contratado y los fines y objetivos que está en condiciones de alcanzar. Ha de tenerse muy presente que en los contratos sobre bienes informáticos, éstos pueden ser un objeto aislado o una diversidad unificada: unidad central, monitores, módem, teclado, impresoras, scanners, tarjetas, placas, programas, etc... forman un conjunto diversificado que se integra en un "equipo" suma de todos ellos. Por tanto, la determinación del objeto posee en este campo una especial relevancia dada la multiplicidad de elementos aislados cuya suma puede ser por si misma susceptible de considerarse como un objeto unificador. Son por ello deberes de colaboración mutua que corren en interés de ambas partes y cuya infracción es causa de una responsabilidad contractual ex artículo 1258 CC, como antes dijimos.

Así mismo, la aplicación del artículo 1258 CC en este campo supone la exclusión de aquellas cláusulas o exigencias contractuales que sean

inadmisibles por dolosas, abusivas o contrarias a la equidad contractual que la buena fe defiende. Tal sería el caso de una cláusula contractual que pretenda excluir la responsabilidad de una de las partes en cuanto a un daño o incumplimiento que le sea imputable, ya sea por la Ley o bien porque forma parte connatural del contrato que le vincula.[10]

Téngase en cuenta que cuando hablamos de responsabilidad nos referimos también al saneamiento, a la evicción y a la garantía pues todos ellos son términos utilizados por el Código para hacer referencia a la obligación de las partes de responder por su cumplimiento en una relación contractual.[11]

Una cláusula limitativa de responsabilidad no es sólo aquella que reduce o anula el ámbito de eventos o supuestos en que una parte a de responder, sino aquellas otras que implican reducir plazos de reclamación, excluir supuestos que de ordinario han de cubrirse o reducen el alcance de la reparación del daño injustificadamente.

Las cláusulas limitativas de la responsabilidad han sido definidas por GARCÍA AMIGO como aquellos "pactos insertos en un contrato mediante los cuales el acreedor y el deudor se ponen de acuerdo para establecer preventivamente y en virtud del principio de autonomía de la voluntad una limitación cualquiera de la responsabilidad de la que la ley dispositiva atribuye al deudor por el incumplimiento imputable de sus obligaciones contractuales".[12] Se trata así de pactos insertos previamente en el propio contrato mediante los cuales las partes de común acuerdo deciden excluir los supuestos de responsabilidad de una de ellas que vienen establecidos por una norma dispositiva, por lo que

■[10] Sobre la aplicación del artículo 1258 C.c. como elemento integrador y límite del contenido de los contratos, véase Alfaro Aguila-Real, J.:" Las condicones generales de la contratación". Madrid, Cívitas, 1991, páginas 374 ss y 442 ss.

■[11]Vid. García Amigo, M.:" Lecciones de Derecho Civil II: Teoría General de las Obligaciones y Contratos ". Madrid, MacGraw Hill, 1995.

■[12]Vid. " Cláusulas limitativas de la responsabilidad contractual ".Madrid, 1965 y " El contrato en la perspectiva comunitaria ". En Revista Actualidad Civil, 1992 y su obra general:" Lecciones de Derecho Civil II. Teoría General de las Obligaciones y los Contratos". McGraw-Hill; Madrid, 1995, página 206 y siguientes.

cuando esa cláusula excluya o limite la responsabilidad en un caso de incumplimiento cuya cobertura viene ordenada por Ley imperativa, esa cláusula ha de entenderse como nula por abusiva, ya que excluye cumplir una obligación legalmente sancionada o implica una renuncia nula ex art.2.3 de la Ley de Consumidores y, en todo caso, es contraria a la naturaleza o equilibro del contrato que la buena fe como exigencia imperativa del artículo 1258 C.c. consagra y que se plasma en el concepto de cláusula abusiva del artículo 10.1.3° de la Ley de Consumidores:

" .... entendiendo por tales las que perjudiquen de manera desproporcionada o no equitativa al consumidor, o comporten en el contrato una posición de desequilibrio entre los derechos y las obligaciones de las partes en perjuicio de los consumidores o usuarios ".

Esta "preocupación" por el equilibrio contractual no es nueva, pues se encontraba ya en el Código civil como principio inspirador de diversos preceptos del mismo tales como el 1091, 1255, 1256,1258 y 1269, entre otros, pues como afirmaba el Tribunal Supremo en la sentencia de 23/11/1962, se ha de tener en cuenta cualquier evento que afecte " al elemento de justicia objetivo implícito en la exigencia de causa en los contratos y a la equivalencia de las prestaciones ".(Cfr. STS 17/1/86; 21/10/86;21/10/90 y 31/10/92, entre otras)[13]

A nuestro entender esta cuestión cobró nueva vitalidad merced a la influencia directa de la Constitución de 1978 sobre el Derecho civil y, en concreto, sobre las materias relativas a la teoría general del contrato y la responsabilidad civil. Si partimos del análisis del artículo 14 CE que consagra el principio/derecho a la igualdad y lo conectamos con el artículo 9.2 del mismo Texto según el cual " corresponde a los poderes públicos promover las condiciones para que la libertad y la igualdad del individuo y de los grupos en que se integra sean reales y efectivas; remover los obstáculos que impidan o dificulten su plenitud y facilitar la participación de todos los ciudadanos en la vida política, económica, cultural y social ".

■[13] Vid. Fernández Rodriguez, A.:" Grandes directrices y principios informadores del Código civil. Estimación conjunta". En:" El centenario del Código civil en el Tribunal Supremo". M° de Justicia, Madrid, 1989, pág.49 y siguientes.

Como afirma SUAREZ PERTIERRA este precepto pretende del Estado una actitud específica para la correcta realización de la libertad y la igualdad, de tal suerte que ese Estado se convierte en social en la medida en que dota a la igualdad de un contenido de redistribución y de compensación para enriquecer los derechos de los menos dotados y se limitan los de aquellos que poseen una superioridad social o económica para compensar las discriminaciones reales que proceden del modelo social imperante. [14]

Con ello se convierte aquél principio formalista de la igualdad del Antiguo Régimen en un factor transformador de la sociedad, de suerte que en palabras de SANCHEZ AGESTA el principio de igualdad jurídica convierte en " principio de desigualdad jurídica que proteja a la parte natural o socialmente más débil " , y ello porque no se puede tratar igual a los desiguales.[15] Esto supone aplicar este principio/mandato constitucional a los diversos ordenes de la vida social, pues no se trata simplemente de una igualdad formal ante la Ley, sino de una efectiva igualdad entre los ciudadanos en el seno de las relaciones sociales. Es por ello por lo que no se puede admitir la existencia de una ética para las relaciones regida por el Derecho público, distinta substancialmente a la que ha de regir en el campo de las relaciones sometidas al derecho privado, máxime cuando la frontera entre ambos tiende a difuminarse, no sólo en el Derecho de familia, sino en ámbitos tradicionalmente reservados a la autonomía privada como derechos reales y obligaciones y contratos.[16]

Todo lo que antecede ha de ser puesto en conexión con el artículo 149.1-8 que confiere al Estado la competencia exclusiva " en todo caso " sobre las reglas relativas a las bases de las obligaciones contractuales y con el principio de seguridad jurídica consagrado en el artículo 9.3 de nuestra Carta Magna, pues el Derecho civil patrimonial ha de conectarse ahora con los principios y valores constitucionales, tal y como afirma PERLINGIERI:

■[14] Vid. " Comentarios a las Leyes Políticas: Constitución Española de 1978". Dir. O. Alzaga, EDERSA, Madrid, 1985, Tomo II.

■[15] Citado por Suárez Pertierra en op. cit. pág.291

■[16] Sobre las relaciones entre Constitución y Derecho civil véase Arce y Florez-Valdés, J." El Derecho civil constitucional". Cívitas, Madrid, 1986

" Las cláusulas generales que caracterizan la conducta del deudor y del acreedor en su relación de cooperación, y sobre todo los principios de la buena fe y de la diligencia en el cumplimiento de la obligación, no pueden ya ser dotados de contenido a la luz de cuna concepción meramente productivista de las relaciones intersubjetivas patrimoniales, sino que deben asumir, en la elaboración jurisprudencial y doctrinal, contenidos diferentes, más adecuados a los valores fundamentales del ordenamiento".[17]

BERCOVITZ mantiene que tales bases se encuentran o inducen a partir del propio Código civil, Libro IV, Títulos 1° y 2°, y demás normas conexas como aquellas que regulan tipos concretos de contratos o aspectos determinados de la contratación.[18] La STC 71/82 de 30 de noviembre sostuvo que tales bases se relacionan con las exigencias de la unidad de mercado y abarcan cuestiones capitales como el régimen general de la responsabilidad civil, las limitaciones a la autonomía privada, la regulación general de las condiciones generales de la contratación y de las cláusulas abusivas y su sanción y la unidad del mercado nacional.[19]

Estas bases, merced a su papel vertebrador de tan importante sector de la vida económica y social, han de estar necesariamente imbuidas de los principios constitucionales y, en concreto, del principio/mandato de igualdad como exigencia impuesta por vía de la seguridad jurídica, que a la vez que sirve de criterio/valor para determinar el control de "calidad" de una norma e, incluso,

■[17] Vid. " Por un Derecho civil constitucional español". ADC, 1983, pág.5. Sobre la seguridad jurídica véase Mezquita del Cacho, J.L.:" Seguridad Jurídica y sistema cautelar" Barcelona, Bosch, 1989.

■[18] Vid. " Las Bases de las obligaciones contractuales en el artículo 149.1.8ª de la Constitución". En:" Competencia en materia civil de las Comunidades Autónomas ". Coord. B. Moreno Quesada. Técnos, Granada, 1989

■[19] Sobre esta sentencia véase Bercovitz y Rodríguez Cano, R.:" La defensa contractual del consumidor y el reparto de competencias entre el Estado y las Comunidades Autónomas en la doctrina del Tribunal Constitucional ". En:" Estudios jurídicos sobre protección de los consumidores ". Técnos, Madrid, 1987. Sobre el diseño constitucional de sistema de economía social de mercado y sus repercusiones en el moderno Derecho de contratos véase Santos Briz, J.:" Los contratos civiles. Nuevas perspectivas". Granada, Comares, 1992

de una estipulación contractual que funciona como " ley entre partes". Esta exigencia se acentúa en los casos en que dicha estipulación forma parte de un contrato de adhesión normado, razón por la cual la legislación sobre esta materia impone unos controles previos y un principio de " desequilibrio equitativo " cual es el "contra estipulatoren" del artículo 10.2 de la Ley de Consumidores " las dudas en la interpretación se resolverán en contra de quien las haya redactado ". Incluso se impone una norma " de cierre" que asegura el equilibrio, pues el artículo 10.4 de esta Ley establece la ineficacia del contrato cuando las cláusulas subsistentes del mismo " determinen una situación no equitativa de las posiciones de las partes en la relación contractual ".[20] Es por ello que la aplicación de los principios constitucionales a este campo se materializa por medio de nuevas normas o mediante la utilización de aquellos principios como criterios interpretativos e integradores y ello porque, como afirma DIEZ PICAZO " la defensa de la equidad contractual y de la corrección en la ejecución de los contratos masificados, es claro.... que no puede resolverse con los esquemas e instrumentos jurídicos tradicionales". [21]

Todo lo anterior se proyecta en nuestro ordenamiento en supuestos como el del precitado RD 515/1989 de 21 de abril, sobre protección de los consumidores en cuanto a la información a suministrar en la compraventa y arrendamiento de viviendas, pues su Disposición adicional segunda declara su aplicación supletoria respecto de las Comunidades Autónomas que estatutariamente hayan asumido la competencia plena sobre la defensa de los consumidores y usuarios, " excepto los artículos 3.2 y 10 que tendrán vigencia en todo el Estado , en virtud de lo dispuesto en la regla 8ª del artículo 149.1 de la Constitución Española ". Tales preceptos consagran el carácter vinculante de la publicidad, ofertas y promociones, ya comentado, y la aplicación imperativa de los principios de buena fe y justo equilibrio de las prestaciones que prohiben la inclusión de cláusulas abusivas, en sus diversas vertientes.

■[20] Así Arce y Florez-Valdés, siguiendo a Larenz, entiende que tales bases proecriben los **contratos leoninos** " cuyas condicones someten a una de las partes a una completa dependencia de la otra". Vid. op. cit. página 77.

■[21] Vid. " Derecho y masificación social. Tecnología y Derecho privado. (Dos esbozos)". Cívitas, Madrid, 1979

Esta necesidad de "reequilibrar" las relaciones de intercambio económico de bienes y servicios se ha hecho más patente con el fenómeno de la contratación en masa, dado que en este caso se trata de estipulaciones de carácter general redactadas previa y unilateralmente por la Empresa y cuya aplicación no puede evitar el consumidor si quiere obtener el bien o servicio. Su proliferación ha sido tal que se ha llegado incluso a discutir su naturaleza normativa, tal y como reflejaba DE CASTRO.[22]

Esta protección del equilibrio contractual que impone la buena fe y que se ha convertido en uno de los principios capitales del sistema jurídico-privado, ha adquirido una dimensión extranacional como lo demuestra la política del la Unión Europea en esta materia. Para ello se consagran los principios antes enunciados que inspiran a la Directiva 93/13 CEE de 5 de Abril sobre cláusulas abusivas que se incluyen en contratos entre consumidores,("persona física que actúa en tales contratos con un propósito ajeno a su actividad profesional") y el profesional,(" persona física o jurídica que, en las transacciones reguladas por la presente Directiva, actúe dentro del marco de su actividad profesional, ya sea pública o privada"). En razón de ello su artículo 3° dispone:" Las cláusulas contractuales que no se hayan negociado individualmente se consideraran abusivas si, pese a las exigencias de la buena fe, causan en detrimento del consumidor un desequilibrio importante entre los derechos y obligaciones de las partes que se derivan del contrato". Esta concepción sintoniza con la recogida en el artículo 10.1-C.3° de la ya citada Ley 26/84 de Consumidores que proscribe las cláusulas abusivas entendiendo por tales " las que perjudiquen de manera desproporcionada o no equitativa al consumidor, o comporten en el contrato una posición de desequilibrio entre los derechos y las obligaciones de las partes en perjuicio de los consumidores o usuarios ".

Como puede verse, la norma entra directamente en el eje del problema: la contratación por adhesión en la cual una de las partes sólo puede manifestar su voluntad de adherirse un contenido clausular previsto por la otra parte; es decir, son contratos exentos de negociación que suelen imponer un contenido predeterminado por el proponente, parte fuerte del contrato. Por ello si la cláusula ha sido previamente redactada y el consumidor no ha podido influir en

■[22] Cfr. " Las condicones generales de los contratos y la eficacia de las leyes". Cívitas, Madrid, 1985

su contenido, se considera no negociada. Aunque haya existido una negociación parcial, se considera contrato de adhesión si de la apreciación global se deduce la necesidad de aplicar la Directiva.[23] El profesional que afirme que tal cláusula se ha negociado individualmente, ha de probarlo.

En el artículo 4 se establecen los criterios para apreciar el carácter abusivo de una cláusula: se tiene en cuenta la naturaleza de los bienes o servicios que sean objeto del contrato y considerando, en el momento de la celebración del mismo, todas las circunstancias que concurran en su celebración, así como todas las demás cláusulas del contrato, o de otro contrato de que dependa. Esto implica puede ser abusivo el contrato o cláusula de un contrato dependiente: por ejemplo el contrato accesorio de garantía o mantenimiento informático en el que se pueden fijar condiciones que desvirtúen o anulen de facto lo establecido en el contrato principal. Las cláusulas han de estar redactadas de forma clara y comprensible, pues si hay duda se interpreta en favor del consumidor; si ello es posible se anula la cláusula abusiva y se mantiene la validez del resto del contrato. Finalmente, es de destacar que el consumidor no debe verse privado de sus derechos por el hecho de haberse elegido el Derecho de un Estado tercero como aplicable al contrato "cuando el contrato mantenga una estrecha relación con el territorio de un Estado miembro de la Comunidad".

En este punto es interesante la STS del 20/11/96 que analiza el diferente criterio del artículo 3 de la Directiva y el 10.2 de la Ley 26/84 pues en aquél basta que el consumidor no haya podido influir sobre el contenido de las cláusulas redactadas previamente, concepto "amplísimo" de cláusula abusiva, que " convierte en realidad a todo contrato de adhesión en particular receptor de cláusulas que pueden ser declaradas abusivas, como así viene a reconocerlo el apartado 2 del citado artículo 3". En cambio, continua la sentencia " el artículo 10.2 de nuestra Ley 26/84 requiere que la aplicación - de la cláusula abusiva - no la pueda evitar el consumidor o usuario, siempre que quiera obtener el bien o

[23] El artículo 10.2 de la Ley de Consumidores entiende por clausulas o condiciones generales " el conjunto de las redactadas previa y unilateralmente por una Empresa o grupo de Empresas para aplicarlas a todos lo s contratos que aquélla o éste celebren,y cuya aplicación no puede evitar el consumidor o usuario, siempre que quiera tener el bien o servicio de que se trate ". No obstante, conviene recordar la afirmación del Tribunal Supremo de que " la contratación por adhesión no es, por si misma, una fuente automática de nulidades".(Cfr. STS 29/6/95)

servicio de que se trate. No es suficiente, pues, que el consumidor o usuario no haya podido influir sobre el contenido de la cláusula, se le exige que no haya podido eludir su aplicación, en otras palabras, no una actitud meramente pasiva. La LGDCU se muestra sí más restrictiva, no basta que existan cláusulas prerredactadas unilateralmente, y cualquiera que fuese la opinión que se tenga sobre el acierto o desacierto del legislador, no hay duda de que esta Sala sólo se encuentra vinculada al precepto legal, y ha de aplicarlo en su integridad ".

Es interesante constatar esta diferencia de criterio entre nuestra Ley y la Directiva que aún no ha sido incorporada a nuestro Ordenamiento interno, pero como la misma dispone en su artículo 10 que se procederá a su aplicación a los contratos celebrados a partir del 31/12/1994 aunque no se haya dictado la Ley de incorporación correspondiente, tarea que actualmente se realiza por nuestro legislador. A tal efecto, es conveniente recordar la ya citada STS de 20/11/96 según la cual " ciertamente la Directiva 93/13 ha de servir de guía para la interpretación de los Derechos nacionales vigentes tanto anteriores como posteriores para alcanzar el resultado a que se refiere cuando no se haya adaptado el Derecho interno a la misma, pero sin que sea aplicable directamente en cuanto confiere derechos a los particulares respecto de otros. Así lo dice el Tribunal de Justicia de la C.E. en la sentencia de 14 de julio de 1994 ".

El anteproyecto de ley sobre condiciones generales de la contratación, que incorpora la Directiva 13/93 CEE sobre cláusulas abusivas en los contratos celebrados con los consumidores, ya comentada, introduce nuevos matices en esta cuestión. En su artículo 5 asiente un "criterio negativo" de integración del contenido del contrato en la medida en que, más que declarar la nulidad, se establece una tipología de cláusulas que se consideran no incorporadas al contrato. Tales condiciones generales son:

- Aquellas que no haya tenido oportunidad el adherente de tomar conocimiento real al tiempo de la celebración del contrato o cuando no hayan sido firmadas cuando sea necesario en los términos que establece el artículo 4 del mismo texto. Según este precepto las condiciones generales deben ser aceptadas y firmadas por las partes, estando redactadas conforme a los criterios de transparencia, claridad, concreción y sencillez. En todo caso, el predisponente debe informar al adherente de su existencia facilitándole el acceso a su conocimiento mediante un ejemplar de las mismas o publicitándolas debidamente.

- Las que resulten "insólitas" de acuerdo con las circunstancias y la naturaleza del contrato y, por tanto, el adherente no hubiera podido contar razonablemente con su existencia.

La no incorporación y la declaración de nulidad de la cláusula no determinan la ineficacia total del contrato, sino que aquella parte del contrato afectada por tal "laguna" se integra con arreglo a lo dispuesto en el artículo 1258 C.c., según establece el artículo 9 del mismo anteproyecto.

En su disposición final primera introduce una serie de modificaciones el texto de la ley 26/1984 LGDCU y, de entre ellas, destacamos, en lo que a nosotros nos interesa, la cuarta por la que se añade un nuevo artículo 10.bis que viene a fijar el criterio antes apuntado para conceptuar una cláusula como abusiva. A su tenor:

" Se considerarán cláusulas abusivas todas aquellas estipulaciones no negociadas individualmente que en contra de las exigencias de la buena fe causen, en perjuicio del consumidor, un desequilibrio importante de los derechos y obligaciones de las partes que se derivan del contrato.

El carácter abusivo de una cláusula se apreciará teniendo en cuenta la naturaleza de los bienes o servicios objeto del contrato y considerando todas las circunstancias concurrentes en el momento de su celebración, así como todas las demás cláusulas del contrato o de otro del que éste dependa. Tal apreciación no se referirá a la materia objeto del contrato ni a su adecuación con el precio pactado, siempre que las cláusulas que lo definen se redacten de manera clara y comprensible".

En consecuencia, nuestro legislador parece optar por un criterio más amplio a la hora de determinar si la cláusula es injusta: la falta de un proceso previo de negociación individualizada que posibilite una oposición razonable y el consecuente desequilibrio relevante de las prestaciones.

No obstante, nuestra jurisprudencia ha venido aplicando el espíritu de este criterio, tal y como lo demuestra la STS de 13/11/92 cuando sostiene que aunque el contrato tenga fuerza de ley entre las partes (art.1091CC) cuando una cláusula de ese "ordenamiento contractual" infringe una lesión a un bien o valor protegido por la seguridad jurídica, se despliega el efecto negativo de esta que deroga aquella cláusula introducida por la autonomía de la voluntad pues la

legalidad es el medio de control del contenido de los convenios entre particulares para evitar que atenten contra los principios y valores inherentes a la seguridad jurídica. Y uno de estos valores es la igualdad de las partes en el seno de las relaciones jurídico-privadas cuya defensa se hace más precisa en aquellos campos donde la actuación de entidades con poderes económicos y de control de mercado superiores a los del particular que contrata con ellas da origen a prácticas prepotentes por vía de imposiciones de monopolios o de cláusulas abusivas.

La propia Directiva contiene un anexo con un catálogo no cerrado de cláusulas abusivas entre las cuales la primera es aquella que tiene por objeto " excluir o limitar la responsabilidad legal del profesional en caso de muerte o daños físicos del consumidor debidos a una acción u omisión del mencionado profesional". Esta misma técnica se aplica en el precitado anteproyecto de condiciones generales en cuyo artículo 7.2 se hace referencia al nuevo artículo 10 bis que introduce en la LGDCU por vía de su disposición final primera.

El Derecho debe asegurar unos mínimos de justicia en estos casos por vía de la igualdad para que esa relación sea éticamente admisible, valiéndose para ello de los principios constitucionales que han inspirar las normas del Derecho privado, en los términos antes enunciados por vía de las citadas "bases de las obligaciones contractuales" que la Constitución enuncia y consagra. Para ello el contenido preestablecido de las reglas o cláusulas que la disciplinan ha de ser claro, conocido y conforme a la buena fe y a la equidad. El principio de autonomía privada no es absoluto sino que debe respetar unas exigencias éticas ineludibles consagradas en las norma imperativas y en los principios generales del derecho; frente a ello no cabe tan siquiera alegar una norma consuetudinaria o usual pues estas han de respetar siempre aquellos límites.(Cfr.STS 30/4/93 y 29/6/95)

Como antes pudimos constatar esta cuestión se agudiza en el campo de los contratos por adhesión pues en estos no suele haber una negociación previa de cláusulas, incluso no se conoce parte de ellas, por lo para su interpretación ha de estarse a la realidad social del momento que hoy viene esencialmente preocupada por la igualdad contractual y el justo equilibrio de las prestaciones, tal y como lo demuestra la actual Ley de consumidores (L.19/7/84) en su artículo 10 donde consagra una garantía de equidad contractual que limita el alcance del artículo 1255 y la libertad de pacto para proteger a la parte débil del contrato pues declara nula toda cláusula que infrinja el principio de buena fe y

justo equilibrio de las prestaciones. A tenor de ello, la Jurisprudencia viene declarando nulas las cláusulas que infringen estos principios imponiendo limitaciones de responsabilidad en condiciones de "semi exoneración" de la misma.(Cfr. S A.P. Castellón 6/3/93)

En consecuencia, cuando el daño surge de una conducta que se aparta de aquella que razonablemente puede esperarse de una adecuada ejecución del contrato conforme a su naturaleza y a la buena fe, surge el deber de responder por el quebranto, de cualquier tipo, que de ella se deduce, sin que quepa admitir una cláusula contractual que limite o excluya esa responsabilidad cuando sea considerada abusiva merced a los criterios antes apuntados. El contrato, y menos el de adhesión, no puede ser un medio de alusión de la responsabilidad por su propio incumplimiento.

Finalmente diremos que no basta la existencia de un contrato o relación de otra naturaleza entre las partes para que opere la responsabilidad contractual con exclusión de la extracontractual, sino que se requiere que el hecho dañoso acontezca dentro de la rigurosa órbita de lo pactado y como desarrollo normal del contenido negocial.(A.P.Tarragona 6/6/93) No obstante, cuando concurre un incumplimiento contractual con un ilícito extracontractual, el perjudicado puede optar entre una u otra acción para obtener el resarcimiento.(Cfr. S.A.P.León de 17/1/92)

No podemos dejar de hacer una breve mención a la responsabilidad precontractual pues en el campo de la informática posee mucha relevancia. Con ocasión de los tratos preliminares suele haber conversaciones, presupuestos, desplazamiento de técnicos, etc... que sirven para determinar el objeto del contrato, como antes vimos, y fijar el contenido de la oferta de ese futuro contrato, salvo en los supuestos de contratos en masa o de adhesión en la que esa negociación no tiene lugar. La doctrina entiende hoy que cuando esos tratos preliminares existen su ruptura no suele conllevar obligación de resarcir; pero si ellos comportan unos gastos, gestiones, etc... a una parte y la otra injustificadamente, inobservando su deber de buena fe, realiza una ruptura unilateral, habría una responsabilidad precontractual aunque no haya contrato. Para ello se basa en la aplicación de los artículos 7.1, 1258 y 1902 del Código Civil, pues son casos en que esa ruptura ocasiona un daño injustificado a una

parte, que por ejemplo adquirió el equipo al mayorista, o un perjuicio, en cuanto dejó de venderlo a un tercero.[24]

A titulo de ejemplo pensemos en la empresa que envía un técnico a evaluar las necesidades del cliente, elabora el presupuesto según sus indicaciones aprobadas por el futuro adquirente, pide los equipos y programas al fabricante y, posteriormente, la otra parte desiste o rompe la relación de forma injustificada, ocasionando un daño real y efectivo representado por los gastos y equipo adquiridos, y los posibles perjuicios si con ello se impidió su venta a un tercero interesado.[25]

Dentro de este campo, hemos de aludir al grado de compromiso o vinculación que los documentos precontractuales poseen a la hora del desarrollo y ejecución del contrato. Estos documentos de los que se valen las empresas para dar a conocer sus productos y resaltar sus cualidades y utilidades vinculan contractualmente a las empresas en la medida en que facultan legalmente a la otra parte para exigir al oferente que el producto se adecue fielmente a las condiciones, características y prestaciones ofertadas en la publicidad. Tal y como hemos expuesto en páginas precedentes, la citada sentencia de la A.P. de Toledo de 3/10/94 basa el respaldo legal de esta vinculación en el artículo 8.1 de la Ley de Consumidores pues éste precepto exige que la promoción y publicidad de los bienes y servicios de consumo se ajusten a su naturaleza, características, condiciones, utilidad o finalidad y, añade, " su contenido, las prestaciones propias de cada producto o servicio, y las condiciones y garantías ofrecidas, serán exigibles por los consumidores o usuarios, aún cuando no figuren expresamente en el contrato celebrado o en el documento o comprobante recibido".

De ello deducimos que las propiedades, funciones o utilidades "prometidas" al ofertar y asesorar sobre el producto vinculan al vendedor en la medida en que éstas quedan comprometidas frente a la otra parte, de manera que su insatisfacción origina incumplimiento. Este deber vinculante se acentúa especialmente en su exigibilidad en el campo de los contratos informáticos donde

[24]Vid. Lasarte Alvarez:" Principios de Derecho Civil".Madrid, 1995

[25] Vid. Hoorens, Schoenmaeckers y Lamsweerde:"Les contrats de développement de logiciel sur mesure".Bruxelles, 1986 y "I contratti di utilizzazione del computer".Dir.G.Alpa, Milano,1984

los equipos y el software suelen ser objeto de asesoramiento y especificación para el usuario que expone sus necesidades al proveedor.

B- La responsabilidad civil extracontractual:

Surge cuando se infringe un deber genérico impuesto a todo ciudadano por el contrato social: no dañar a nadie; de suerte que quien mediando culpa o negligencia, por acción u omisión, produce un daño a otro, viene obligado a repararlo, pues tal es el mandato del artículo 1902 CC. Actualmente, para el estudio de esta materias se ha consagrado la unidad de criterio y método y surge el llamado Derecho de daños, derivado del Law on torts anglosajón que pone su acento en el daño efectivo que sufre la víctima que puede ser de distinta naturaleza, moral o patrimonial. Es indiferente que esa obligación surja por un mandato legal con independencia de que exista o no un previo contrato, lo cierto es que quien realiza una actividad de riesgo debe prever y cubrir sus consecuencias lesivas.

A tenor del artículo 1089 CC los actos u omisiones ilícitos o en los que media culpa o negligencia producen la obligación de reparar sus consecuencias. Ello se ha de conectar con el artículo 1902, antes citado, " el que por acción u omisión causa daño a otro, interviniendo culpa o negligencia, está obligado a reparar el daño causado". El Tribunal Supremo ha establecido que en este precepto se asienta un principio objetivo fundamental en nuestro sistema que da origen a una obligación de carácter civil.(STS 13/12/83)

De otro lado, existe una responsabilidad civil originada por los delitos y faltas que se regula por las normas del Código Penal a tenor del artículo 1092 CC, aunque no existe una vinculación automática e indisoluble entre ambas, pues la acción civil es subsidiaria aunque cabe ejercicio conjunto.(Cfr.STS 30/12/92) Pero ha de tenerse en cuenta que las sentencias penales sólo obligan al juez civil en aquellas afirmaciones fácticas declaradas probadas que son integrantes del tipo que se define y castiga por lo que las declaraciones civiles de la sentencia penal carecen de fuerza en la jurisdicción civil.(STS 10/12/92)

Como vimos anteriormente, la obligación extracontractual de responder posee un fundamento objetivo pues, salvo ciertas excepciones ya citadas, la responsabilidad subjetiva ha sido superada por la teoría del riesgo y la persona que actúa esa actividad debe atenerse a la obligación de responder por sus consecuencias si hay un nexo o vínculo causa entre su conducta y el daño. El

Tribunal Supremo ha dicho que se trata de un sistema que " sin hacer plena abstracción del factor moral o psicológico y del juicio de valor sobre la conducta del sujeto, acepta soluciones cuasi objetivas, si bien no permite la exclusión sin más del básico principio de responsabilidad por culpa que responde nuestro Ordenamiento ".(STS 21/11/90)

En consecuencia si hay un acto u omisión ilícito, contra deberes de esa conducta social típica y esperable, un daño infringido injustamente y un vínculo causal entre ambos, se presume que hubo "algún fallo" y surge la obligación de responder, salvo que se pruebe culpa de la víctima o cualquier otra causa de exoneración admisible. Cuando no se pueda individualizar la cuota de responsabilidad correspondiente a cada uno de los sujetos, se impone la solidaridad.(STS 4/11/92) Hay una obligación de responder porque así lo impone un imperativo social de solidaridad con el sujeto que sufre el daño sin que ello se le pueda imputar.

Para su aplicación se exige que el acto u omisión suponga una conducta voluntaria que omite el deber de respetar el mandato neminem non laedere y que infringe un daño que causa un perjuicio patrimonial o moral probado por el sujeto que lo padece. Entre ambos debe haber un vínculo o nexo causal en una relación de causa a efecto; no obstante pueden intervenir factores externos que rompen esa vinculación: caso fortuito o fuerza mayor, intervención de un tercero o una acción del propio perjudicado. Estos elementos rompen el nexo e impiden que pueda imputarse al sujeto el daño producido.

3°- <u>El daño: concepto, valoración y naturaleza</u>.

Daño es el detrimento o destrucción en sus bienes que una persona sufre como consecuencia de cualquier evento, pero no se trata del lucro cesante que tiene un carácter futurible, el daño es una realidad actual que implica una pérdida o disminución de carácter patrimonial que se padece. Pero como veremos después existe también un daño moral equivalente a un sufrimiento o erosión moral que la persona puede sufrir en sus bienes o valores morales, sea por un ataque a si mismo o a un tercero. Jurídicamente, daño es toda perturbación o deterioro que una acción delictiva causa a las personas o a sus bienes, pero en el campo civil esta referido al menoscabo, deterioro o perjuicio que no proviene de delito pero que da lugar a la obligación de resarcir. En la actualidad, este daño no tiene porqué ser infringido sólo a bienes ajenos pues en el campo de la propiedad y merced al concepto de función social puede haber un daño a bienes propios que

la sociedad sancione con la obligación de resarcir impuesta al mismo propietario autor del mismo.

Dentro de este concepto jurídico civil del daño caben distintas figuras pero en lo que a nosotros interesa hemos de resaltar el de daño emergente referido a la perdida real y efectiva que sufre el patrimonio del lesionado y el llamado daño negativo o lucro cesante que se refiere a la ganancia razonablemente esperable que deja de percibir como consecuencia del anterior. La distinción entre ambos tiene su origen en el Derecho Romano en el que, en un principio, la obligación del responsable del daño alcanzaba hasta el valor de la pérdida o minusvaloración ocasionada.

Posteriormente, esta obligación se extendió también al lucro cesante o daño negativo. Para aclarar esta diferencia surge el concepto de daños y perjuicios identificando el daño con la pérdida o detrimento real sufrido y el perjuicio con la ganancia, lucro o beneficio que se deja de percibir. En consecuencia, la expresión "daños y perjuicios" supone una duplicidad de conceptos que no siempre han de ir unidos pues se puede ocasionar un daño real y efectivo sin que ello implique perjuicios inmediatos. Ambos pueden ser personales, sean corporales o morales, o bien de naturaleza patrimonial.

El daño moral afecta a la esfera espiritual de la persona por cuanto atenta contra aspectos, valores o bienes de la personalidad del sujeto afectado, tengan o no una realidad física. Su origen lo encontramos en la clásica STS de 6/12/1902 que aplicó el artículo 1902 CC a un supuesto de intromisión ilegítima en el honor y la intimidad de unas personas por un diario. Dentro de este concepto cabe distinguir:

a) Daño directo: está referido a la lesión que se opera de modo inmediato contra un bien inmaterial de la persona: honor, imagen, etc... En este campo, la L.O. de 5/5/82 presume que si existe la intromisión, existe el daño, sin entrar en motivaciones o finalidades, pues la importancia de estos bienes jurídicamente protegidos y su relevancia social así lo imponen. Así la STS de 11/2/92 entiende que el ataque al honor de una persona se desenvuelve tanto en el marco interno de la propia persona afectada, e incluso de la familia, como en el ámbito social externo y, por lo tanto, profesional, en que cada persona desarrolla su actividad. Este tipo de daños suelen causarse en los casos de lesión a la intimidad, honor, etc... por vía de la relación entre informática y libertades.

b) Daño Indirecto: se produce como consecuencia mediata de un daño material o personal: desfiguración de una persona, pérdida de un miembro de la familia, etc...

Este daño moral o "pecunia doloris" puede a su vez diferenciarse según se trate de un daño traducible en un interés económico en cuyo caso el resarcimiento es fácil de llevar a cabo: la pérdida de prestigio y clientela profesional por haberse dado unos datos o informaciones erróneas sobre la solvencia económica de un profesional o comerciante.(Cfr.STS 24/1/1923) Más problemático es el caso en que ese daño moral no tiene una traducción o evaluación económica directa, pues en estos casos se consideró que estábamos más ante una pena que ante un resarcimiento. Sin embargo, la moderna doctrina admite este "pretium doloris" pues si bien con el dinero no se puede devolver el bienestar moral anterior, si pueden, sin embargo, obtenerse con él nuevos goces que compensen aquellos que fueron arrebatados por la conducta injusta. Se trataría de, al menos, mitigar el dolor que el daño produce en el patrimonio moral de la persona ya que este no puede restablecerse en su estado inicial.

Es aquella demanda de la solidaridad social que exige que la víctima no soporte sola las consecuencias del evento daños, ejemplo de ello es la STS de 23/4/92 es un ejemplo claro de ello cuando entiende que existe daño moral en las consecuencias desafortunadas de un acto médico pues " ... es de una evidencia cegadora el dolor moral que experimenta una madre al ver a su hija en la situación tan lamentable como la que presenta, habida cuenta, además, de que es ella sola la que tendrá que soportar los inmensos trastornos que supone cuidar de una inválida, ya que se encuentra separada del esposo por sentencia judicial en la que se le transfirió la guarda y custodia de sus hijas...".

De todo ello deducimos que el concepto jurídico de daños y perjuicios es plurisemántico pues posee una diversidad de proyecciones, sean personales o patrimoniales. Una vez probado el daño, sea incluso por presunción objetiva, surge la obligación de resarcir salvo que concurran circunstancias de exención como las antes comentadas. La determinación de su cuantía esta encomendada a los Tribunales, quienes se valen de los medios adecuados al caso: tasación, precio, peritos, etc.... (STS 26/12/91) Cuestión diferente es la determinación de los perjuicios sufridos, que han de probarse en su efectividad y cuantía, salvo supuestos de indemnizaciones pactadas previamente por las partes.

Técnicamente, la teoría de los daños y perjuicios tiene su aplicación principalmente en el campo del Derecho de obligaciones. Cuando se

produce el incumplimiento el Derecho reacciona contra el patrimonio del sujeto con la finalidad de obtener de este bienes suficientes para restaurar el desequilibrio patrimonial que su conducta a ocasionado a la otra parte. Pero ello no se agota en este campo dado que se ha extendido a otros supuestos en los cuales la conducta de una persona produce una perturbación en la esfera personal o una disminución en el patrimonio de otra. Ya de antiguo la Jurisprudencia ha afirmado que los preceptos legales que disciplinan el incumplimiento son de carácter general y aplicables a todo género de obligaciones.(STS 19/12/1916)

En concreto, los daños y perjuicios pueden originarse a partir de diversos supuestos:

a) De los incumplimientos contractuales.(1115 CC)

b) De la concurrencia de un hecho previsto como causa en el propio contrato: así el siniestro cubierto por el contrato de seguro.(1791CC)

c) Cuando lo han previsto las partes estableciendo una cláusula que origina la obligación de indemnizar: cláusula penal.(1152 CC)

d) En los supuestos en que ha lugar a responsabilidad según la Ley.(1902, 1905 y otros CC)

Como puede observarse, en unos casos el resarcimiento posee un carácter de recurso subsidiario y en otros actúa como objeto inmediato de responsabilidad. Ha sido definida esta obligación de daños y perjuicios como " la obligada restauración del desequilibrio patrimonial ocasionado por la conducta injusta del obligado, satisfaciendo al perjudicado aquellos que se le originaron". Ello implica una serie de requisitos:

a) Una conducta injusta en la medida que ocasiona un quebranto injustificado ya sea por culpa, dolo, negligencia o morosidad, si bien las nuevas corrientes jurisprudenciales presumen esa culpa o negligencia en la conducta del causante objetivizando esa responsabilidad.

b)Supone igualmente la imposibilidad de obtener el cumplimiento forzoso de una manera específica, lo cual implica que la obligación no puede cumplirse tal y como se había pactado.

c) La concurrencia efectiva de unos daños o la pérdida de una ventaja razonablemente segura.

d) Un nexo causal entre conducta y daño. Será el juez el que debe analizar caso pos caso la concurrencia de este requisito teniendo en cuenta las precisiones hechas en páginas precedentes sobre la objetivización de la culpa, la concurrencia de culpa de la víctima o el caso fortuito.

En relación al contenido de esta obligación hemos de decir que, básicamente, consiste en restablecer el patrimonio del sujeto en la misma situación que ostentaba antes de producirse el evento dañoso. Para ello hemos de tener en cuenta dos conceptos arriba mencionados: el daño efectivo (damnum emergens) y la ganancia pérdida (lucrum cessans), tal y como sanciona el artículo 1106 CC. Para evaluar ese daño efectivo no podemos detenernos en la mera valoración del objeto específico sobre el que recae aisladamente considerado sino que hemos de tener en cuenta que tales bienes están en relación con el resto del patrimonio del afectado de manera que esa pérdida de valor del objeto del daño puede repercutir en los demás. Así el fallo del sistema operativo inutiliza el ordenador y le hace inútil para la tarea prevista: contabilidad, ficheros, datos, etc... pueden perderse como consecuencia del fallo del programa, ese daño no se resarce simplemente con reponer otro ejemplar del programa. Si falla el ordenador que controla las operaciones de vuelo de un aeropuerto se pueden producir accidentes que indirectamente son consecuencia de aquél fallo.

Por otra parte, la cuestión de los perjuicios es más complicada pues se trata de un concepto de más difícil cuantificación y prueba. No es lo mismo alegar, cuantificar y probar un daño efectivo referido a hechos ya sucedidos que hacerlo respecto de unas posibilidades de futuro, muchas veces indeterminadas y aleatorias. La Jurisprudencia ha asentado un criterio más o menos claro: las ganancias cuya percepción se frustra no han de ser dudosas y contingentes, no cabe pues basar la condena en daños y perjuicios en meras y simples suposiciones; así cabe pensar que existe ese lucro cesante cuando la ganancia se hubiese producido desplegando una diligencia normal, cuando dependiera de una simple aceptación, o de una condición potestativa o del transcurso normal de los acontecimientos.

Pensemos en un hipermercado cuyo sistema informático de control de caja falla impidiendo su normal funcionamiento, una cuestión a dirimir será averiguar la causa del fallo e imputar la responsabilidad correspondiente, pero

parece claro que se estimará que por cada día de cierre pierde una media de 10.000 clientes diarios con un gasto aproximado de 4000 pts por cliente. No sólo habremos de evaluar la pérdidas por mercancías perecederas, puesta en funcionamiento del sistema, salarios devengados, sino las ventas que, normalmente, se hubieran podido realizar.

A la hora de imputar esta obligación el Código distingue al deudor de buena o mala fe, a tenor del artículo 1107 CC, el primero responde de aquellas consecuencias necesarias de su falta de cumplimiento; el segundo de todas aquellas que conocidamente se deriven de aquella circunstancia. Sin embargo, la Jurisprudencia ha incidido en la necesidad de un nexo causal entre daños y conducta: ambos deudores responden de aquellos daños y perjuicios que estén directamente unidos o conectados con el hecho causante. Por ello el deudor de buena fe responde de los daños y perjuicios previstos y los previsibles al tiempo de constituirse la obligación, mientras el doloso responde de aquellos incluso de aquellos que no fueran previstos o no podían preverse, y además no puede acogerse al función moderadora del Tribunal que beneficia al anterior en los casos de negligencia, recogida en el artículo 1103 CC.

Siguiendo el ejemplo anterior, si el fallo no se debe a una conducta dolosa, deberá hacer frente el causante a aquellos daños previstos en el contrato y los que normalmente hubiera podido preverse: reparación o sustitución, pérdida de clientes, etc... pero no cabe alegar que algunos proveedores se han desligado del perjudicado o las posibles ganancias derivadas de una futurible campaña de ofertas, etc... El deudor doloso pagará incluso daños y perjuicios no previsibles paro conectados con el acto generador: encarecimiento de productos, pérdida de cartera, créditos lesionados, etc...

En cuanto a la liquidación para determinar la cuantía puede operarse por las mismas partes según acuerdo entre ellos, anterior o no al evento, por la propia Ley, como hace el artículo 1108 CC o por decisión judicial. En todo caso deberá el que la reclama probar el daño y los perjuicios, pudiendo establecerse su cuantía durante el proceso o en el fase de ejecución de sentencia, siempre que deriven de hechos acreditados en la misma. Al ser una cuestión de hecho su apreciación queda reservada a la soberanía del juzgador.

Todo ello debe aplicarse a los distintos supuestos que se pueden plantear en el campo de la informática, si bien la valoración y alcance de los daños y perjuicios se deberá hacer atendiendo a cada caso en concreto. A efectos de este

estudio, vamos a atender a los tres grandes supuestos que, a nuestro juicio, merecen mayor atención: la responsabilidad civil por los productos informáticos, la de los profesionales que prestan servicios informáticos y la de los titulares de los ficheros automatizados de datos. Para ello partimos de los conceptos y principios expuestos en esta primera parte, eludiendo entrar en una complicada casuística a la que seríamos profanos dejando fuera toda una panoplia de problemas concretos que la práctica irá planteando con toda seguridad.

SEGUNDA PARTE

I- INFORMATICA Y RESPONSABILIDAD CIVIL.

Queda patente que la tipología y alcance de los daños y perjuicios es muy diversa pues a su producción pueden concurrir distintos factores y agentes causantes lo cual implica la necesidad de solucionar cada caso concreto según tales circunstancias. Para ello debemos valernos de las normas generales que disciplinan la responsabilidad para cada uno de los tipos de esta pues no existe un régimen jurídico especifico y concreto al que podamos acudir. En consecuencia, vamos a proceder a enunciar cuales serían tales normas y, seguidamente, abordaremos los tres supuestos más interesantes, a nuestro juicio, es decir la responsabilidad del profesional por los servicios informáticos, la responsabilidad por los daños causados por los productos y la del titular de una base o archivo de datos automatizado.

En definitiva, en este campo se dan cita diversas normas relativas a la responsabilidad civil que deberán ser aplicables atendiendo a las circunstancias de cada caso. Así, cuando sean daños originados en el desarrollo del contenido prestacional de un contrato estaremos ante responsabilidad contractual y habremos de distinguir si se trata de un contrato relativo a productos informáticos o a prestación de servicios, cuando el daño provenga del incumplimiento del deber de conducta diligente, sin media contrato, estaremos ante una responsabilidad extracontractual. El carácter objetivo o subjetivo de la misma nos lo indicará el tipo de obligación, medios o resultado, que el sujeto se comprometiera a asumir. Cuando el daño provenga de la intromisión en la intimidad o transmisión de datos sensibles sin consentimiento del afectado, el empresario o autoridad titular del fichero responderán por si mismos y por los hechos causados por sus empleados, merced a las normas de responsabilidad "in eligiendo" impuestas para ellos por el Ordenamiento.

Vamos ahora analizar brevemente los tres supuestos más importantes que pueden plantearse para fijar su régimen jurídico específico de responsabilidad.[26]

II-LA RESPONSABILIDAD POR LOS PRODUCTOS INFORMATICOS.

En lo relativo al software y al hardware hemos de partir del hecho de que se trata de productos fabricados para su comercialización en el mercado de bienes de consumo por lo que quedan sometidos a las normas reguladoras del tráfico y la responsabilidad vigentes en este campo. Lógicamente, el adquirente de tales productos pretende que estos desarrollen todas las prestaciones que el fabricante les atribuye pero, además, contrata la garantía por el correcto funcionamiento de estos y la seguridad de ser resarcido por los daños y perjuicios que un mal funcionamiento de los mismos pueda ocasionarle. Del mismo modo, el adquirente de un programa no sólo ha de ver compensado su interés en que este realice las tareas esperadas, sino que también espera que éste sea original y no se trate de una copia ilegalmente obtenida sobre el que quepa una vindicación de terceros. En cuanto al equipo, este ha de responder a las cualidades exigidas conforme a las normas técnicos normalizadoras que se aplican en ese campo industrial: radiaciones, consumos, etc... vienen establecidos para "normalizar" tales productos y si el equipo no responde a esas normas no cabe admitir su comercialización pues ello puede ser fuente de peligros y daños inadmisibles.

Todas estas consideraciones cobran especial interés en la actualidad pues el proceso de informatización que las pequeñas empresas y los profesionales aumente vertiginosamente, si bien ello no ha sido paralelo a la adquisición de conocimientos técnicos por parte de estos. Es por ello que el deber de asesoramiento y consejo del proveedor se acentúa especialmente, lo cual nos da una medida de la necesidad de que la determinación y cumplimiento de la prestación por parte de éste es de capital importancia.

Pero tampoco debemos olvidar el deber de colaboración de la otra parte, pues sólo una exacta información acerca de las necesidades, objetivos y problemas que plantea el adquirente podrá permitir al suministrador del equipo el

■[26] Vid. Messina de Estrella Gutiérrez:" La responsabilidad civil en la era tecnológica".Buenos Aires, 1989 y "Computers e responsabilitá civile". Dir.G.Alpa, Milano, 1985

hacer una propuesta de solución adecuada al caso; así pues, el deber de lealtad es mutuo. Para ello debe ofrecer al cliente una información veraz, objetiva y exacta de las cualidades, funciones, alcance y limitaciones del equipo o programa propuesto. Ambas partes han de ser diligentes y colaborar a la hora de determinar el contenido de la prestación contractual, sin que por ello olvidemos que a la hora de ejecutar el contrato ambos vienen obligados a cumplir además de lo expresamente previsto, todas aquellas consecuencias que según su naturaleza se deriven de la buena fe, los usos y la Ley.(1258 CC)

Para medir el nivel de cumplimiento debemos atender, en primer lugar, al titulo lícito merced al cual se accede al uso del equipo, sea compraventa, leasing, arrendamiento, préstamos u otro, pero en todo caso hay unas obligaciones de garantía, mantenimiento y responsabilidad ineludibles y la cláusula que imponga una limitación injustificada en este sentido será considerada abusiva. Cada tipo de contrato conlleva un contenido especifico de prestaciones, pero los deberes contractuales antes apuntados de consejo, lealtad, colaboración, etc... permanecen en todos ellos. Aún cuando las posibilidades son varias, nosotros nos ceñimos a la compraventa como supuesto más extendido e interesante a tratar.[27]

En este campo se deben aplicar los dictados de la responsabilidad de carácter contractual cuando el daño se produce dentro de la esfera intersubjetiva de las partes del contrato. Pero en el supuesto en que ese daño se produce en la esfera de un sujeto ajeno a esta relación ha de aplicarse la responsabilidad objetiva para cubrir este evento. Es decir, cuando el daño ocasionado por el producto es consecuencia del incumplimiento contractual debemos atender a si el perjudicado es la otra parte de contrato o un tercero ajeno al mismo. Por ejemplo, si un asesor fiscal recibe un equipo y un programa para realizar la declaración del IRPF a sus clientes y estas dan resultados equivocados que provocan un quebranto a los declarantes tenemos una "cadena" de daños: el que sufre el asesor por pérdida de prestigio y clientela y el de sus clientes por la sanción. La responsabilidad del proveedor deberá establecerse según si el mal funcionamiento es del programa o del equipo y responde por el daño ocasionado al adquirente. Otro cuestión será la responsabilidad frente a los declarantes

■[27] Sobre el contenido más usual de los contratos informáticos, véase Heredero Higueras:" Cláusulas ilustrativas para la negociación de contratos de bienes y servicios informáticos". Rv.Informática y Derecho, nº 1 de 1992, pág,.101 y siguientes.

sancionados: en principio responde el prestador del servicio, asesor, pues cabe exigirle los conocimientos suficientes para que, mediando la diligencia adecuada, pueda detectar el error y subsanarlo. Si el fallo no era detectable ni aún con una diligencia adecuada al caso, tendríamos una responsabilidad exigible al fabricante.[28]

Podríamos establecer un régimen genérico de responsabilidad basándonos en el Código Civil y en ciertas normas especiales:

1- Obligación de saneamiento por vicios ocultos y por evicción:

Los contratos sobre equipos y programas conllevan la obligación de responder por los vicios o defectos que estos padezcan y no fueran conocidos, o cognoscibles, por el adquirente. Así lo dispone el Código en sus artículos 11475 a 1499 y 1553.

Cuando el adquirente encarga un equipo concreto conforme a un asesoramiento previo y un presupuesto dado, los componentes deben ser aquellos pactados, originales y en perfecto estado de funcionamiento, siendo exigible la aprobación del mismo en el acto de la entrega del equipo, si bien esa recepción no supone excluir de plano la responsabilidad pues el cliente no suele ser un perito en la materia y los defectos pueden ser de tal naturaleza que éste no pueda reparar en ellos. (Cfr.1598 CC) Cuando sean equipos standard de marcas oficiales, no clónicos, la responsabilidad recae sobre el fabricante, salvo que el vendedor haya incumplido alguno de los deberes contractuales que le incumben y ello haya sido causa de determinante de una elección errónea o inadecuada. El fenómeno de equipos clónicos que el propio vendedor suele montar en sus dependencias conlleva una doble nota de responsabilidad: como vendedor y como fabricante porque no cabe admitir que se pretenda diferir ésta a un remoto fabricante de un componente dado que ello sería en la practica igual a una exoneración abusiva.

Esta cuestión plantea un especial interés en el caso del software por cuanto el vendedor debe garantizar la originalidad del mismo y la licitud del título por el cual se trasmite, respetando por tanto las normas de la protección de

■[28] Sobre los deberes del proveedor, véase Dario Bergel:" Responsabilidad civil derivada de la informática".Rv. Informática y derecho, nº 4 de 1994

la propiedad intelectual del mismo que nuestra legislación contiene.(Ley de Propiedad Intelectual y Ley 16/93 de 23 de Diciembre.

GETE ALONSO pone de manifiesto que en el software no cabe una plena adaptación de las reglas sobre vicios ocultos pues, por su naturaleza de bien inmaterial, no es admisible la calificación de vicio oculto a los fallos, errores o carencias que puedan presentar. Se inclina por considerar que tales fallos conllevan un incumplimiento de contrato siguiendo la línea que entiende que estamos ante una obligación de medios. Lo cierto es que cuando se comercializa un programa se comprometen funciones que el mismo desarrolla pero no siempre los resultados pues en parte dependen de los conocimientos, aptitudes y habilidades del usuario.

No obstante, cuando el fallo o error sea de una naturaleza que impida el adecuado cumplimiento de la funciones atribuidas al programa, estaremos ante un incumplimiento que ocasiona la obligación de responder por los daños y perjuicios que se ocasionen a consecuencia del mismo.[29] En ningún caso deberá admitirse una cláusula de exoneración que no obedezca a conductas imputables al usuario por mal uso del programa.

De otro lado, la inexistencia de la "atadura o interdependencia" entre máquina y función que el ordenador ha roto implica que el equipo esta capacitado para desempeñar distintas tareas en función del programa que haya de ejecutar; lo cual permite inicialmente,,disociar el binomio hardware-software a efectos de responsabilidad. Pero ello produce a su vez varias consecuencias:

1ª- Que esta disociación depende del software según esté más o menos vinculado a la máquina: no será igual la dependencia del equipo al sistema operativo y de este con el programa de aplicación, que la que vincula al ordenador con el programa concreto que se quiere ejecutar.

2ª- Según las características físicas del ordenador, su capacidad, así serán las posibilidades funcionales que posea de admitir un sistema operativo y de ejecutar programas de aplicaciones. Un equipo obsoleto, con falta de memoria en disco duro o insuficiente memoria RAM, no puede "soportar" determinado software.

[29] Vid. " La contratación..." cit.

3ª- Según el tipo de equipo podrá haber compatibilidad o no con cierto software cuyo empleo será inviable en ese equipo.

Todo ello parte de una base: la necesidad de que ambas partes cumplan con sus deberes contractuales a la hora de fijar las prestaciones: el usuario debe poner en claro sus necesidades, objetivos y posibilidades y el suministrador debe asesorarle y orientarle para que adopte la decisión adecuada. El fabricante, por su parte, debe poner de manifiesto las posibilidades reales de su producto, sus limitaciones, características técnicas y exigencias de equipo o programas que precisa.

2- La obligación de Garantía:

La ley de Consumidores en su artículo 11.2 impone la obligación legal de garantía para todos aquellos bienes duraderos que deberá ser entregada y formalizada por escrito por los productores o suministradores a los usuarios. Ello implica que la garantía no sustituye a la obligación anterior pues son diferentes y compatibles sin que quepa eludir ninguna de ellas por vía de cláusula contractual. Además, como la sentencia de la A.P. de la Coruña de 2/12/94 nos recuerda el artículo 11.3,b de la Ley de Consumidores cuando el producto adquirido es defectuoso es obligación impuesta por la garantía la reparación del mismo, pero si ésta no fuere satisfactoria y el objeto no revistiera las condiciones óptimas para cumplir el uso a que estuviese destinado, el titular de la garantía tendrá derecho a la sustitución del objeto adquirido por otro de idénticas características o a la devolución del precio pagado.

La sentencia de la A.P. de Alava de 6/6/94 precisa que en este caso "no se trata de que la cosa resulte absoluta y materialmente inservible para el uso a que se le destina, sino que es suficiente que su función se vea alterada de forma relevante y las prestaciones que de la misma se esperan incidan en aspectos esenciales de su uso o disfrute", en cuyo caso cabe estimar la existencia de un incumplimiento relevante por la vía del artículo 1124 CC y se procede a declarar la resolución del contrato.

Es reiterada la jurisprudencia que ha establecido que el defecto o fallo ha de presentarse dentro del plazo de garantía y a partir de este momento nace la acción para reclamar el resarcimiento que tiene un plazo de prescripción

de 15 años, a tenor del Código Civil. Los plazos de garantía son pues distintos al de prescripción y al de caducidad.(STS 7/2/95)

El problema se ha venido planteando a la hora de establecer quien es el sujeto ante el que cabe dirigir la acción, pues en unos sistemas el adquirente tiene acción directa contra el fabricante y en otros ha dirigirse hacia el suministrador. En nuestro país, en la práctica, el vendedor entrega la carta de garantía y el usuario ha de dirigirse al servicio técnico que el fabricante tenga instalado; ello ha ido consagrando la práctica del que el suministrador quede desvinculado con el comprador una vez que ha vendido el equipo. Realmente ello no debe ser así pues las obligaciones de saneamiento y garantía son consecuencia del contrato de adquisición y la Ley de Consumidores no excluye al suministrador del equipo, sino que le coloca junto al fabricante a la hora de responder ante el adquirente; máxime cuando sean los equipos clónicos de fabricante original desconocido por lo que el comprador sólo puede dirigirse contra el vendedor que debe responder por el equipo que comercializa por su cuenta y riesgo.

En cuanto al software hemos de precisar que cuando es software de base éste ha de adecuarse al equipo y sus condiciones especificas, por lo que ha de ser compatible e idóneo, obligación que se acentúa cuando se adquiere conjuntamente con el hardware. Normalmente, se suele proveer junto con el equipo y ya instalado, y su elección se hace conforme a las necesidades planteadas por el usuario al vendedor y éste lo propone en base a su deber de consejo y asesoramiento, respondiendo de su licitud e idoneidad, pues de lo contrario hay incumplimiento contractual pues en este caso cualidades y objetivos van más unidos que en el caso del software de aplicación.

En lo relativo a los programas de aplicación el usuario adquiere el derecho de utilización de los mismos y queda sometido a los deberes que la legislación sobre propiedad intelectual le impone. En cuanto a su correcto funcionamiento debemos estar a las normas generales aplicables al resto de los productos. Cuando sea un programa creado ex profeso estamos ante un contrato de obra con todas sus consecuencias.

3- Responsabilidad por productos defectuosos:

Hasta aquí hemos analizado la teoría general sobre responsabilidad basándonos en la idea de la insatisfacción de la utilidad esperada por el usuario o adquirente del producto informático. Para ello hemos utilizado

las normas reguladoras de la compraventa, en la medida en que tratan de proteger a una parte frente a la utilidad frustrada que razonablemente cabe esperar del bien según sus circunstancias y propiedades; es decir, "protegen al comprador contra los defectos que impiden o afectan a la utilidad del objeto de la prestación del vendedor" pues nos desenvolvemos en el campo del incumplimiento.[30]

No obstante, para el campo de la protección del consumidor frente a los riegos o daños imprevisibles que ocasionen los productos hemos de hacer una mención especial a la Ley de 6 de Julio de 1994 relativa a la responsabilidad civil por los daños causados por productos defectuosos, que incorpora la Directiva 85/374/CEE de 25 de Julio que pretendía establecer un régimen jurídico armonizado en toda la Comunidad sobre esta materia, para lo cual consagra la aplicación del principio de responsabilidad objetiva y solidaridad en caso de daños personales o materiales que afecten a las personas con independencia de que sean o no consumidores en sentido estricto, lo cual amplia el ámbito subjetivo de protección pues supera el estricto concepto de " consumidor " del artículo 1.2 de nuestra Ley 26/84 que se circunscribe a las personas, físicas o jurídicas, destinatarios finales del producto o servicio.

Este punto es una de las más interesantes aportaciones con respecto a la Directiva de origen, dado que la doctrina entendía que la norma comunitaria era aplicable solamente al consumidor, quedando las empresas y profesionales fuera de su ámbito de protección, para ello se basaban en el hecho de que estos sujetos ostentarían una posición de mayor igualdad con respecto a fabricantes e importadores y que tales daños podían estar previstos en los contratos celebrados al efecto; ello no siempre es así pues cada vez se da una mayor concentración en el mercado en favor de las grandes multinacionales, como sucede actualmente en la informática. Sin embargo no sería lógico admitir que el afectado sea sólo el consumidor "strictu sensu" por lo que esta ampliación del ámbito de los sujetos protegidos por la norma es, a nuestro entender, justa y adecuada por igualitaria y precisa.

Los derechos reconocidos por esta Ley tienen un plazo de caducidad de diez años desde que se pone en circulación el bien mueble causante del daño, pero ejercitada la acción por el daño, se abre un plazo prescriptivo con relación a

■[30] Vid. Alcover Garau:" La responsabilidad civil del fabricante".Madrid, 1990

la misma. Dicha prescripción funciona conforme al sistema siguiente: dentro de ese plazo si se produce el daño o perjuicio el afectado tiene un plazo de 3 años para ejercitar la acción de reparación a contar desde que se sufre el perjuicio, a consecuencia del defecto o del daño ocasionado por aquél, y siempre que se conozco al responsable. El sujeto que haya satisfecho la indemnización tiene una acción para dirigirse contra los demás responsable sometida a un plazo prescriptivo de 1 año a contar desde que hace efectivo el pago de la misma. Como se trata de prescripción extintiva, todos sus extremos, no sólo la interrupción, se rigen por las normas generales del Código Civil.

El ejercicio de estas acciones no afecta a la defensa de otros derechos que el perjudicado pueda tener como consecuencia de la responsabilidad contractual o extracontractual del fabricante, importador o cualquier otra persona responsable. Con ello se mantiene la teoría de la concurrencia de acciones antes expuestas, sobre todo en relación a posibles responsabilidades penales.(art.15)

En su artículo 1 señala como responsables a los fabricantes e importadores de los productos, con lo cual se instituye una responsabilidad que les vincula a ambos frente al perjudicado. Se entiende por fabricante al que produce el producto terminado, o uno de sus elementos integrantes o las materias primas; tiene esta misma calificación la persona que se presenta al público como tal colocando su nombre, denominación social, su marca o cualquier otro distintivo en el producto, envoltorio, envase o en cualquier otro elemento de protección o presentación. (fabricante aparente) La doctrina incluye en este concepto amplio al llamado "assambler" que encaja o combina los componentes o productos manufacturados por otros sujetos, pero no al mero instalador. Con ello se aplica un concepto muy amplio que sirve para determinar el ámbito subjetivo aplicable a esta Ley y se facilita su cumplimiento. Además, si no pudiera identificarse al fabricante, será considerado como tal quien haya suministrado o facilitado el producto, salvo que en el plazo de tres meses indique al dañado o perjudicado la identidad del fabricante o de quien le hubiera suministrado el producto. Esto mismo se aplica si el producto es de importación, si en este no figura el nombre del importador aún cuando se indique el del fabricante. Es importador el empresario que introduce en la Unión Europea un producto para su venta, arrendamiento financiero o cualquier otra forma de distribución.(Art.4) La Disposición adicional única dispone que el suministrador del producto defectuoso responderá como si fuera el fabricante o importador cuando haya suministrado el producto a sabiendas de la existencia del defecto, aunque luego pueda ejercitar la acción de repetición contra aquellos.

Esta responsabilidad es solidaria conforme al artículo 7 pues se trata de impedir que el sujeto que sufre el daño pueda quedar sin reparación como consecuencia de no poder hacerse una imputación individualizada de la responsabilidad. A titulo de ejemplo, las concesionarias de marcas de vehículos o sus agentes son considerados por los Tribunales como mandatarios o comisionistas del fabricante, importador o filiar del primero y ello con independencia de las relaciones internas que no pueden perjudicar a terceros compradores en la medida en que estos son ajenos a aquella relación, por lo que se impone una responsabilidad directa y solidaria de ambos.(Cfr.A.P. Alava 6/6/94)

Incluso cuando media la intervención de un tercero, el artículo 8 sigue la línea de asegurar la reparación, pues la responsabilidad del fabricante o importador no se reduce cuando el daño sea causado conjuntamente por un defecto del producto y por la intervención de un tercero; aunque luego pueda repetir al tercero la parte que le corresponda de la indemnización que ha satisfecho en base a su tanto de intervención en el daño. Tal y como vimos antes, se trata de la aplicación a este campo de las modernas líneas del Derecho de Daños, pues hoy el comerciante va perdiendo relevancia en su papel frente al consumidor en la medida en que éste se relaciona más con el fabricante pues en el comercio actual muchas veces el vendedor es un profano en la materia relativa al producto y se limita a cobrarlo.

Sin embargo, cuando media culpa del perjudicado o de una persona por quien este haya de responder civilmente (menores, empleados) la responsabilidad se reduce o suprime si el daño es consecuencia del defecto del producto y de la conducta de aquellos sujetos. Esa concurrencia de causas puede deberse a una actividad conjunta de ambas o a que una sea determinante de la otra, lo cual implica que en cada caso habrá de probarse lo que se alegue pero, en principio, si hay defecto habrá responsabilidad.(art.9)

En su artículo 14 la Ley declara la plena nulidad de las cláusulas limitativas o d exoneradoras de la responsabilidad prevista en ella.

Se considera producto todo bien mueble aún cuando esté unido o incorporado a otro mueble o inmueble; esto implica que se incluyen los alimentos, los materiales de la construcción, los productos artesanales y artísticos, los componentes electrónicos, el gas, la electricidad, los productos de la minería,

incluso agua mineral y aquellos que se facilitan en el seno de una relación de servicios y los bienes usados. Por el contrario, se excluyen los servicios, los inmuebles, los residuos, los órganos humanos, la sangre y aquellos similares que no se producen para la venta o son excluidos por la Ley: materias primas agrarias y ganaderas, y los de caza y pesca que no hayan sufrido transformación inicial. (art.2)

El artículo 3 recoge el concepto legal de producto defectuoso aquél que no ofrezca la seguridad que cabría legítimamente esperar atendiendo a su presentación, uso previsiblemente razonable y el momento de su puesta en circulación. Se considera defectuoso en todo caso si no ofrece la seguridad normalmente ofrecida por los demás ejemplares de la misma serie. Como consecuencia de ello se deduce que no se trata de proteger al sujeto de un riesgo evidente y previsible que el producto pueda ocasionar, pues ello le era conocido: el adquirente de un explosivo o de un medicamento con efectos secundarios conocidos y previstos, sabe, conoce y asume el riesgo y no cabe apoyarse en la Ley para reclamar. Además, debe estudiarse cada caso en concreto pues según el tipo de producto y sus destinatarios habremos de evaluar cual se su utilización adecuada: no es lo mismo un juguete para niños que un disolvente químico para especialistas de laboratorio, pues hay más riesgo de una utilización inadecuada por aquellos, que su manipulación imprudente por estos. es por ello que para valorar esa ausencia de seguridad habremos de atender a una serie de criterios que la misma Ley establece: presentación, uso razonablemente previsible y momento de su puesta en circulación.(art.3)

La jurisprudencia hace hincapié en la necesidad de prever que determinados sujetos como niños, ancianos, deficientes mentales, etc... pueden observar una conducta imprudente por lo que se han de extremar las cautelas en tales casos. Cada producto posee su destinatario-tipo y a ello debe atenderse. (Cfr. A.P. Palencia de 21/12/94)

A titulo de precedente podemos citar la sentencia del Tribunal Supremo de 19 de Diciembre de 1994 en un caso de explosión de un artefacto pirotécnico cuya comercialización y uso se regula por una normativa legal específica en la cual se impone la obligación de que sea utilizado exclusivamente por personal perteneciente a un taller de pirotecnia debidamente legalizado; además debe ir correctamente etiquetado, lo cual no se cumplía en este caso, no advirtiéndose tampoco de sus riesgos al adquirente. Tal conducta no supone una mera infracción administrativa, sino que constituye la causa directa del daño cuya

reparación se reclama pues se ha creado un grave riesgo para el usuario, por lo que cabe deducir la responsabilidad de quien ha sido creador de ese riesgo merced al artículo 1902 CC. La Sala aplica además la Ley de Consumidores sobre la base de la Directiva 85/374 CEE, que en ese momento no había sido incorporada aún, por tratarse de un producto peligroso sometido a unos requisitos legalmente previstos. En tal sentido, afirma la sentencia:" El artefacto explosivo entra, sin ninguna duda, en el supuesto de hecho del párrafo 1° del artículo 28 de la Ley de Consumidores. El fabricante no ha controlado su elaboración a fin de su debida clasificación según los Decretos aplicables, con radical influencia en las personas que lo podían utilizar. Se impone la responsabilidad objetiva del artículo 28". Cuando el fabricante alega la incorrección del uso por parte del perjudicado, la Sala le contesta que es irrelevante pues no se trata de un explosivo de clase 2ª, que puede ser utilizado por los mayores de 18 años, sino de uno de clase 3ª cuya utilización es exclusiva para personal especializado; máxime cuando no había etiquetado que lo anunciara, ni el afectado era pirotécnico. Finalmente, establece la responsabilidad solidaria conforme al artículo 27 de la ley de Consumidores para los demandados: fabricante y vendedor del producto que originó el daño.

No se entiende defectuoso el producto por el mero hecho de que posteriormente se le ponga en circulación de forma más perfeccionada: sería el caso de automóviles que incorporen el ABS o monitores que poseen un índice más bajo de radiación; pero si lo es cuando uno de ellos ofrece menos seguridad que el resto de productos de su misma serie.

El artículo 10 establece el ámbito de protección en cuanto a la tipología de daños cubiertos: muerte, lesiones corporales y los daños patrimoniales causados a las cosas distintas al propio producto cuando estas se hallan destinadas objetivamente al uso o consumo privado y en tal concepto la hubiera utilizado principalmente el perjudicado. En este caso existe una franquicia de 65000 pts y en todo caso un límite de 10.500.000.000 pts, siendo estas cuantías revisables periódicamente según la disposición final tercera. Para los demás daños y perjuicios, incluidos los morales, se puede acudir a la vía de la legislación civil general para su resarcimiento. La prioridad concedida a los daños personales es lógica pues la salud-integridad física es el objetivo fundamental a proteger por la Ley, sea muerte o lesión corporal la indemnización alcanza al daño efectivo y al lucro cesante, pues así se deducía del artículo 9 de la Directiva de la que ésta trae causa.

En lo relativo a daños patrimoniales, de salida se excluye el propio producto pues viene resuelto en el propio contrato de compraventa. La ley exige un requisito objetivo: bienes normalmente destinados al uso o consumo privado; y otro subjetivo: que se utilicen principalmente para tal fin. Pero el término "privado" no debe ser interpretado en un sentido restrictivo pues ello sería contrario al espíritu de la norma ya que esta no se limita a proteger actividades privadas de consumo. Los bienes que objetivamente sean de uso privado pueden ser utilizados en actividades de empresa o profesionales, pero quedarían fuera del ámbito de aplicación de la norma, tal y como se ha interpretado la Directiva 85/374 CEE; pero la terminología utilizada por los textos citados no es demasiado clara. Pensemos en el equipo informático instalado en una consulta privada y susceptible de una doble utilización profesional y personal, o en el de una pequeña empresa familiar; no parece lógico excluir de raíz del ámbito de la Ley tales supuestos dudosos pues ello generaría desprotección lo cual es contrario a los principios generales del Derecho de daños antes citado. Por ello la doctrina establece un criterio doble:

- La protección alcanza a todas las personas por los daños personales cuando realicen una actividad de consumo, de empresa o profesional.

- Cuando se trate de daños materiales la protección alcanza al consumidor o adquirente o a cualquiera que utilice el producto o resulte dañado por él. Este segundo criterio restrictivo debe ser tratado con cautela pues el término principalmente del artículo 10.1 no admite una interpretación extensiva.

En cuanto a la valoración del daño patrimonial, la ley se refiere a los daños en cosas distintas al propio producto, de ello parece deducirse que se cubre el daño efectivo causado a las mismas, pero no los perjuicios y lucros cesantes que han de reclamarse por la vía de las normas generales, como establece el artículo 10.2 de la Ley. Así, la pérdida del disco duro se sustancia por esta vía, pero la de su contenido y el tiempo sin poder utilizarlo deben reclamarse por las vías antes comentadas, según proceda.

En cuanto a los daños morales no parece que puedan revestir excesiva importancia pues la pérdida o deterioro del producto no debe ser muy "dolorosa", pues realmente estos van aparejados a los daños personales y muerte en los cuales no hay franquicia según la propia norma.

El establecimiento de una franquicia en los daños materiales se debe al deseo de evitar una excesiva proliferación de pleitos sobre la cuestión, si bien es lógico coincidir con ALCOVER GARAU que cuando la suma de los daños individualizados supere la franquicia debe aplicarse la protección legal. También cabe decir que deben crearse vías más rápidas y eficaces para las reclamaciones de cuantía inferior pues ello provocará sin duda desprotección.

Para la prueba de los daños y perjuicios el artículo 5 asienta el principio base de todo el moderno sistema de responsabilidad: el perjudicado ha de probar el defecto, el daño y la relación de causalidad entre ambos. Para ello, pensamos, debe atenderse al uso adecuado y la diligencia esperable del usuario, pero si hay daño y defecto existe nexo, salvo causa de exoneración que debe probarse. Para ello, las normas técnicas de normalización en la fabricación de los productos y su observancia servirán de criterio de control a tales efectos.

También debemos atender a la prueba de presunciones que es hábil para inducir la relación causal como recuerda la sentencia de la A.P. de Córdoba de 8/11/94 que la conecta con los artículo 25 y 26 de la Ley de Consumidores que protegen al consumidor de una prestación no idónea e incorrecta. Basándose en los indicios deduce que el incendio operado en un vehículo reparado en un taller y que derivan de que "el accidente se produjo a las pocas horas de sacar el vehículo del garaje, de forma sorpresiva e inesperada, y cuando el usuario del mismo hacia un uso totalmente normal"; en razón de que a esa inmediatividad temporal entre el servicio prestado y el resultado producido se une otro factor de importancia decisiva "cual es la entidad del servicio prestado ya que la razón por la que el turismo fue llevado al taller era precisamente el calentamiento anómalo del motor". Seguidamente, analiza el sistema establecido por la Directiva 85/374 que posee una doble proyección: una, excepcional, de carácter objetivo de su artículo 28 y otra normal de índole cuasi-objetiva en su artículo 25 que presume la culpa por la que basta al reclamante acreditar el daño y la relación de causalidad entre el mismo y la utilización del vehículo. Siguiendo al Tribunal Supremo, establece la inversión de la carga de la prueba de manera que para exonerarse de su obligación de indemnizar ha de probar, o bien un uso indebido, negligente o temerario por el usuario, o bien que ha cumplido por su parte todas las previsiones que le son exigibles. Como nada de ello se ha probado "ante el cúmulo de datos indiciarios que permiten inducir la relación causal" se condena al taller de reparación.(Cfr.STS 20/10/90 y 23/5/91)

La STS de 1/2/95 nos recuerda que los artículos 1249 y 1253 CC dedicados a las presunciones no operan en los casos en que se obtienen claras conclusiones por otras vías objetivas de prueba como la documental.

Las causas de exoneración de responsabilidad están recogidas en el artículo 6 y recogen varias posibilidades que atienden a criterios diversos. Un primer grupo de causas generales son aquellas que exigen prueba por parte del fabricante o importador pues sólo juegan cuando estos demuestran:

a) Que no habían puesto en circulación el producto.

b) Que, dadas las circunstancias del caso, es posible presumir que el defecto no existía en el momento en que se puso en circulación el producto.

c) Que el producto no se fabricó para su venta o distribución con finalidad económica, ni tampoco fabricado, importado, suministrado o distribuido en el marco de una actividad profesional o empresarial.

d) Que el defecto se debió a que el producto fue elaborado conforme a normas imperativas existentes. Se ha de referir a normas técnicas normalizadoras de esa actividad productiva industrial que sirven de criterio básico para contrastar estos supuestos de responsabilidad objetiva como ha consagrado la jurisprudencia.

e) Que el estado de los conocimientos científicos y técnicos existentes en el momento de la puesta en circulación no permitía apreciar la existencia del defecto. Se incorpora aquí una causa de exoneración utilizada en otros campos cual es la del estado de la técnica, es decir, que los medios y conocimientos aplicables en aquél momento a la producción no permitían razonablemente conocer que el producto era defectuoso. Esta causa no opera en el caso de que se trate de medicamentos, alimentos o productos destinados al consumo humano, pues los sujetos responden en todo caso.

Por otra parte, cabe una exoneración parcial de responsabilidad en favor de uno de los sujetos que participa en el proceso de producción: el fabricante o importador de una parte integrante de un producto terminado no serán responsables si prueban que el defecto es imputable a la concepción del producto al que ha sido incorporada o a las instrucciones dadas por el fabricante del producto. Ello es lógico en cuanto se trata de una "mala utilización" del

componente a la que es ajeno el sujeto exonerado pues no participa en la producción final del producto o sigue instrucciones del fabricante.

Finalmente, para asegurar la eficacia de la norma se introduce una reforma en el artículo 30 de la ley de Consumidores merced a la cual el Gobierno prevé la posibilidad de establecer un seguro obligatorio de responsabilidad civil por los daños causados por los productos o servicios defectuosos y un fondo de garantía que cubra, total o parcialmente, los daños consistentes en muerte, intoxicación y lesiones personales. Con ello se pretende asegurar el resarcimiento mediante el progresivo establecimiento de lo que se ha dado en llamar "una sociedad de seguros" en la que toda actividad de riesgo ha de ser cubierta con el correspondiente contrato de cobertura de responsabilidad.

Esta Ley es aplicable a los productos puestos en circulación con posterioridad a su entrada en vigor el día 8 de Julio de 1994. Con ella se completa el panorama amplio del régimen jurídico de responsabilidad aplicable a los productos informáticos si bien, como hemos dicho, habremos de atender al tipo y contenido concreto de los contratos que con respecto a los mismos se celebren por las partes, si bien estos han de respetar en sus cláusulas los límites ya apuntados. Por tanto, se debe distinguir en cada supuesto cuando estamos ante un incumplimiento contractual que faculta para resolver el contrato y cuando entra en funcionamiento la obligación de garantía, cuyas consecuencias están reguladas por la teoría general del contrato y las cláusulas válidas del mismo. Por otra parte, existen supuestos de responsabilidad extracontractual en los que el afectado puede ser el mismo adquirente o un tercero y que se regulan por la vía de la responsabilidad extracontractual establecida por la Ley.

En este campo, la doctrina ha venido distinguiendo la responsabilidad del fabricante del hardware regida por una responsabilidad objetiva que impone la obligación contractual de reparar el vicio o defecto del equipo y la extracontractual de responder por los daños ocasionados a terceros. Normalmente, los defectos suelen ser fácilmente subsanables, pero los daños, más que físicos, suelen consistir en quebrantos económicos difícilmente mensurables.

En el campo del software se diferencia el sistema operativo cuando éste proviene del propio productor de los equipos por lo que en caso de error hace inviable la obtención de determinadas utilidades del equipo y se vincula a este. Cuando procede de otro fabricante, se habrá de tener en cuenta la relación entre el sistema operativo elegido y el equipo en el que se pretende utilizar, pues

la atribución de responsabilidad depende de la idoneidad objetiva de uno y otro; en caso de error en el sistema operativo, deberá el acudirse a los criterios de responsabilidad por el producto antes apuntados. En cuanto a los programas es más difícil poder mensurar adecuadamente la medida en que un fallo en la concepción o elaboración del mismo pueden provocar el daño, no obstante, podemos considerar que si no se alcanza el resultado comprometido por el fabricante o vendedor, según sus deberes contractuales, deberá valorarse el alcance del daño que ello produce al usuario a efectos de su reparación.[31] Es necesario, por tanto, que el fabricante, importador o proveedor de los productos informáticos suscriba un contrato de seguro para cubrir la responsabilidad, legal o contractual, por los daños que su actividad ocasione y asegurar la indemnización.[32]

III LA RESPONSABILIDAD DEL PROFESIONAL PRESTADOR DE SERVICIOS INFORMATICOS.

1- El status del profesional.

La posibilidad de elegir libremente una profesión u oficio es una auténtica "conquista" social pues supone consagrar una autonomía de decisión personal en orden a la posibilidad de decidir el libre desarrollo de nuestra personalidad en una esfera tan esencial como la del trabajo. Pero ello no pasaría de ser una mera retórica sino se pudiera igualmente acceder a los conocimientos y técnicas profesionales que capacitan al sujeto para ostentar ese "status" profesional que le identifica y distingue. Por tanto, la libertad de acceso a la profesión forma parte de esos principios fundamentales del orden político y la paz social que la Constitución consagra.[33] La profesión se define como "el empleo, facultad u oficio que cada uno tiene y ejerce públicamente", lo cual implica una "publicidad natural" pues se realiza de forma pública y notoria ante los demás. Existe, por otra parte, una "publicidad formal" que se deduce de determinados

■[31] Vid. "Computers...".cit. pág.75 y ss

■[32] Sobre el contenido ususal de tales contratos de seguro, véase Linant de Bellefonds y Hollande:" Droit de l'Informatique".París, 1984, página 208 y siguientes.

■[33] Vid. Gálvez en "Comentarios a la Constitución".Dir. G.Falla, Madrid, 1985

instrumentos que patentizan esa cualidad: expedición del titulo correspondiente, colegiación, inscripción en un registro específico, etc... Merced a ello cabe entender la profesión como una ocupación que requiere una formación especifica previa, que está gobernada por su propio código de conducta deontológica.[34]

Lo que caracteriza a la profesión así entendida son lo saberes intelectuales, científicos y técnicos, que se han de aplicar en su ejercicio y cuya posesión por el sujeto se sobrentienden y forman la base del reconocimiento social de esa actividad. Hay por tanto, un "núcleo esencial de saberes " cuya adquisición y dominio puede estar, o no, refrendada oficial y formalmente por un título expedido al efecto. El profesional tiene así una cualificación especial: es aquella persona que posee los conocimientos y la experiencia necesaria para aplicarlos adecuadamente en el ejercicio de su actividad. En consecuencia, la titulación o colegiación no son los elementos que identifiquen al profesional, sino su nivel técnico o científico, su experiencia y su aptitud para asumir y desempeñar las tareas aparejadas a su actividad.

Según desempeñe su labor podremos obtener los criterios necesarios para medir el grado de cumplimiento de sus obligaciones profesionales y establecer la medida de la responsabilidad que le es imputable por las consecuencias del desempeño de las mismas. Incurrirá en ella si no llega a alcanzar el nivel de competencia que cabe esperar razonablemente de él, lo cual implica una titulación adecuada y una continua puesta al día en consonancia con la evolución de los conocimientos y las técnicas de su campo de actuación profesional.

De los artículos 35 y 36 CE cabe deducir que no se identifica la profesión con el "modus vivendi", pues puede ser una simple expresión de la personalidad del sujeto sin necesidad que se obtengan rendimientos económicos de su ejercicio. Igualmente, esta capacitación previa implica la consagración de una esfera o área de libertad profesional, entendida en dos sentidos:

- Libertad de elegir voluntariamente una profesión determinada.

■[34] Vid. Souviron Morenilla:" La configuración jurídica de las profesiones tituladas en España y en la CEE".Madrid, 1988

- Libertad de ejercicio de la profesión como consagración de una esfera de libre decisión del contenido de los actos del profesional.

No obstante, el interés general impone unas ciertas intervenciones de distinto tipo:

- Unas se basan en los llamados "presupuestos subjetivos de ejercicio profesional" referidos a los conocimientos y aptitudes previas exigidos al sujeto.

- Otras se basan en "presupuestos objetivos", que implican unas condiciones previas que el sistema impone para acceder a la profesión: numerus clausus, oposiciones, pruebas o colegiación.

- Las intervenciones "de ejercicio" están referidas al desempeño de esa actividad: honorarios, tasas, impuestos, etc...

La importancia de todo ello exige que la regulación del ejercicio de tal actividad se haga por "Ley" o "en base a una Ley" permitiendo que las cuestiones esenciales las regule una norma jurídica de este rango, aunque su desarrollo posterior se haga por vía reglamentaria. Ello se debe a que en esta materia el interés público es bien patente pero limitado por el respeto a la libertad de la persona y a los valores antes apuntados. De ahí que se haya consagrado un contenido esencial que asegura un marco de libre decisión y actuación al profesional responsable que ninguna norma puede invadir.(art.36 CE) En consecuencia, podemos afirmar que ninguna norma, legal, colegial o empresarial puede invadir ese "ámbito de libertad" de ejercicio asegurado al profesional que se basa en el "núcleo esencial" de saberes y aptitudes exigidos para desempeñar la profesión.[35]

Esto implica una independencia profesional que no se empaña por el hecho de que este realice su actividad por cuenta propia, como autónomo, o mediante una relación funcionarial o laboral por cuenta ajena. Su libertad e independencia está referida a ese marco de libre actuación responsable que se plasma en la posibilidad de decidir el contenido de sus actos de esta índole libre de injerencias o imposiciones inadmisibles.

■[35] Vid. Sáinz Moreno:" Comentarios a las Leyes Políticas".EDERSA, Madrid, 1985

En lo que a nosotros interesa es básico referirnos a la profesión sujeta o reglamentada cuyas condiciones de acceso y ejercicio están reguladas por normas, pero además para su desempeño se exige la posesión de un título previo que acredita la capacitación adecuada; de ahí surge el concepto de profesión titulada que es aquella para la que el titulo capacita. Esa reglamentación profesional ha de respetar aquel marco de independencia y libertad del que antes hablábamos, pues se trata de una libertad responsable en base a la cual se valora la idoneidad técnica y científica de la conducta profesional, constatando si sus actos se adecuan o no a las reglas que rigen su profesión y de ese juicio se obtiene la base para una posible pretensión por incumplimiento contra el profesional.

De todo ello se deduce la necesidad de elaborar un catálogo de categorías de los profesionales informáticos y la relación de competencias, titulaciones y reglas de actuación, para ello sería útil la creación de un Colegio Profesional u otro organismo similar que coordinara tales cuestiones y actividades.

2- El profesional prestador de servicios. Consecuencias de su actuación.

Dependiendo del tipo de profesión y el vínculo que liga al profesional con el destinatario de sus servicios podremos establecer si estamos ante una obligación de medios que implica un deber de diligencia, con una responsabilidad que se basa en un criterio subjetivo o de culpa, o bien se trata de una obligación de resultado, sometida profesionalmente a una reglas técnicas y cuya responsabilidad es objetiva, ajena a toda idea de culpa. Básicamente, el problema a solucionar es el de la valoración de las dos fases que componen el acto profesional: la concepción y su ejecución o resultado. Para ello podemos atender a dos criterios diferentes: en primer lugar, contrastar se la actuación profesional se ajusta a las reglas del arte u oficio que rigen su profesión ("Lex Artis") valorando la diligencia y conocimientos desplegados; o podemos atender al resultado, en la medida que sea el que debe obtenerse como consecuencia de la adecuada aplicación de las "normas técnicas".

En el primer caso, buscamos un nexo causal entre la conducta y el resultado, basándonos en un criterio subjetivo: si se puso o no la diligencia adecuada al caso; en el segundo, utilizamos un criterio objetivo analizando el resultado obtenido, basándonos en las reglas técnicas que "normalizan" ese tipo de actuación.

En esta tarea es imprescindible distinguir si estamos ante una obligación de medios o de resultado, y para ello seguimos a la doctrina según la cual "en la prestación de actividad, el deudor se compromete únicamente a su esfuerzo y por consiguiente cumple cuando este esfuerzo ha sido desarrollado. Si existe una actividad del deudor destinada a cumplir, habrá sólo cumplimiento defectuoso en la medida en que no observe una diligencia normal. En cambio, si la prestación es de resultado el deudor no compromete su actividad , sino también el resultado que ha de obtenerse con ella. Por eso, si hay actividad, pero no resultado, no habrá cumplimiento aunque defectuoso, sino verdadero y propio incumplimiento". En consecuencia, cabe concluir que la prestación de actividad forma parte de un contrato de trabajo o de servicios, por el que el profesional se compromete a desplegar su actividad diligente, mientras que la de resultado se integra en el contrato de ejecución de obra.[36]

La sentencia del Tribunal Supremo de 24/12/1994 deja muy claro en que consiste esta relación jurídica cuando dice que en supuesto en que se contratan servicios se configura un negocio consensual, oneroso, bilateral y conmutativo en el que su objeto viene determinado por una por una específica actividad que se presta por una de las partes a la otra, pero no se compromete ni se contrata un efectivo resultado, por lo que el negocio se concreta a llevar a cabo la actividad pactada, aunque la misma se oriente a producir el resultado que se espera de la prestación recibida. Igualmente, resalta la imprescindible colaboración de la otra parte para que la actividad desplegada sirva para lograr el resultado previsto, pero no comprometido; es el deber de diligencia y colaboración del receptor del servicio. Como dice la STS de 7/2/95 en el arrendamiento de servicios no es determinante la consecución del resultado, al contrario que en el de ejecución de obra.

En el primer tipo de contrato aunque no se logre el resultado el profesional ha cumplido si despliega toda su diligencia conforme a los conocimientos y prácticas exigibles según el estado de la ciencia o arte y del momento y los medios puestos a su alcance; de manera que le será imputable el no lograr el resultado cuando medie una conducta ignara o negligente conforme a su "lex artis" profesional. En el segundo, valoramos el resultado, de suerte que si no se ha alcanzado existe responsabilidad por incumplimiento del objeto

[36] Vid. Diez Picazo:" Fundamentos de Derecho Civil Patrimonial".Madrid,1986, vol.1°

comprometido en el contrato, con abstracción de cualquier valoración subjetiva de conductas; nos valemos de las normas técnicas que normalizan esa actividad. En razón de ello, la doctrina francesa denomina a las primeras como "normas de saber hacer" y a las segundas "normas de resultado". A titulo de ejemplo, podemos citar en el primer caso a un médico y en el segundo a los profesionales de la construcción.[37]

Aplicando todo ello al campo del profesional de la informática podemos concluir que esta es una profesión titulada y reglada que implica la adquisición previa de unos conocimientos y aptitudes que son esperables merced a la acreditación profesional que se ostente. A la hora de establecer la responsabilidad civil por su actuación habremos de atender a la circunstancia concreta de cada caso: tipo de relación que le liga con el sujeto que ha sufrido el daño, sea contractual o extracontractual y cual fue el compromiso adquirido. No obstante, podemos ya avanzar que conforme a las líneas que la jurisprudencia actual mantiene y a la legislación futura sobre la materia, al informático se le aplica la responsabilidad objetiva como prestador de servicios, tal y como se deduce de la Propuesta de Directiva CEE de 9 de noviembre de 1990, pues en virtud de esta se invierte la carga de la prueba en favor de la víctima. A tenor de su artículo 1 el prestador de servicios es responsable del daño causado por su culpa en el marco de la prestación del servicio, ya sea a la salud y a la integridad física de las personas, o a la integridad física de los bienes muebles o inmuebles, incluidos los que sean objeto de la prestación.

En consecuencia, si el profesional ocasiona un daño de cualquier tipo, personal o económico, como consecuencia de su actuación, éste le será imputable pues la carga de la prueba le incumbe a él. Así, el informático que daña el sistema, o los equipos u ocasiona un defectuoso funcionamiento de los mismos deberá responder por el mismo, salvo que pruebe que ello obedece a una causa externa a su actuación que él no pudo prever o impedir. El artículo 4 entiende por daño a tales efectos:

a- el daño directo causado por la muerte o por cualquier atentado a la salud o la integridad física de las personas.

■[37] Vid. Pennau:" Regles de l'art et normes techniques".Paris, 1989 y Hoorens y otros:" Les contrats..." cit. pág.19 y siguientes.

b- el daño directo causado por cualquier atentado contra la integridad física de los bienes muebles o inmuebles, incluidos los animales cuando sean de un tipo destinado normalmente al uso o consumo particular.

c- los daños materiales de carácter económico derivados de los anteriores.

Será prestador de servicios cualquier persona física o jurídica que en el marco de su actividad presta cualquier prestación a titulo profesional o de servicio público , de forma independiente, a titulo oneroso o no. En este concepto se incluye a los que proporcionan tales servicios utilizando un representante o cualquier otro intermediario jurídicamente dependiente. Esta responsabilidad no se atenúa aún cuando el daño sea causado conjuntamente por culpa suya y por intervención de un tercero, pero si se atenúa o desaparece cuando a concurrencia de culpas de la víctima o de una persona de quien esta sea responsable. En consecuencia, cuando el profesional actúe por cuenta ajena hemos de aplicar las normas del Código civil relativas a la responsabilidad por hechos de terceros, siendo responsable su empleador, pero pudiendo éste repetir contra su empleado. Cuando la responsabilidad recaiga sobre varias personas estamos ante un supuesto de solidaridad, con independencia de la acción que cada una tenga contra la otra para repetir aquello que hubo de pagar por ella. En ningún caso, se admite que el prestador del servicio aplique en el contrato una cláusula limitativa o de exclusión de responsabilidad, pues esta será nula.

Finalmente, corresponde a la víctima probar la existencia efectiva del daño y la relación de causalidad entre éste y el servicio prestado, pero debe ser el prestador quien pruebe la ausencia de culpa de su parte para lo cual es esencial atender a su comportamiento quien debe garantizar la "seguridad que cabe esperar legítimamente". Esta es la cuestión más polémica del texto en cuanto que supone la inversión de la carga de la prueba lo cual implica subvertir todo el sistema de responsabilidad profesional. Hasta ahora, era la víctima la que debía probar la existencia del daño y el nexo causal de éste con la actuación del profesional, favoreciendo al prestador la presunción de ausencia de culpa. En consecuencia, no es tanto que se presuma la culpa, sino que debe el prestador demostrar que en su actuación no medió culpa de su parte; por ello más que aplicar los principios de la llamada responsabilidad objetiva, se trata de la consecuencia de la aplicación de la llamada "teoría del riesgo" al campo de la prestación de servicios.

Por otra parte, esta corriente no sólo afecta al prestador de servicios que actúa en régimen de autonomía e independencia, sino también a los que trabajan bajo su dependencia. Igualmente, las sociedades de profesionales quedan sometidas a este régimen en la medida de que son personas jurídicas prestadoras de servicios que se valen de sus socios y personal dependiente.

Así pues, el prestador de servicios informáticos debe responder por toda actuación en la que no actúe conforme a los dictados de las normas técnicas y deontológicas que integran el "código profesional". Su preparación, su diligencia y la vinculación con el destinatario de tal servicio serán la base para imputarle la cuota de responsabilidad que le incumbe por el resultado lesivo de su actuación. El problema es que según el tipo de actividad o servicio que se demande se tratará de una obligación de medios o de resultado, con lo que los criterios han de variar.

3- El profesional funcionario o asalariado.

No cabe la menor duda de que la actividad del profesional informático puede desarrollarse con plena autonomía e independencia y también en el seno de una estructura organizada como sociedad, empresa o funcionarial. El fenómeno de las sociedades de profesionales ha crecido de forma notable en nuestro país por cuanto es muy útil a la hora de aunar medios, conocimientos y actividades que se complementan y conjuntan, sin que ello implique una relación de dependencia entre sus miembros, salvo cuando la sociedad a su vez contrata un personal bajo su dirección. Ello no implica modificar la cuota de responsabilidad, en cuanto que la sociedad será responsable de la actuación de sus socios- profesionales, así como la personal dependiente de la misma. Téngase en cuenta que la constitución de la sociedad en ningún caso puede servir para defraudar esa obligación de responder que pesa sobre sus miembros y personal.

Más interés posee el caso del profesional que presta sus servicios en un régimen de relación laboral con un empresario o funcionarial con una Administración. Las notas de ajeneidad, dependencia y subordinación a las ordenes o directrices de la empresa, sociedad u Organismo, no puede suponer de ninguna manera un menoscabo de la independencia técnica y deontológica que el status del profesional le asegura, tutelada por la Ley en aras de respetar ese contenido esencial de su libertad profesional.

En consecuencia, cualquier conflicto que pudiera plantearse entre la directriz ordenada por el empresario, sociedad u Organismo, y las normas o reglas que regulan su actividad profesional debe ser resuelto en favor de estas. Ello quiere decir que la independencia del profesional ha de quedar siempre a salvo de injerencias inadmisibles en cuestiones sustanciales de los actos profesionales, por los que el autor de los mismos debe responder, en razón de lo cual debe ostentar la capacidad de decidirlos. Tales normas pueden ser deontológicas o de carácter técnico, pero forman el conjunto normativo rector de una actividad de servicio profesional que impone una conducta determinada al sujeto. Se trata de una obediencia limitada pues su capacidad de decisión debe quedar asegurada pues jerarquía no implica sumisión, sino mayor conocimiento y potestad de planificar o coordinar esfuerzos.

En el ámbito laboral la cuestión es aún más clara pues existe una interesante figura denominada desobediencia técnica que impide un abusivo ejercicio de la potestad de dirección del empresario. El artículo 5 del estatuto de los Trabajadores establece como un deber básico de estos el de "cumplir las órdenes e instrucciones del empresario en el ejercicio regular de sus facultades directivas". Pero ese deber de obediencia tiene unos límites: que las ordenes recibidas sean legítimas. Será ilegítima o improcedente una orden que ha sido impartida por persona no cualificada o incompetente para ello (subjetiva) o por que su contenido sea ilícito. (objetiva)

Efectivamente, toda orden ha de reunir unos requisitos formales y de contenido para ser legítima:

- Licitud moral: no debe ser contraria a la moral o ética social o buenas costumbres: son aquellas que infringen el mandato ético de una norma.

- Licitud penal: no deben constituir ni implicar un delito o falta.

- Licitud laboral: no pueden infringir los derechos del trabajador.

Ello quiere decir que cualquier orden que suponga por su contenido una consecuencia lesiva para los derechos del propio trabajador, para los derechos o bienes de terceros o para la sociedad en general, o bien suponga la comisión de un delito o falta, es considerada ilícita y, por tanto, susceptible de desobediencia. La Sala 6ª del Tribunal Supremo cuando analiza las notas esenciales del contrato de trabajo lo tipifica como una prestación personal de

servicios en un régimen de ajeneidad, retribución y dependencia pero considera esta " no como una subordinación rigurosa, sino como inserción del sujeto en el ámbito de organización y dirección del empleador". El problema es que la frontera entre el contrato de prestación de servicios y el de trabajo es muchas veces borrosa e imprecisa como el mismo Alto Tribunal reconoce.(Cfr. STS 6ª de 25/2/88 y 12/9/88)

Todo ello nos permite concluir que las reglas que rigen el actuar profesional constituyen un límite al poder de dirección del empresario que no puede invadir esa esfera de decisión que el profesional tiene reconocida como integrante de su status profesional, pues el contenido esencial de los derechos reconocidos en la Constitución forma un núcleo inabordable para ese poder.(Cfr. TCT 21/7/88) La postura de " calla y reclama" no es admisible pues si la orden implica un delito o falta o infringe una lesión a un derecho o bien protegido, el profesional debe negarse a su cumplimiento, sin que pueda alegar obediencia debida. En la práctica, ordenes que implican un perjuicio grave e irremediable, suponen vejaciones o un riesgo inaceptable, han sido consideradas como ilícitas.(Cfr.STCT 26/6/80)

En concreto, cuando dicha orden carece de fundamento técnico o es contraria a la lex artis o normas técnicas que rigen la actividad profesional, puede suponer un resultado dañoso para terceros, acarrear un menoscabo al prestigio profesional, o cualquier otra consecuencia injusta que impone una obligación de responder por su comisión. Luego si se responde por el acto, se debe estar en condiciones de decidir libremente, por lo que la autonomía técnica ha de quedar salvaguardada en todo caso.(Cfr.STS 6ª de 6/7/82)

En definitiva, una actividad sólo es profesional cuando se realiza bajo el principio de responsabilidad personal del actor, responsabilidad que sólo existe cuando éste dispone de la adecuada y necesaria libertad de actuación. Partiendo de la cualificación profesional que cabe presumir del profesional en función del titulo y puesto que desempeña podremos valorar el nivel de exigencia de conocimientos y diligencia que cabe esperar de su actuación y, en base a ello, valorar el alcance de su cuota de responsabilidad en el resultado lesivo que se haya producido como consecuencia de su actuación. Atenderemos igualmente al tipo de obligación contraída, circunstancias concretas del caso y vínculo que le liga con el afectado, sin admitir en este caso tampoco cláusulas que le exoneren de una responsabilidad que, en principio le atañe.

Todo lo anterior pone de manifiesto que la actividad del prestador de servicios informáticos es una actividad de riesgo y por ello el profesional debe asegurar la cobertura de tales riesgos merced al correspondiente contrato de seguro que contemple esos eventuales daños.[38]

IV - LA RESPONSABILIDAD DEL TITULAR DEL FICHERO AUTOMATIZADO.

1- Introducción:

Tal vez sea este el supuesto más "nebuloso" dada la ausencia de un régimen jurídico concreto que aplicar a los casos que se pueden plantear pues la legislación existente es incompleta, lo que nos obliga a tener en cuenta el régimen general apuntado en la primera parte de nuestro trabajo. De salida, no cabe distinguir entre los ficheros de titularidad pública y los privados a efectos de cubrir la responsabilidad pues, en ambos casos, existe la obligación de responder por lo daños y perjuicios de todo orden que pueden producirse como consecuencia de la actividad de riesgo que la gestión de estos ficheros implica. No cabe por tanto, consagrar una exoneración previa en favor de nadie, sino establecer unos criterios de delimitación a la hora de la atribución de responsabilidades.

El tratamiento automatizado de datos es una actividad de riesgo en la que cabe exigir unas cautelas que se acentúan en los ficheros que contienen datos sensibles. Puede haber accesos no autorizados, autorizaciones inadmisibles, desaparición de datos, errores en los mismos, cesiones inconsentidas, y otras circunstancias de las que se deduzcan daños y perjuicios para las personas afectadas. Tales consecuencias pueden ser de diversa índole pues varían según la causa que las origine: condenas penales no borradas, detenciones basadas en datos erróneos, sanciones administrativas, pérdida de bienes o derechos patrimoniales, denegación de créditos, etc... son apenas algunos ejemplos de lo que se puede producir como consecuencia de una actuación negligente del titular del fichero.

■[38] Vid. Van Houte:" El seguro de responsabilidad civil profesional de los informáticos".Rv. Informática y Derecho, nº 4 de 1994, página 445 y siguientes.

Esta actividad está sometida a una serie de principios de los que se deducen a su vez un catálogo de deberes. Tales principios podrían sintetizarse de la siguiente forma:
- Principio de respeto a los derechos de las personas consagrados en la Ley.
- Principio de responsabilidad por los riesgos y consecuencias que la actividad de tratamiento comporta.
- Principio de calidad de los datos: licitud de adquisición y finalidad, adecuación, veracidad, oportunidad, exactitud, seguridad, caducidad y secreto de estos.

Como hemos señalado, de estos principios se deducen unos deberes que atañen al titular responsable del fichero y a los sujetos que desempeñan labores con relación al mismo y de cuyo cumplimiento responde el titular.

Puede destacarse como el supuesto más interesante, a nuestro juicio, sea el de los ficheros de titularidad privada en los que la información se utiliza como un producto o servicio que se ofrece a los clientes y su actividad es más difícil de controlar pues nosotros estamos continuamente facilitando información personal. Desde el alumno que rellena el impreso de matricula y la ficha de asignatura, al cliente que solicita el crédito o la tarjeta, al huésped que facilita sus datos al hotel, todos "cedemos" información que, bien tratada, se convierte en la primera y más importante mercancía de la actualidad. Es necesario, por tanto, establecer unas condiciones básicas para el ejercicio de esta actividad de adquisición, tratamiento y cesión de datos para los ficheros, sean públicos o privados.

En todo caso, el respeto a los derechos reconocidos en la LORTAD incumbe a todos ellos, públicos y privados, pero en estos últimos es más difícil controlar el uso adecuado de los mismos. Aunque la LORTAD no establece un régimen especifico de responsabilidad civil, ya que se remite a la legislación general para esta materia en su artículo 17 como afirma DEL PESO, si podemos obtener de ella el capitulo de deberes que el titular del fichero debe observar y de cuya inobservancia se pueden deducir los daños a reparar.[39]

■[39] Vid." Confidencialidad y seguridad de la información: la LORTAD y sus implicaciones socioeconómicas".Madrid, 1994 y Carrascosa López:" La LORTAD: una necesidad en el panorama legislativo español". Rv. Informática y derecho, nº 6/7 de 1994

2- La figura del responsable o titular del fichero:

Por otra parte, la propia Ley hace referencia a la figura del responsable si bien no delimita de forma clara su concepto.[40] Inicialmente, a tenor del artículo 3.d, se trata de la persona física o jurídica, pública o privada, u órgano administrativo " que decida sobre la finalidad, contenido y uso del tratamiento". Realmente, el término adecuado hubiese sido el de titular pues se trata de aquél sujeto que posee la capacidad para decidir el tratamiento, ya sea ejecutándolo por si mismo o mediante personas a su cargo. Esta facultad de decisión implica todos los aspectos de organización del fichero, su contenido, gestión, transmisión, puesta al día, borrado de datos, etc... es el responsable del exacto cumplimiento del catálogo de deberes que impone la Ley y quien debe soportar las consecuencias de su infracción.

No obstante, esta distinción entre titular y responsable si aparece en el artículo 10 podría obedecer, a nuestro juicio, a la posibilidad de desligar al titular, autoridad u organismo en el caso de fichero público, y responsable, funcionario o técnico que está al frente de la gestión del fichero y con ello "romper" el nexo o vínculo de cobertura de responsabilidad entre el organismo(Administración) y el funcionario encargado de esas tareas. Esta posible ruptura del vínculo no se aplicaría en ningún caso en los ficheros de titularidad privada dada la postura que la jurisprudencia mantiene con respecto a la responsabilidad civil del empresario y en cuanto a los públicos será una de las más interesantes cuestiones a resolver.

En el campo de los ficheros públicos, nos estaremos refiriendo a la persona o autoridad que esta al frente del organismo titular del fichero; en el campo privado, se trata del empresario o empresa titular del mismo. Por ello el autor antes citado distingue la figura del titular-responsable de las personas que bajo su dirección, con mayor o menor autonomía, ejecutan las ordenes y directrices marcadas para el tratamiento; incluso introduce la figura del administrador de los datos, que a veces coincide con el anterior, pero

■[40] Esta figura ha sido estudiada por Del Peso Navarro en:" La figura del responsable del fichero de datos de carácter personal en la LORTAD".Rv Informática y Derecho, nº 6/7, trabajo al que nos remitimos.

necesariamente debe ser una persona física; esta figura se asemeja al responsable del tratamiento que sería aquella persona dirige técnicamente el tratamiento, pero es inadecuado llamarle responsable pues se trata de un director técnico, co-responsable si llega el caso, pues es que dirige y decide un tratamiento determinado.

Por tanto, la persona por cuya cuenta y riesgo se realiza la actividad de tratamiento del fichero, sea persona física o jurídica, es la que debe velar por el exacto cumplimiento de los imperativos éticos que la Ley consagra como deberes a cumplir en la actividad de tratamiento desarrollada en el fichero. En otro caso, responderá por los daños y perjuicios que este incumplimiento cause. Por eso puede suceder que el titular del fichero no posea conocimientos técnicos en la materia, que si son exigibles a quien dirija el tratamiento, pero si debe conocer los imperativos éticos que se han de observar en los mismos; a la par debe velar por la cualificación técnica del personal y el exacto cumplimiento, técnico y legal, de sus funciones ya que va responder de ello.

En definitiva, no cabe la creación de " categorías interpuestas " a efectos de responsabilidad entre el titular y el fichero, pues de acuerdo a lo dispuesto en nuestro Ordenamiento, el titular, empresario o Estado, responde de forma objetiva y directa por los daños que la actividad riesgo del fichero cause a las personas en sus bienes y derechos.

3- <u>Catálogo de deberes exigibles</u>:

Partiendo de los principios antes enunciados y consagrados en la LORTAD se pueden deducir unos deberes de conducta exigibles a los sujetos relacionados con el fichero y su tratamiento, según la cualificación de cada sujeto y las funciones que desempeñen en esa actividad, les serán exigibles unos u otros en mayor o menor grado. En todo caso, el titular responde por todos ellos, deberes y sujetos, según los actuales criterios de responsabilidad, salvo excepcionales casos de exoneración legalmente prevista y debidamente probada.

Tales deberes han sido sintetizados por DEL PESO de la siguiente forma:[41]

■[41] Vid. " La figura...".cit. página 258 y siguientes.

1- Deber de publicidad:

Ha de ser conocida la existencia del fichero mediante se oportuna inscripción, así como identidad y dirección la de su titular para lo cual se crea el Registro General y se notifica a la Agencia de Protección de datos.

Con ello se asegura la posibilidad de poder dirigir adecuadamente la acción de responsabilidad contra el sujeto o sujetos responsable del fichero.

2- Deber de seguridad:

Afecta al contenido del fichero para evitar pérdidas, fugas o usos indiscriminados o prohibidos por la Ley. Se trata de un deber de diligencia en la gestión y administración del fichero que se acentúa conforme la "sensibilidad" de los datos almacenados acrecienta el riesgo por su pérdida o uso indebido.(art.9.1) No se pueden registrar datos personales si no se reúnen las condiciones de seguridad necesarias en cuanto a equipos, programas, sistemas y locales que permitan impedir cualquier quiebra de este deber de seguridad.(9.2)

3- Deber de secreto:

Es uno de los más interesantes por cuanto impone una conducta silente a los sujetos que por sus relación con el fichero tienen acceso a los datos objeto de tratamiento. Este deber pesa sobre todos aquellos que intervienen en cualquier fase del tratamiento y se extiende no sólo al tiempo en que realizan estas tareas sino también con posterioridad a la finalización de su relación con el titular del fichero.(art.10) Esto implica el evitar el llamado "ruido informático" que se produciría en caso de que tales datos pudieran ser revelados o utilizados inadecuadamente por las personas que están relacionadas con el fichero según sus diversas actividades. De otro lado, el deber de lealtad, derivado de la buena fe, que liga al funcionario o empleado con el titular del fichero se mantiene incluso después de terminada la relación entre ambos de suerte que no puede revelar los datos a los que tuvo acceso por su trabajo ni, menos aún, "llevárselos" a su nueva actividad o empresa.

4- Deber de rectificación y cancelación de datos:

Estos deberes le incumplen en cuanto titular diligente del fichero pues debe proceder a cumplir este mandato, no sólo cuando así se lo exija el afectado o una autoridad competente, sino por si mismo en cuanto es un modelo de conducta que tiene que observar necesariamente pues así se lo exigen las normas que disciplinan su actividad.(art.15) Paralelamente, este deber implica el facilitar en todo momento el ejercicio de los derechos y garantías que la Ley consagra en favor de los ciudadanos para conocer y acceder a los ficheros que les conciernen.(art.14)

5- Deber de indemnización:

Es consecuencia lógica de la aplicación de los dictados que regulan la responsabilidad civil a la actividad de riesgo que el tratamiento automatizado implica.(art.17) Debe responder penal y civilmente asegurando la debida reparación de los daños y perjuicios que se puedan deducir de un incumplimiento de los deberes que la Ley impone. Según se trate de un fichero de titularidad pública o privada, la cuestión se resolverá a través de las normas correspondientes.

6- Deber de información:

Supone la puesta en conocimiento de determinadas circunstancias a los sujetos que les afectan y posee una doble faceta. En primer lugar, cuando se produzca la primera cesión de datos deberá comunicarlo al afectado ("dueño" de los datos) así como la finalidad del fichero, la naturaleza de los datos cedidos y el nombre y dirección del cesionario.(art.25.1) Cuando esté referida a ficheros sobre solvencia patrimonial y crédito este deber se acentúa pues el afectado puede solicitar que se le comuniquen los datos y las "apreciaciones" o "evaluaciones" que sobre él se hayan comunicado en los últimos seis meses y los datos de identificación del cesionario.(art.28.2)

Esta es una de las cuestiones más "espinosas" de la Ley por cuanto no suele cumplirse este deber por parte de los titulares de ficheros privados en la medida en que recaban información de la persona con una finalidad (tarjeta de crédito, por ejemplo) y, salvo que se haga constar por escrito la oposición, esos datos se transmiten o venden a otras empresas sin comunicarlo al sujeto afectado. Esta cuestión se deriva del hecho de que el artículo 11 no es demasiado claro pues aunque parece consagrar en su párrafo 1° un derecho de bloqueo al exigir el consentimiento del afectado para la cesión, las excepciones

previstas en el párrafo 2º son tan "elásticas" que en la practica lo hacen quedar bastante "capitidisminuido".

Además, la practica empresarial ha creado una suerte de "presunción de consentimiento" para la cesión pues ha de constar la oposición expresa en el documento de recogida de datos, lo cual ha sido muy criticado en cuanto que, de hacer constar el consentimiento expreso, se ha pasado a exigir la oposición expresa. Ello es fruto de la falta de previsión del Legislador pues era de prever que el deber de información no sería escrupulosamente cumplido por las empresas titulares de ficheros privados, aunque hay honrosas excepciones. Este consentimiento es esencialmente revocable, y será nulo cuando no recaiga sobre un cesionario determinado o determinable.

Mayor discrecionalidad se consagra en el artículo 19 cuando se trata de cesión entre ficheros de las Administraciones Públicas, si bien no queda demasiado bien patente la negativa de la cesión de los datos de estos ficheros a los de titularidad privada que debe considerarse prohibida, salvo consentimiento expreso del sujeto afectado.

En segundo lugar, y como consecuencia de lo anterior, el cedente viene obligado a comunicar al cesionario las rectificaciones y cancelaciones de datos que se hayan producido y que afecten a los datos cedidos. El cesionario, a su vez, queda obligado al cumplimiento de los deberes consagrados por la Ley en cuanto titular del fichero.

7- Deber de colaboración:

Implica la obligación de cumplir las directrices que los organismos competentes dicten para el desarrollo de sus actividades. En concreto quedan obligados al cumplimiento de las normas establecidas por la Agencia, proporcionarle la documentación e información que ésta recabe y permitir la función inspectora de la misma cuando así se le exija.

Es de destacar que la misma Ley prevé en su articulo 31 la posibilidad de que los titulares de estos ficheros elaboren unos códigos deontológicos que regulen las condiciones de organización, régimen de funcionamiento, procedimientos aplicables, normas de seguridad, programas, equipos, obligaciones de los implicados en el tratamiento y uso de la información y garantías, en su ámbito, para el ejercicio de los derechos consagrados por ella,

con el pleno respeto a los principios y disposiciones legales aplicables. Además, podrán contener las reglas operacionales detalladas de cada sistema y estándares técnicos de aplicación, y si no se incorporan al código directamente, las instrucciones y órdenes que los establecieran "deberán respetar los principios fijados por aquél".

Esta esfera de autonomía de coordinación ética y técnica supone la aceptación de un fenómeno positivo ya existente en otros campos de la actividad empresarial y de prestación de servicios (ej. venta por correo) y sería deseable que se potenciara la formulación de tales acuerdos o convenios. Y ello porque, en sentido estricto, se puede decir que sólo obligan a quienes los firman o se adhieren a ellos, pero no cabe la menor duda de que la jurisprudencia utilizará estos códigos deontológicos como criterios definitorios para medir el nivel de diligencia de los titulares en el desempeño de sus funciones, al igual que lo hace en otros campos de la responsabilidad civil con conceptos tales como "lex artis" o normas técnicas. Por lo tanto, no obligan, inicialmente, si no se suscriben, pero servirán como criterio para medir el nivel de cumplimiento de estos deberes en cuanto suponen la consagración del "nivel deseable" de conducta ética y diligente exigible en esa actividad. Esta posibilidad se ve reforzada por el hecho de que tales códigos pasan un previo control de calidad legal en cuanto han de ser depositados o inscritos en el Registro General de Protección de Datos pudiendo denegarse su inscripción si no se ajustan a las disposiciones legales y reglamentarias.

Así pues, cabe afirmar que de estos deberes se deducen unos requisitos por cuya concurrencia responderá el titular o responsable. Así, con referencia al fichero cabe decir que debe ser público, en el sentido técnico-jurídico del término, seguro, en cuanto reúna las condiciones técnicas que garanticen la seguridad de los datos, accesible en cuanto no sólo sea conocido sino puede llegarse a él para recibir la información precisa y ejercitar los derechos que la Ley reconoce.[42]

En relación al contenido de los datos del fichero:

■[42] Sanchez de Diego Fernandez:" La transparecia de las bases de datos como mecanismo de protección de la intimidad de las personas"; y Orzabal:" Bases de datos, privacidad y responsabilidad civil". En Rv. Informática y Derecho, nº 4 de 1994

- Licitud del titulo de adquisición de los mismos, ya sea por autorización legal o por mediar consentimiento. La Ley así lo afirma, a sensu contrario, en el artículo 4.7:" se prohibe la recogida de datos por medios fraudulentos, desleales o ilícitos".

- Veracidad y exactitud: son requisitos de calidad impuestos por la Ley en el artículo 4 pues deben ser datos puestos al día, para que respondan a la situación real de la persona. Todo dato que no responda a ello debe ser rectificado de oficio.

- Oportunidad: los datos han de ser adecuados, pertinentes y no excesivos en relación con el ámbito y la finalidad legítima para la que fueron recabados. En otro caso, el dato debe ser cancelado de oficio o a petición del interesado.[43]

En cuanto a su tratamiento no cabe admitir que se utilicen clasificaciones basadas en criterios que se presten a prácticas ilícitas. Así, cabe preguntarse si el color, hábitos sexuales, ideas políticas no son sino clasificación basadas en criterios "perversos" por si mismos pues implican una discriminación y una intromisión en la intimidad sin que necesariamente tengan que desembocar en prácticas de aquella naturaleza. No cabe por tanto, fijar un criterio aprioristico en la medida en que debemos atender a todas las circunstancias, tipos de datos, finalidad del fichero, técnicas de tratamiento, etcétera para poder decidir si se ha infringido el precepto. Ello pone de manifiesto la necesidad de esos códigos deontológicos antes comentados.

En cuanto a la cesión de estos datos es necesario que se produzca en base a un titulo lícito, sea por consentimiento o en base a una autorización legal o en situaciones que la misma Ley no exige el consentimiento. Esta doble condición de accesibilidad o consentimiento se aplica a los ficheros de publicidad, si bien cabe acceder a ellos y exigir ser dados de baja.(art.29)

En los ficheros afectos a la prestación de servicios por cuenta de terceros la Ley establece unos límites a su gestión en el artículo 27. No pueden

■[43]Vid. Montero:" Las obligaciones y responsabilidades del titular de un fichero de datos nominativos en cuanto a la cualidad de su producto". Rv. Informática y Derecho, nº 4 de 1994, página 129 y siguientes.

utilizar esos datos nada mas que para la finalidad que figure en el contrato de servicios, y no pueden cederlos a terceras personas, ni aún para su conservación. Cumplida la prestación, deben ser destruidos, salvo que su conservación sea autorizada expresamente por la persona para quien se prestan los servicios, porque se presuma razonablemente la posibilidad de ulteriores encargos. En tal caso, han de almacenarse en condiciones de seguridad por un plazo de cinco años. Incluso en los ficheros cuyos datos se realizan con fines de investigación o de encuestas es preciso el consentimiento del afectado, y en ningún caso cabe utilizar o ceder los datos para otra finalidad, de forma que puedan ser puestos en relación con una persona concreta.

Tal vez el caso más interesante sea el de las decisiones de ámbito privado que se adoptan merced a los datos relativos al crédito y solvencia patrimonial de las personas, normalmente recogidos en los "ficheros de morosos" que se anuncian como información-mercancía. El artículo 28 de la LORTAD exige que tales ficheros deben contener datos obtenidos de fuentes accesibles al público, de informaciones facilitadas por el afectado, o con su consentimiento. Cuando se trate de datos relativos al cumplimiento de las obligaciones dinerarias pueden tratarse si proceden de aquellas fuentes o del acreedor o persona que trabaje por su cuenta e interés, lo cual excluye adquisición de datos por vías fraudulentas como terceros ajenos a estas relaciones o fugas de otros ficheros o cesiones inconsentidas por los sujeto legitimados para ello. En estos casos, datos procedentes del acreedor o su representante, debe comunicarse al afectado una referencia de tales datos y se le informará de su derecho a conocerlos en su totalidad.

Incluso las evaluaciones y apreciaciones que sobre ellos se hayan realizado y comunicado en los últimos seis meses deben ponerse en conocimiento del afectado cuando lo solicite. Finalmente, sólo pueden registrarse y ceder datos que sean determinantes para enjuiciar la solvencia económica de los afectados y, cuando sean adversos, no pueden estar referidos a más de seis años. En la práctica, estos ficheros "mercantilizados" cuyo titular no es el acreedor ha creado muchos problemas pues el titular no posee competencia y conocimientos, pero si el deber, para modificar o cancelar datos incorrectos u obsoletos.[44]

■[44] Vid. Dwe Julios Campuzano:" Derecho a la intimidad y publicidad de datos personales de carácter patrimonial". En Rv Informática y Derecho, nº 4 de 1994.

Para paliar el problema se ha dictado la Instrucción de la Agencia de Protección de Datos de 1/95 de 1 de Marzo que exige en cuanto a calidad de estos datos unos requisitos:

- Existencia previa de una deuda cierta, vencida y exigible que haya resultado insatisfecha.

- Un previo requerimiento de pago al obligado.

- Que no exista un principio de prueba documental que contradiga alguno de los anteriores. En tal caso no puede incluirse el dato en el fichero y, si ya lo está, ha de procederse a una desaparición cautelar.

Es obligación legal que pesa sobre el acreedor o su representante el cerciorarse de la concurrencia de estos requisitos antes de notificar el dato al fichero común. Así mismo, estos sujetos vienen obligados a comunicar la inexactitud o inexistencia del dato para su modificación o cancelación en el plazo máximo de una semana. Este deber pesa igualmente sobre el fichero común y el propio del acreedor o persona que por él actúa. Cuando la incorporación se haya producido con anterioridad a la entrada en vigor de la LORTAD se regirá por la Norma segunda de la Instrucción que impone el deber de diligencia al responsable del fichero para que adopte las medidas técnicas y organizativas que aseguren la comunicación de tal extremo en el menor tiempo posible y, en todo caso, en un año a contar desde la entrada en vigor de esa instrucción.

Los sistemas que almacenen este tipo de informaciones han de contar con los medios y medidas de seguridad adecuados, lo cual se comprobará mediante la oportuna auditoría prevista en la Norma cuarta del mismo texto.

En definitiva, se trata de un normativa que extrema las cautelas en relación con un tipo de actividad que se ha acrecentado enormemente y cuya falta de regulación expresa estaba originado serias quiebras de los más elementales principios jurídicos y conculcando los derechos de los ciudadanos. Como afirma RAMOS deben establecerse los controles y procedimientos adecuados para lograr que cada usuario sólo accede a lo que esté autorizado, para lo que esté autorizado

y cuando esté autorizado.[45] Esta autorización sólo procede cuando el usuario sea una persona legitimada para acceder al conocimiento y disposición de los datos, pues toda autorización del titular del fichero ha de corresponderse con una previa legitimación del solicitante entendido como un interés legítimo jurídicamente relevante que le faculte para pretender el acceso al conocimiento o tratamiento del contenido del fichero que solicita.

4- Reglas de Responsabilidad Civil.

Haciendo abstracción de las actuaciones disciplinarias y sancionadoras, la LORTAD no es demasiado rigurosa a la hora de establecer este régimen de responsabilidad civil. Lo único que hace en su artículo 17 es consagrar el derecho a la indemnización por incumplimiento de la Ley y fijar los criterios de jurisdicción adecuada según el régimen del fichero, estableciendo una competencia específica para la Agencia de Protección de Datos para reclamar ante ella por las actuaciones contrarias a lo dispuesto en la Ley. [46] Ello es así por cuanto se remite a las normas generales en base a los cuales incumbe esta responsabilidad al titular responsable del fichero salvo que pruebe la concurrencia de una causa de exoneración legalmente admisible. De salida, pues, deberá responder la Administración, en el caso de ficheros de titularidad pública, y el empresario-titular en el caso de los ficheros privados.[47]

Pasamos ahora a establecer cuales son los criterios por los que se rige la responsabilidad del titular de estas ficheros partiendo de la base de la obligación de responder por hechos ajenos, pues ésta es la que más se ha de aplicar al caso. Esta surge cuando la acción ha sido realizada por un a persona que

■[45] Vid. " La Seguridad y la Confidencialidad de la información y la LORTAD". Rv. Informática y Derecho, nº 6/7 de 1994, pag.133 y siguientes.

■[46] Sobre el tema véase Heredero Higueras:" La Agencia de Protección de Datos" y Castillo Jiménez:" Estatuto de la Agencia de Protección de Datos". Ambos en Rv. Informática y Derecho, nº 6/7 de 1994

■[47] Véase la crítica al sistema de la LORTAD de López-Muñiz Goñi en " La Ley de Regulación del Tratamiento Automatizado de Datos de Carácter Personal"; en cuanto al tema penal véase Romeo Casabona:" Infracciones administrativas y penales en relación con la protección de datos". Ambos en Rv. Informática y Derecho, nº 6/7 de 1994

no es el propio titular paro que mantiene con éste una vinculación a la que la Ley le confiere la consecuencia de tener que responder por él. Tal es el caso de padres y tutores, centros docentes y empresarios. Así lo impone el artículo 1903 CC: son personas por quienes se debe responder. Se basan estos supuestos en la idea de estimar que el sujeto ha incurrido en culpa in vigilando por no haberlo controlado diligentemente, o en culpa in eligiendo por no haberle seleccionado de forma idónea. No obstante, esta diligencia cesa cuando el sujeto demuestra haber aplicado toda la diligencia posible que quepa exigir en el supuesto concreto.

No obstante, esta responsabilidad ha adquirido tonos cada vez mas objetivos por lo que se entiende que la obligación de reparar vincula ya directamente al responsable con la víctima y pocas veces queda exonerado.

A) La Responsabilidad en los ficheros de titularidad pública:

Como la propia LORTAD establece esta responsabilidad se rige por las normas de la Responsabilidad civil del Estado que vienen disciplinadas sobre la base del artículo 106.2 de la Constitución:" Los particulares, en los términos establecidos por la Ley, tendrán derecho a ser indemnizados por toda lesión que sufran en sus bienes y derechos, salvo en los casos de fuerza mayor, siempre que la lesión sea consecuencia del funcionamiento de los servicios públicos". Derogado el extraño párrafo 5° del artículo 1903 CC "..cuando obra por medio de un agente especial ..." por la Ley de 7/1/91, la norma básica es la Ley 30/92 de 26 de Noviembre Régimen Jurídico de la Administración del Estado y Procedimiento Administrativo común y el Reglamento sobre Responsabilidad Patrimonial de la Administración de 26 de Marzo de 1993.

En base a estas normas, cabe afirmar que la obligación de indemnizar que recae sobre el Estado es objetiva y directa, a consecuencia del normal o anormal funcionamiento de un servicio público. Es decir, objetiva en cuanto no se toma en consideración la posible culpabilidad del funcionario actuante, pero si el nexo entre la actividad por cuenta de la Administración que éste desempeña y el daño causado, que se rompe cuando concurre la fuerza mayor. Es directa en la medida en que no existe mediatez o subsidiariedad con respecto al funcionario: el perjudicado se dirige contra el Estado al ejercitar la acción de resarcimiento. Cuestión diferente es que el Estado pueda repetir después contra el funcionario por esta causa. Se trata de relaciones de Derecho Público, donde el estado actúa con imperium en un plano de desigualdad y desempeñando las funciones y servicios que le competen pero sucede que ha

habido un funcionamiento normal o anormal del servicio público que origina un daño al particular. En tales casos responde directamente y se actúa en la jurisdicción contencioso administrativa.

Cuando la Administración actúa en relaciones de Derecho Privado responde de forma directa ante los particulares por los daños que causen sus funcionarios a los particulares, pero no es por el funcionamiento de un servicio público, sino porque actúa en una relación de Derecho privado. Se entiende que los actos de tal naturaleza que realice el personal al servicio de las Administraciones son actos propios de las mismas. Así, cuando actúa como un empresario privado, se le aplica el régimen general previsto para estos en la legislación civil y las acciones se plantean ante la jurisdicción civil.(Cfr.STS 30/1/90 y 27/3/92)

En consecuencia, cuando el daño se produzca como consecuencia del funcionamiento, normal o anormal, del fichero automatizado, sea en relaciones de naturaleza pública o privada, el Estado responderá directamente por el acto lesivo causado por el personal que presta su servicio en dicho fichero, en aplicación de las normas y principios antes citados. No cabe, por tanto, crear un status intermedio entre titular y responsable del tratamiento a estos efectos pues, en todo caso, el órgano titular del fichero viene obligado a responder frente al particular que ha sufrido el daño.

B) La responsabilidad en los ficheros de titularidad privada:

Ya hemos comentado anteriormente que la figura del titular o responsable del fichero hace referencia a la persona, física o jurídica, que ostenta la titularidad del conjunto de medios humanos y materiales que conforman ese fichero automatizado. En principio, pues, estamos ante el empresario: el dirige y decide la gestión y tratamiento de los datos que contiene el fichero, es decir, realiza una actividad empresarial de tratamiento automatizado de datos. Para ello puede actuar directamente o valiéndose de un personal dependiente que actúa con mayor o menor autonomía, pero en cualquier caso él es quien elige el personal, aporta los medios y ostenta, en última instancia, la facultad de decidir y dirigir el tratamiento y obtener los rendimientos económicos que se deduzcan. Es su deber elegir y controlar adecuadamente al personal que presta su servicio en el fichero y, en consecuencia, será responsable de los daños que se ocasiones cuando se incumplen los deberes que la Ley establece.

El régimen jurídico de aplicable a esta responsabilidad tiene su eje central en el artículo 1903.4°CC a tenor del cual son responsables " los dueños o directores de un establecimiento o empresa respecto a los perjuicios causados por sus dependientes en el servicio de los ramos en que los tuvieran empleados, o con ocasión de sus funciones". Al margen de su terminología más o menos obsoleta, lo cierto es que este precepto ha servido para fijar las condiciones de la responsabilidad del empresario. De esta norma, cabe deducir que la responsabilidad del titular de la empresa que explota el fichero es directa y solidaria con el propio empleado. A veces, el director y el empresario coinciden en la misma persona, pero en otras ocasiones el director no es el titular del mismo, en cuyo caso hay una responsabilidad solidaria de ambos.

El criterio que se ha utilizado para fijar este carácter objetivo es que se trata de una culpa in vigilando, cuando no se ha controlado adecuadamente la actuación del empleado, o in eligiendo, supuesto en el que no se eligió adecuadamente al sujeto. En ambos casos, más que presumir negligencia, se trata de asegurar un resarcimiento a la víctima de la acción que origina el daño, para lo cual se utiliza como base la subordinación del empleado a la potestad de dirección del empresario: o no se controló la adecuada ejecución de las ordenes empresariales, o estas fueron inadecuadas.

Para ello cabe exigir que la acción sea culpable en los términos objetivos antes comentados y que sea consecuencia de la actuación del empleado con ocasión del desempeño de sus funciones en la empresa, lo cual excluye los supuestos de actividades particulares del empleado ajenas a la empresa. Por ejemplo, si el técnico del fichero extrae información sensible la divulga o cede sin conocimiento del empresario, incumple su deber de secreto, pero el empresario, a su vez, incurre en la inobservancia de su deber de seguridad.

A tenor del artículo 1904 CC el empresario podrá repetir posteriormente aquello que haya debido pagar como consecuencia de la acción lesiva cometida por el empleado.

La jurisdicción competente para este supuesto es la de los Tribunales ordinarios pues estamos en el campo de las relaciones de Derecho privado.

5- El daño y su resarcimiento:

La tipología de los daños y perjuicios que un incumplimiento de los deberes antes citados puede ocasionar es muy varia pues su valoración dependerá de diversos factores. De salida hemos de decir que caben dos tipos esencialmente: daño moral y daño patrimonial, a la vez que podemos excluir el daño físico como consecuencia directa aunque no indirecta, es decir, un error de contenido en los datos de un enfermo pueden llevar a un diagnostica desacertado y a una intervención quirúrgica inadecuada que, por ejemplo, ampute un miembro sano, lo cual sería un daño físico indirectamente causado por el incumplimiento del deber de veracidad y exactitud.

El daño moral básicamente se produce cuando se incumplen los deberes que impiden almacenar o transmitir datos sensibles o cuando su tratamiento se basa en criterios que dan lugar a prácticas ilícitas. Es decir, cuando se producen casos de intromisión en la privacidad, se recaban o ceden datos sin consentimiento, en los casos en que se produce un atentado contra el honor de la persona por la "fuga" de datos sensibles, al incumplirse el deber de secreto el de seguridad, o erróneos, cuando se adoptan decisiones o actos administrativos en base al perfil informático de una persona o a un dato erróneo u obsoleto, o se impide el pacifico ejercicio de los derechos reconocidos en la misma Ley.

Pero no todo incumplimiento de estos deberes produce un daño efectivo: así, si no se borra de oficio un dato obsoleto no habrá un daño si no se cede o se utiliza como criterio de alguna decisión o acto incorrecto que perjudique al afectado; si el dato se debió borrar por anticuado e inútil hay responsabilidad frente a la autoridad competente, pero si no sirve de base a un acto lesivo, no cabe reclamar pues la concurrencia efectiva del daño y su relación de causalidad deben ser probados por quien reclama. Es decir, la falta del requisito de calidad de los datos debe medirse como criterio de atribución de responsabilidad en la medida en que sea la causa del acto lesivo, no cuando su incumplimiento sea cierto pero irrelevante pues el daño o perjuicio debe ser efectivo y probado.

En cuanto a los daños patrimoniales, básicamente cabe que se produzcan por la pérdida o fuga de datos relevantes y necesarios de cuya custodia responde el titular del fichero y de ello se deduzca el evento lesivo. Así, la pérdida de los datos relativos a cuentas bancarias, carteras de clientes, de pedidos o de cualquier otra información que produzca un daño efectivo o la pérdida de una

ventaja para el sujeto "dueño" de los datos. La fuga puede implicar que un tercero entre en conocimiento de los datos y con ello infrinja el daño: adquiere información sobre aspectos internos de un competidor que le permiten competir desde una posición de ventaja deslealmente adquirida. En este caso, además del deber de seguridad, el deber de secreto se vuelve muy relevante.

Pero el titular del fichero no sólo responde ante el "dueño" de los datos incorporados al fichero, sino, por vía contractual y extracontractual, con el adquirente y cesionario de la información. Este puede adoptar unas decisiones inadecuadas en base a datos erróneos u obsoletos, en tal caso el titular-cedente será responsable frente a él por los daños y perjuicios que ello le irrogue. Incluso si el cesionario, a su vez, incurre en responsabilidad por tales datos que le han sido cedidos por el primer fichero, deberemos valorar si el titular-cesionario incumplió también sus deberes de diligencia o le era imposible constatar la falta de calidad del dato pues ello incumbía al cedente.

El problema, una vez más, será probar el daño y su relación con el incumplimiento del titular del fichero, sobre todo a la hora de alegar posibles perjuicios más que daños reales y efectivos. Y ello en un campo, sobre todo en el mercado de bienes y servicios, donde un error de evaluación puede originar graves consecuencias. Un dato erróneo sobre la solvencia de un banco o empresa puede provocar la caída de su cotización en la Bolsa, o la pérdida de depósitos o clientes. La negativa a la concesión de un crédito en base a un índice de solvencia equivocado puede producir la pérdida de una cuenta importante. En tos estos casos esa "ganancia o ventaja futura" frustrada será difícil de demostrar.

En cuanto al resarcimiento, si es un daño moral se impone, como primera media cancelar o modificar el dato y, si procede, el pago de una indemnización económica e, incluso, cabría plantearse una publicidad de ello si el dato se hubiera hecho público y fuere falso o inexacto. En los caso de daño patrimonial, procederemos a evaluar la cuantía del mismo y los posible perjuicios mediante los medios de prueba admitidos en Derecho.

La Sociedad de la Información: Oportunidades y Riesgos.

Mª EUGENIA GAYO

Profesora Titular de la Facultad de Derecho. UNED

El fenómeno de las tecnologías de la información, emergente con especial intensidad en las ultimas décadas, ha planteado un gran número de cuestiones que han sido objeto de análisis desde perspectivas diversas (legales, éticas, económicas, sociales, etc). Es obvio que, como toda nueva situación, también ha dado lugar a diferentes posturas que, desde ópticas distintas, intentan poner de manifiesto los aspectos, tanto positivos como negativos que se pueden producir, si bien es cierto que, como consecuencia del *miedo a lo desconocido*, son más las actitudes de crítica (e incluso, en algunos casos de rechazo), que las que ensalzan los beneficios que se pueden alcanzar.

A lo largo de las siguientes páginas vamos a intentar analizar y valorar las posibles ventajas, y también los riesgos que pueden producirse en lo que se ha llamado *" la Sociedad de la información "*; partiendo, en cualquier caso, de la premisa de que los avances tecnológicos que dan nombre a la nueva sociedad, no son valiosos o perjudiciales per se, sino que lo que puede permitirnos calificarlos como tal es, principalmente, el uso o utilización que de ellos se realice, así como los fines que con ellos se pretendan alcanzar. Este planteamiento nos va a situar en un ámbito cercano a la ética, por cuanto lo que en algunos casos vamos a cuestionar es la posible mutación de valores, principios, hábitos que se puede producir, así como los límites que desde distintos planos parece necesario establecer.

Asimismo cabe resaltar que, con relación al tema que nos ocupa, sucede algo parecido a lo que viene ocurriendo en otros campos científicos o técnicos con el descubrimiento y desarrollo de técnicas y terapias diversas. Y la actitud o respuesta que cabe adoptar también parece que habrá de ser la misma. Parece claro, por ejemplo, que los avances en el ámbito de la llamada *ingeniería genética* han permitido la realización de operaciones hasta hace poco tiempo impensables, y casi nadie (salvo quienes adoptan posturas fuertemente dogmáticas y en algunos casos impregnadas de connotaciones de corte religioso) pone en discusión lo beneficioso de estas nuevas terapias para la investigación, prevención o curación de ciertas enfermedades, aunque también existan riesgos derivados no sólo de su reciente implantación sino, principalmente, de su utilización para fines no aceptados socialmente [1].

Lo mismo, en cierta medida, parece ocurrir en el campo de las nuevas tecnologías de la información, donde casi diariamente comprobamos cómo están cambiando nuestra vida y, además, en todos sus sentidos. ¿ Qué actitud conviene que adoptemos ante ello ? De un lado parece sensato considerar como beneficioso la existencia de medios como, por ejemplo, INTERNET, que nos permite no sólo estar informados, sino que además nos proporciona una información cada vez más amplia, completa y accesible para un sinfín de sujetos. Sin embargo, esta actitud puede resultar excesivamente optimista, por cuanto no analiza los problemas que puede producir una masificación de la información, una generalización indiscriminada de la misma, etc.

Hemos de tener presente que la formación de las personas depende no sólo de que cada vez se conozcan más cosas, sino principalmente de la asimilación que realicen de dichos conocimientos y de los fines que con ellos se pretenda alcanzar. Es decir, no basta con una *cultura informativa*, que afecta al ámbito estricto del conocimiento y basada primordialmente en una información de carácter descriptivo, sino que debemos pretender también el desarrollo de una *cultura valorativa* que afecta en gran medida al ámbito del comportamiento y que, por tanto, concierne a hábitos, creencias, principios, valores, etc [2], que cambian muy lentamente en relación con los hechos o datos que los sustentan.

■[1] Es conocido el rechazo social, e incluso científico, que suscita el hecho de que una utilización indiscriminada de estas técnicas pudiera dar lugar a fenómenos como la clonación humana, la selección de raza, etc. De ahí los esfuerzos por establecer un código deontológico para estas actividades.

■[2] BILBENY, N: La revolución en la ética. Ed. Anagrama. Colección Argumentos. Barcelona, 1997. Págs 35 y siguientes.

Junto a lo anterior, también hemos de considerar que en las modernas *sociedades digitales*, en muchas ocasiones las cosas no son como son sino como nos las presentan o cuentan, y ello también puede, en gran medida, condicionar nuestro sistemas de valores, hábitos y creencias. Es decir, de qué modo o mediante qué medio se nos trasmita la información determinará la idea que nos hagamos de la realidad y cómo la percibamos. Así, hasta la irrupción de la era audiovisual, la información (obtenida principalmente a través de medios impresos) permitía al sujeto imaginar cómo serían realmente ciertos objetos o cómo habrían sucedido determinados acontecimientos aun a riesgo de errar en la percepción (quien no ha reproducido mentalmente las distintas escenas que leía en una novela o imaginado cómo sería el rostro de la persona que le hablaba a través de la radio). En las actuales sociedades, donde los medios audiovisuales parecen imponerse frente a otros, el margen para la imaginación se reduce considerablemente, en cuanto que casi todo se plasma en imágenes tan reales como casi perceptibles, y ello con el riesgo de saturar nuestra sensibilidad o incluso llevarnos a un estado de indiferencia, puesto que ya casi nada resulta sorprendente.

Anteriormente señalábamos que la denominada *cultura valorativa* concierne principalmente a hábitos (aunque también a creencias, principios, valores, etc.), lo que nos obliga a analizar, aunque sea brevemente, cómo surgen éstos. Si partimos de la consideración del hábito como " el modo especial de proceder o conducirse adquirido por la repetición de actos iguales o semejantes "[3], podemos considerar que su existencia se encuentra fuertemente vinculada con el aprendizaje, lo que no necesariamente permite atribuirles un carácter puramente mecánico, sino que, debido a que los hombres se caracterizan principalmente por la racionalidad, utilizan los hábitos de forma dinámica y abierta, es decir, manteniendo los que interesen y desestimando los que, por distintas circunstancias, en un determinado momento pudieran carecer de sentido. En cualquier caso, esta consideración de los hábitos implica que se pueden ver sometidos a un proceso de transformación si se modifica los pilares sobre los que se sustentan. Así, se ha señalado que " cuando cambian las condiciones de nuestro hábitat no pueden por menos que cambiar los hábitos personales y con ellos las creencias o ideas que crecen a su lado para justificarlos "[4].

■[3] RAE: Diccionario de la Lengua Española. 21° Ed. Madrid, 1992.

■[4] BILBENY, N: ob. cit.Pág.43.

Y es obvio que la irrupción de la cultura digital está provocando cambios en el modo de proceder no sólo del individuo sino del propio grupo social, que ha comenzado a seleccionar nuevos valores o principios que sustenten los actuales hábitos. Por tanto, parece que en el momento actual ya no se trata de seleccionar valores o principios absolutos, ni siquiera permanentes, sino que se tiende a establecer unas escalas de valores que puedan ir ajustándose a este nuevo orden de vida inestable ante el que nos encontramos. Esto explicaría la justificación de comportamientos que durante siglos han resultado rechazables, o incluso la demanda de sujetos con una mayor capacidad de adaptación a las nuevas situaciones y no dependientes de criterios en desuso u olvidados. Podemos analizarlo ejemplificativamente: en el momento actual, desde ciertos sectores sociales y económicos se pone de manifiesto cada vez en mayor medida la tendencia a desarrollar el denominado *teletrabajo*, modalidad laboral consistente en realizar la prestación en el propio domicilio, o al menos sin la necesidad de desplazarse a un mismo entorno de trabajo. Obviamente no todos los sujetos van a tener la misma capacidad de adaptación ante esta situación, sino que, probablemente, sólo lo conseguirán los más versátiles. Pero incluso sería discutible, o al menos cabría preguntarse, ¿ por qué ha de aceptarse esta nueva modalidad como buena o válida ? Si prescindimos de consideraciones de carácter económico, un planteamiento como el descrito va a producir profundos cambios en el ámbito de las relaciones interpersonales, pudiéndose incluso llegar a desvirtuar el propio proceso de socialización humana [5].

El panorama se ensombrece aún más si pensamos que las nuevas tecnologías también nos ofrecen la posibilidad de ocupar los momentos de ocio en soledad, al permitirnos *"practicar"* deportes, juegos, etc., sin necesidad de desplazarnos a ningún lugar. Dejando a un lado lo que esta actividad tiene de *"fraude físico"*, por cuanto al no estar realmente jugando no se ejercita físicamente el cuerpo, en estas situaciones resulta imposible detectar en los restantes participantes, si los hubiera, la más mínima señal de duda, emoción, fragilidad, etc., que en la práctica real podría conducir a un cambio en la estrategia y por ende del resultado. Todo ello contribuye a que se produzca una pérdida de contacto real con otros sujetos que puede provocar la aparición de conductas o comportamientos, los cuales en muchos casos, al no estar

■ [5] Pensemos que la socialización del hombre comienza cuando sale del entorno personal y familiar más cercano para encontrarse y relacionarse con otros sujetos, y este proceso que comienza en la infancia continúa a lo largo de toda la existencia del sujeto.

que se produzca una pérdida de contacto real con otros sujetos que puede provocar la aparición de conductas o comportamientos, los cuales en muchos casos, al no estar basados en una real interacción y amparándose en el *"anonimato tecnológico"* podrían resultar no deseables.

Asimismo, anteriormente señalábamos que, aunque es posible que se produzcan mutaciones en los hábitos y creencias y, por tanto, que evolucione la *cultura valorativa*, la producción de estos cambios no se realiza al mismo ritmo que las evoluciones tecnológico-sociales. Y ello principalmente debido a, entre otras, las siguientes razones:

1º/ Porque los sujetos se encuentran ante una ininterrumpida y vertiginosa sucesión de cambios, en gran medida imprevisibles, de tal forma que lo único que llegan a intuir es la necesidad de cambiar sus comportamientos, pero sin conocer de qué forma o en qué dirección.

2º/ Porque carecen de un referente o modelo, es decir, no existen pautas que les guíen, ya que la mayoría de los sujetos se limitan a asumir la nueva situación y ajustarse a ella en la medida de lo posible, sin disponer de tiempo suficiente ante el cúmulo de información que recibe para depurarla, analizarla, discutirla y valorarla.

Quizás por todo ello, en las sociedades tecnológicamente avanzadas, los modernos comportamientos carecen de un cierto arraigo, lo que afecta a (y puede llegar a imposibilitar) la identificación de una sociedad sobre la base de dichos hábitos, por cuanto casi ni lo son. Este planteamiento nos conduce a una cuestión problemática: la consideración del concepto de identidad en una sociedad como la actual dominada por el desarrollo y expansión de la revolución tecnológica. Incluso en estas circunstancias, cabría preguntarse si es posible adquirir y mantener una identidad tanto individual como social.

Tradicionalmente, la identidad individual o personal se construía sobre un rol (hereditario o adquirido), un rango o un estatus. Esta forma de entender la identidad queda desvirtuada en una sociedad digital como la actual donde lo que se exige es, precisamente que el sujeto se acomode a distintas posiciones, situaciones, es decir, una sociedad en la que cabe hablar de " roles mutantes " [6]; lo que permite pensar

■[6] BILBENY, N: ob.cit.Pág.16.

que se trataría, más que de una identidad en parte creada por el propio sujeto, de una identidad generada o, cuando menos, atribuida o asignada por la propia sociedad digital, con la inseguridad que esto puede generar por la capacidad de manipulación. Por ello resulta paradójico que, en los últimos años, la literatura iusfilosófica principalmente se haya ocupado con gran intensidad de los problemas que las nuevas tecnologías podrían provocar en el ámbito del derecho a la intimidad, resaltando la necesidad de establecer unos mecanismos de protección y garantía (Habeas Data, Leyes de Protección de Datos)[7] sin tomar apenas en consideración el problema que afecta al concepto de identidad, ya que dependiendo de quién o cómo soy (identidad), así se desarrollará mi privacidad.

En cuanto al ámbito de la identidad social y cultural, hasta el momento presente, la individualización de una determinada sociedad se ha venido realizando tomando en consideración una serie de datos que contribuían a determinar su personalidad, que le conferían su propia idiosincrasia y que generalmente no eran compartidos, al menos de forma total, por otras estructuras sociales, como podrían ser, entre otros: sus manifestaciones espontáneas, su lenguaje, sus tradiciones, su cultura, etc. Con la irrupción de la sociedad audiovisual las diferencias entre unas sociedades y otras comienza a debilitarse, y con la expansión de las nuevas tecnologías informáticas y la generalización de las informaciones, resulta cada día más difícil evitar una cierta uniformización de las sociedades.

En definitiva, con respecto a la cuestión de la identidad (ya sea individual, cultural o social), actualmente podemos afirmar que, en gran medida, se

■7 Son numerosos los autores de la doctrina española que han resaltado en sus obras la necesidad de conjugar el régimen jurídico de los derechos fundamentales del hombre, y más concretamente el derecho a la intimidad, con la utilización de las nuevas tecnologías en las modernas sociedades informatizadas. Vid. PEREZ LUÑO, A.E." Nuevas tecnologías, sociedad y Derecho. El impacto socio-jurídico de las N.T. de la información ", Ed. FUNDESCO. Madrid, 1987.Id. " Los Derechos Humanos en la sociedad tecnológica ", en Cuadernos y Debates nº 21, Centro de Estudios Constitucionales. Madrid, 1989. Págs. 139 y sg. Id.: " Los derechos humanos en la sociedad tecnológica ",publicado en Cuadernos y Debates nº 21. Centro de Estudios Constitucionales. Madrid, 1989. GARCIA SAN MIGUEL, L (ED); PEREZ LUÑO,A.E. y OTROS:" Estudios sobre el derecho a la intimidad ". Universidad de Alcalá de Henares. Editorial Tecnos. Madrid, 1992. GAYO SANTA CECILIA, Mª.E: " Garantías del ciudadano ante la LORTAD: posibles vías de defensa y protección de sus derechos fundamentales ", en Actas del III Congreso Iberoamericano de Informática y Derecho (Vol.I) publicadas en Informática y Derecho, nº 4. Ed.UNED.Centro Regional de Extremadura y Aranzadi Editorial, Mérida, 1994.

encuentra mediatizada, o incluso manipulada, por quien o quienes manejan y transmiten la información, por lo que podríamos llamar el *poder telemático.*

Todo lo anteriormente expuesto nos conduce a analizar, y en parte rechazar, otro de los *"mitos"* que se ha creado en relación con las nuevas tecnologías de la información, como es el del control que puede ejercerse sobre las informaciones que se reciben a través de los nuevos medios y quién lo ejerce realmente. Es cierto que el usuario de las modernas *autopistas de la información* controla hasta cierto punto las informaciones a las que accede al poder seleccionar, por ejemplo, qué páginas visitar y cuáles no; sin embargo su capacidad de control no puede remontarse sobre las fuentes u orígenes de dichas informaciones, ni siquiera en relación con su forma de obtención, lo que en cierta medida le obliga a guiarse en parte por su instinto para intentar depurar la información recibida, lo que no deja de resultar curioso en un mundo digital tan tecnificado. Por otra parte, el usuario sí puede estar siendo controlado o seguido en sus actuaciones (en el momento actual la tecnología existente permite averiguar cuándo se produce la conexión a la red, en relación con qué temas, a través de qué rutas, etc), lo que de alguna forma permite conocer su perfil. No se trata del clásico problema de averiguar quién es el sujeto a través de su datos personales, sino de elaborar un perfil, inicialmente anónimo, pero que en un determinado momento puede dejar de serlo. Todo ello puede producir la necesidad de cambiar determinados conceptos y esquemas, tanto de carácter jurídico como ético.

También cabría señalar que, históricamente, ética y derecho han coexistido como fundamento del obrar del hombre porque se desarrollaban sobre sociedades que presentaban ciertos hábitos o creencias estables y en algunos casos prácticamente inmutables. En el mundo digital actual, donde la inestabilidad de informaciones, conductas, principios, valores parece una constante, existen serias dificultades para establecer esquemas normativos, tanto de carácter ético como jurídico y, de lograrse su implantación, podrían mantenerse serias dudas acerca de su eficacia.

Como conclusiones a lo expuesto, podríamos señalar que la revolución tecnológica ofrece insospechadas posibilidades de comunicación y producción tanto en el orden personal como en el social, por lo que parece razonable aceptar su desarrollo, lo que no obsta para que tengamos presente algunos aspectos no demasiado beneficiosos que también han de producirse con su implantación.

En este sentido, uno de los principales aspectos menos benéficos sería el que la revolución tecnológica está en gran medida condicionando - e incluso anulando - no sólo el mundo de los sentidos sino, incluso, el de los sentimientos, con

la consiguiente pérdida de sensibilidad. No olvidemos que no resulta lo mismo hablar directamente ante un auditorio que a través de una conexión informática o mediante videoconferencia, puesto que, aunque el mensaje sea el mismo, la forma de transmitirlo necesariamente cambia, lo que deviene en que la recepción pueda no ser unívoca o ser incluso equívoca.

Asimismo, la generalización y uniformización de hábitos y comportamientos podría hacer necesario el intentar universalizar los esquemas normativos, tanto de carácter ético como jurídicos, si bien su eficacia podría ser muy escasa al construirse sobre hábitos y creencias en permanente cambio.

Protección de Datos Personales en Ficheros de Titularidad Pública

EUGENIO ULL PONT

Profesor Titular U.N.E.D.

El artículo 18.4 de la Constitución española de 1978 establece que "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"

Ese es necesariamente nuestro punto de arranque para considerar si tal protección se cumple, o no se cumple, o se cumple mal, respecto a la automatización de la información sobre datos personales y/o familiares, y sobre la utilización de los datos informatizados, por parte de los poderes públicos.

En consecuencia, consideraremos primero el soporte constitucional de la protección y el alcance de dicha protección, para después considerar la protección establecida en la Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal, particularmente, en lo que se refiere a las Administraciones Públicas, y la protección de los derechos personales frente a los ficheros de titularidad pública.

No es objeto de nuestra exposición actual, el tratamiento automatizado de datos personales respecto a los ficheros de titularidad privada.

1. Alcance protector del art. 18.4

La Constitución establece un derecho de protección frente al uso de la informática, y por su propia ubicación en el texto constitucional, constituye un derecho fundamental específicamente protegido.

El contenido de ese derecho o libertad es concretado particularmente referido al derecho al honor, personal y familiar y a la intimidad personal y familiar, de los ciudadanos (no de las personas jurídicas), respecto al tratamiento de datos personales por medios automatizados. Supone una garantía específica de tales derechos, que son reconocidos como tales en el mismo art. 18.1 de la C.E.

La insistencia constitucional para la protección de esté derecho, se manifiesta también en el enunciado del art. 20.4 de la C.E., que pone limites a la libertad de expresión y de información, también derechos fundamentales, al establecer que "estas libertades tienen su limite en el respeto a los derechos reconocidos en este Titulo, en los preceptos de las leyes que lo desarrollen, y, especialmente, en el derecho al honor, a la intimidad, a la propia imagen, y a la protección de la juventud y de la infancia." (Tit. I, que se enuncia como "De los derechos y deberes fundamentales", comprende los arts. 10 a 55 de la C.E.; vid también L.O. 1/1982, de 5 de mayo, de protección civil del honor, la intimidad y la propia imagen, y su protección por L.O. 311 985).

El alcance de la protección del art. 18.4 de la C.E. se entiende también referido al pleno ejercicio de sus derechos. Es decir, libertad para ejercer cualesquiera derechos reconocidos en el art. 18 y en otros artículos de la Constitución, sean calificados como fundamentales o con otro rango de protección.

Es pues un derecho fundamental de libertad, para ejercer cualquier derecho, frente a los obstáculos o intrusiones que puedan producirse con la utilización de la información automática (vid Sentencia del TC. de 20 de julio de 1993, recogida en la pág 11 y ss. de nuestro manual "Introducción al D. Informático I"). Se trata pues, de un derecho fundamental del ciudadano, consistente en la libertad de ejercicio de todos los derechos, frente a la informática.

2. Garantías de los derechos y libertades fundamentales.

El ejercicio de las libertades y derechos fundamentales puede verse impedido o limitado, máxime cuando la Constitución se remite a una Ley reguladora. Veamos la eficacia del derecho proclamado, en dos supuestos. Uno, cuando la remisión a una ley, nos lleva a un vacío legislativo o ausencia de ley reguladora. Otro, cuando habiendo una ley, esta es restrictiva, y reduce o anula el ejercicio del derecho regulado.

En el supuesto de no haber una ley reguladora, conforme al art. 53.1 de la C.E. los derechos y libertades reconocidos en el Capítulo II del Título I (arts. 14 al 38), "vinculan a todos los poderes públicos". Es decir que en sus actuaciones, los distintos poderes no pueden ignorar el contenido de tales derechos, hayan sido, o no, regulados por ley. Es decir es derecho de aplicación directa, pues conforme a la jurisprudencia constitucional (vid. Sentencia del T.C. 75/1982, y también S.T.C. 39/1983), el incumplimiento por el legislador de la obligación legislativa impuesta por la Constitución, no puede ser causa de lesión de los derechos que la misma reconoce.

En el mismo punto 53.1 se dice que solo por ley podrá regularse el contenido de tales derechos, se advierte que la ley "en todo caso deberá respetar su contenido esencial". Incorpora además una protección por inconstitucionalidad (vid art. 161.1.a).

Así que la ley debe respetar su contenido esencial para ser constitucionalmente válida. Sin embargo, la limitación de legitimación para interponer recurso de inconstitucionalidad, permite que la abstención o el consenso entre los políticos, haga imposible la práctica por esta vía (arts. 161.1.a, y 162.1.a).

Ese contenido esencial supone el respeto mínimo necesario para que no sea un derecho meramente semántico, que realmente no proteja aquello que debe proteger conforme a su propio enunciado. La jurisprudencia del T.C. ha ido definiendo y llenando de contenidos este enunciado conceptual sobre la esencia de los derechos protegidos (vid. las SS.T.C. indicadas antes y la 11/1981). En esta interpretación, hay que tener en cuenta necesariamente el art. 10.2 de la Constitución, que exige una interpretación de las normas relativas a los derechos fundamentales y a las libertades reconocidas por ella, "de conformidad con la

Declaración Universal de Derechos Humanos (Asamblea General de la ONU, 10-12-1948) y los tratados y acuerdos internacionales sobre las mismas materias ratificados por España".

Para interpretar cual es contenido esencial del art. 18.4, que debe respetar la legislación que lo desarrolle, es de singular importancia el Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, celebrado en Estrasburgo el 28 de enero de 1981 y ratificado por España el 27 de enero de 1984 (BOE de 15 de noviembre de 1985). Al mismo nos referiremos más adelante al examinar el contenido de la LORTAD en lo referente a la utilización de datos personales por los poderes públicos.

Entre los Tratados internacionales sobre derechos y libertades suscritos por España, hay que destacar por su relevancia el Convenio Europeo para la protección de los Derechos Humanos y Libertades Fundamentales (Roma, 4 de noviembre de 1950, suscrito por España el 24 de noviembre de 1977).

El criterio interpretativo del art. 10.2, y siguiendo la doctrina del Tribunal Constitucional, nos permite interpretar el art. 18.4, y la legislación que lo desarrolla, conforme a los principios de los tratados internacionales ratificados por España. Particular relevancia tienen el art. 12 de la Declaración Universal de Derechos Humanos y el art. 8 del Convenio Europeo de 1950. Dichos principios tienen el mismo valor que la norma constitucional y son principios interpretativos invocados por ésta.

El art. 12 establece que nadie será objeto de injerencias arbitrarlas en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honor o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias y ataques. Idéntico contenido tiene el art. 17, injerencias arbitrarlas o ilegales..., del Pacto Internacional de Derechos Civiles y Políticos, suscrito en Nueva York el 19 de diciembre de 1966 (BOE de 30, de abril de 1977).

A su vez, el art. 8 del Convenio Europeo dice:

8.1. Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia.

8.2. No podrá haber injerencia de la autoridad pública en el ejercicio de este derecho, sino en tanto en cuanto esté injerencia esté previsto por la ley y construya una medida que, en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención del delito, la protección de la salud o de la moral o la protección de los derechos y libertades de los demás.

Para que una medida pueda considerarse necesaria en una sociedad democrática, debe ser proporcionada con el objeto legítimo que se pretenda. Pudiendo recurrirse al Tribunal Europeo de Derechos Humanos.

En el propio Convenio se establece el Tribunal Europeo de Derecho Humanos (art. 38), a cuyas decisiones se someten los Estados que lo han suscrito (art. 53). Por lo que cabe recurrir a dicho Tribunal ante extralimitaciones de cualquiera de los Estados (sobre el funcionamiento del Tribunal y las limitaciones de recurso, vid. García de Enterria, E, y otros, "El sistema europeo de protección de los derechos humanos, Ed. Civitas, 1979; O. de 21 de mayo de 1987 -Disp. 12217 del BOE de 22 de mayo. Sobre protección internacional en general, vid. Nikken, P. "La protección internacional de los derechos Humanos", Ed. Cívitas, 1987, y Ull Pont, E., "La protección de los derechos fundamentales", las X Jornadas de Estudio de la Dirección General del Servicio Jurídico del Estado, Ministerio de Justicia, mayo de 1988).

Por otra parte, el repetido art. 53, reconoce el derecho del ciudadano a pedir la tutela judicial de los derechos y libertades reconocidos en el art. 14 y en la Sección primera, del Cap. II del Tit. I (arts. 15 al 29), por un procedimiento basado en los principios de preferencia y sumariedad (vid. L. 62/1978 de 26 de diciembre, de protección jurisdiccional de los derechos fundamentales de la persona, y el R.D. Legislativo, 342/1379, de 20 de febrero, sobre ampliación del ámbito de la Ley citada, y las SS.T.C. 3/1984, de 27 de marzo, y 43/1989, de 20 de febrero. Ibid. la Disp. Transitoria Segunda, 2, de la L.O. 2/1979, de 3 de octubre, del Tribunal Constitucional)).

Agotado el recurso ante los Tribunales Ordinarios, sin conseguir el restablecimiento de los derechos fundamentales vulnerados, se puede recurrir en amparo ante el Tribunal Constitucional (vid. SS.T.C. 9/1981; 34/1989, y, especialmente la 133/1989). También se puede recurrir en amparo en el supuesto de objeción de conciencia (art. 30).

No entramos a considerar la doctrina favorable a extender la legitimación de ejercicio de recurso de amparo a favor de las personas jurídicas, posición doctrinal que no compartimos (vid. La S.T.C. 64/1988).

Los ilícitos contra las personas jurídicas pueden tener una protección por su contenido económico, que se regula en otros ámbitos. Y cuando afecta a personas físicas, es en defensa de estas cuando procederán otras actuaciones.

3. La ley Orgánica 5/1992, de 29 de octubre. de regulación del tratamiento de automatizado de datos de carácter personal

Con la Ley 5/1992 se cumplen varias previsiones pendientes, pero, en nuestra opinión mal. Por una parte la Constitución Española de 1978, en el artículo que es el principal argumento de nuestro trabajo, el 18.4, da un mandato al legislador para que regule por ley el uso de la informática para garantizar los derechos personales. Se cumple tal mandato 14 años después. Como vemos no tuvo que ser algo apresurado, más bien, parece que no habla prisa.

Si bien es verdad que ya existían invocaciones sectoriales protectoras de los datos personales, automatizados o no. Así, respecto a los funcionarios públicos, en la Ley 30/1984, de 2 de agosto, sobre medidas para la reforma de la función pública, se contempla diferenciadamente lo que son datos incluídos y excluídos en los Registros de Personal de todas las Administraciones Públicas, cuales serán sus contenidos mínimos homogeneizadores y los requisitos y procedimientos para su utilización recíproca. Se establece también que en la documentación individual del personal de las diferentes Administraciones Públicas no figurará ningún dato relativo a su raza, religión u opinión. Reconociéndose al interesado su derecho a tener libre acceso a su expediente individual (art. 13). También se dispone en esta Ley que "las relaciones de puestos de trabajo serán públicas", tanto respecto a la Administración del Estado, como en la Administración Local y las Administraciones de las Comunidades Autónomas (art. 15 y 15). Con esto último se aplica una limitación al derecha personal a la intimidad de sus datos, por razones de interés general de necesaria aplicación en una democracia. Otros ejemplos podemos encontrarlos en leyes reguladoras de actuaciones de las Administraciones en las que su procesan datos personales (vid. también, entre otros L. 230/1963, General Tributaria, arts 111 y s.; D. 2065/74, Texto refundido de la Ley General de Seguridad Social, art. 14; L. 1/82, de Protección civil del honor, a la intimidad personal y familiar y a la propia

imagen, en particular los art. 7 y la Disp. transitoria primera, que ha sido derogada por la LORTAD, por la que se aplicarla dicha Ley en tanto no se desarrollara la legislación prevista por la Constitución para la protección por e, uso de la informática; L.O. 5/1985, de 19 de junio, del Régimen Electoral General, arts. 32.1., 33.4 y 5., y 41; L12/1989, de la Función Publica Estadística, en lo referente al secreto estadístico, etc.).

Conforme al art. 81.1. de la C.E. al tratar del desarrollo de derechos fundamentales, las previsiones legislativas del art.18.4 de la C.E., tenían que desarrollarse mediante una Ley Orgánica. Y lo es, pero quitando tal carácter a determinado articulado, que queda como Ley ordinaria y con previsiones de desarrollo vía reglamento, y, además, con una delegación legislativa que vulnera lo establecido en el art. de referencia y el art. 83 de la misma Constitución. Parece que carencias y abusos aparte, la LORTAD puede considerarse salpicada en muchos de sus preceptos, de inconstitucionalidad legislativa. Así lo han entendido por una parte el Defensor del Pueblo, el Grupo Parlamentario Popular y por otra la Generalidad y el Parlamento de Cataluña, planteando sendos recursos de inconstitucionalidad ante el T.C.

La institución del Defensor del Pueblo entabló el recurso, dentro del ejercicio de sus competencias que le legitiman para ello, con fecha 28 de enero de 1993. Sin entrar en e, análisis de las cuestiones planteadas como inconstitucionales, estas se refieren a los arts. 19.1, 22.1 y 22.2, por considerar se vulnera el art. 18.4 de la C.E., en relación con el 18.1 y el 53.1, por no respetar el principio de reserva de ley, con un régimen en lo referente a las Administraciones Públicas, que no respeta el principio de consentimiento del art. 11.1, ni el de información.

En el recurso del Grupo Parlamentario Popular se cuestionan de inconstitucionalidad los arts. 6.2, 19.1, 20.3 y el 22.1 y 2. y los preceptos conexos con los indicados.

Para la Generalidad refiere su recurso al art. 39 y, además, coincidiendo con el Parlamento de Cataluña a los artíc. 24 , 40.1. y 40.2. Sus recursos se centran en defender posibles competencias de las autonomías, para crear y mantener sus propios ficheros públicos de datos personales.

Es de esperar y deseamos que el alto Tribunal, declare inconstitucionales aquellos preceptos que no respetan el contenido esencial de los derechos

protegidos, por no respetar lo establecido en el 53.1 de la Constitución y los arts. 5, 6 y 8 del Convenio, así como de otros que vulneran los principios de legalidad, de jerarquía normativa y de seguridad jurídica. En su momento, a la vista de los fallos que emita el T.C. revisaremos nuestros planteamientos.

También fue emitido un Dictámen por el Prof. López Garrido, al parecer a instancias de la Comisión de Libertades e Informática del Congreso, con cuyo contenido me encuentro muy identificado (vid. Rev. D. Político de la UNED, nº 38, pags. 13 y ss.). Dicho trabajo es de fecha anterior a la Ley, pero invoca ésta como ya promulgada. Resulta claro que hay alguna error en las fechas, o una actualización posterior de contenidos, de cara a su publicación, pero eso no quita valor a sus planteamientos.

Por otra parte, España suscribe el citado Convenio de Estrasburgo, de 28 de enero de 1981, por el que queda obligada a ajustar su legislación al mismo. Once años después, siguiendo en buena medida sus enunciados, se promulga la LORTAD, que, supongamos, deja para mejor ocasión, el cumplimiento del art. 3.c) del Convenio, según el cual también debe regularse la utilización de ficheros no automatizados, ni destinados a serlo.

Por último, España "se apunta" al Convenio de Schengen de 14 de julio de 1985, referente a la supresión gradual de los controles policiales en las fronteras comunes. Para su efectividad, los países participantes deben tener previamente legislado por lo menos en lo que se refiere a la protección de datos personales requeridos en el Convenio 108 del Consejo de Europa de 1981. España lo suscribió el 25 de junio de 1991.

De ahí nacen "las prisas" de última hora, para poder participar con otros Estados europeos de las ventajas del Convenio de Schengen. Pero esas prisas, no fueron suficientes para evitar concesiones arbitrarias al poder público, que no parecen justificadas por la constitución, ni por la necesidades generales.

También para cumplir con las condiciones de participación en la transferencia internacional de datos establecida por dicho Convenio de Schengen, se dista una Orden del Ministerio de Justicia e Interior, de 2 de febrero de 1995" por la que se aprueba la primera relación de países con protección de datos de carácter personal equiparable a la española. En la misma se enumeran los países adheridos al Convenio que cumplen con las condiciones necesarias, y se hace otra enumeración respecto a terceros países que también cumplen las condiciones

requeridas, en este último supuesto para poder tener en cuenta lo establecido en el art. 32 de la LORTAD, sobre el movimiento internacional de datos de carácter personal.

Recordemos que en art. 9.3 de la C.E. se proclama que tanto los ciudadanos, como los poderes públicos están sujetos a la Constitución y al resto del ordenamiento jurídico. También, que corresponde a los poderes públicos promover las condiciones para que la libertad y la igualdad sean reales y efectivas; remover los obstáculos. Y por último, que quedan constitucionalmente garantizados estos principios:

a) de legalidad,

b) de jerarquía normativa,

c) de publicidad de las normas,

d) de irretroactividad sancionadora de disposiciones no favorables o restrictivas de los derechos individuales,

e) de seguridad Jurídica,

f) de responsabilidad e interdicción de la arbitrariedad de los poderes públicos.

Pues bien, nos parece que la LORTAD se ha apuntado a vulnerar todos o casi todos estos principios, como ya vimos al referirnos a los recursos de inconstitucionalidad presentados ante el T.C.

Pero, con independencia de la inconstitucionalidad de sus preceptos, veamos como queda la persona prácticamente desprotegida del derecho de libertad informativa que le reconoce el art. 18.4 de la C.E., en lo que se refiera a las actuaciones de las Administraciones Públicas para la automatización de datos de carácter personal.

4. Principios para la interpretación de art. 18.4 y la LORTAD.

Conforme venimos exponiendo, el contenido del art. 18.4 de la Constitución debe interpretarse teniendo en cuenta los Tratados y Convenios internacionales ratificados por España (art. 10.2 CE). Sus principios tiene el valor

de derecho interno, pues, conforme con el art. 96.1 de la C. E. los trabajos internacionales válidamente celebrados una vez publicados oficialmente en España formaran parte del ordenamiento interno y además, sus disposiciones solo podrán ser derogadas modificadas o suspendidas en la forma previsto en los propios trabajos o de acuerdo con las normas generales del derecho internacional .

Y en aplicación de tales principios constitucionales, hay que contemplar las normas de el repetido Convenio de 28 de enero de 1981, para la protección de las personas, con respeto al tratamiento automatizado de datos de carácter personal, suscrito en Estrasburgo. Sus principios tiene el valor de derecho interno, y tanto la interpretación de las normas constitucionales, como de las leyes que las desarrollen, no pueden legalmente estar en contracción con aquellos. El objeto del Convenio es garantizar....a cualquier persona física sean cuales fueren su nacionalidad o su residencia el respeto de sus derechos y libertades fundamentales concretamente el derecho a la vida privada con respecto al tratamiento automatizado de los datos de carácter personal correspondiente a dicha persona. (art. 1).

En el Convenio, España, como parte signatoria tiene la obligación en cuanto a su Derecho interno, de tomar las medidas necesarias para que sean efectivos los principios básicos para la protección de datos enunciados en el Capítulo II del mismo (art. 4 del Convenio).

El capítulo 11 del Convenio es la clave para la interpretación del contenido de la LORTAD, con la cual se pretende cumplir el mandato de su art. 4. Tienen especial interés los arts. 5, 6 y 8, en los que se puntualiza las condiciones que deben tenerse en cuenta en el tratamiento de datos, y el art. 9 que determina las excepciones y restricciones que condicionan el tratamiento en determinados supuestos. Veamos.

Art. 5. Calidad de los datos.

Los datos de carácter personal que sean objeto de un tratamiento automatizado:

a) se obtendrán y trabajan legal y legítimamente.

b) se registrarán para finalidades determinadas y legítimas y no se utilizarán de una forma incompatible con dichas finalidades.

c) serán adecuados Pertinentes y no excesivos en relación con las finalidades para las cuales se hayan registrado.

d) serán exactos y si fuera necesario puestos al día.

e) se conservarán bajo una forma que permita la identificación de las personas concernidas durante un periodo de tiempo que no exceda del necesario para las finalidades para las cuales se hayan registrado. .

Según el mismo, no se pueden procesar ficheros de datos personales de tratamiento automatizado si no hay una base legal para ello y deben ser recogidos los datos legítimamente por quien corresponda, sin engaño, ni fraudulentamente.

También tiene que estar justificada tal creación por razón del fin perseguido que debe ser lícito y concreto, y no cabe utilizar los datos en forma que adultere el fin concreto que legitime tales ficheros.

Teniendo en cuenta el fin concreto y lícito, la recogida de datos debe ser correcta y no excederse recogiendo datos relacionados que no se corresponden con la concreción requerida, o que no sean necesarios para el fin concreto perseguido.

La exactitud de los datos y su puesta al día, supone el requerimiento de la rectificación cuando los datos recogidos fueren erróneos o falsos, o estuvieren superados.

Su conservación se limitara al tiempo necesario según el fin concreto y lícito para el cual fueron registrados. Por consiguiente no será licito conservarlos por tiempo indefinido.

Art. 6. Categorías particulares de datos.

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 impersonal referentes a condenas penales.

El Convenio también contempla un limitación en la licitud del tratamiento automatizado de datos, teniendo en cuenta la naturaleza de determinados datos personales. Se refiere a los llamados "datos sensibles", como son la raza, opinión, religión, salud o vida sexual, a los que añade también los antecedentes penales. Para tales supuestos prohibe su tratamiento, salvo que el derecho interno prevea garantías apropiadas. Raza, opinión y religión, son datos específicamente protegidos por la C.E. frente a posible utilización sin consentimiento del interesado (art. 16. 2.). En los supuestos de salud o vida sexual, creemos que son datos que deben tratarse dentro de la normativa del anonimato y secreto estadístico (vid. Ley citada antes).

También el art. 7 tiene relevancia, en lo referente a la seguridad de los datos de carácter personal registrados en ficheros, para evitar su destrucción accidental, y lo que es mas importante aun, para evitar el acceso, la modificación o la difusión no autorizados.

A su vez, la persona concernida, o "afectada", en la terminología de la LORTAD tienen reconocidas en el Convenio unas garantías frente la automatización de su datos personales. En el artículo 8 del mismo se dice:

Art. 8. Garantías complementarias para la persona concernida.

Cualquier persona debe poder:

a) conocer la existencia de un fichero automatizado de datos de carácter personal, sus finalidades principales, así como la identidad y la residencia habitual o el establecimiento principal de la autoridad controladora del fichero;

b) obtener a intervalos razonables y sin demora o gastos excesivos la confirmación de la existencia o no en el fichero automatizado de los datos de carácter personal que conciernan a dicha persona, así como la comunicación de dichos datos en forma inteligible;

c) obtener, llegado el caso, la rectificación de dichos datos o el borrado de los mismos, cuando se hayan tratado con infracción de las disposiciones del

derecho interno que hagan efectivos los principios básicos enunciados en los artículos 5 y 6 del presente Convenio;

d) disponer de un recurso si no se ha atendido a una petición de confirmación, o, si así fuere el caso, de comunicación, de ratificación o de barrado, a que se refieren los párrafos b) y c) del presente artículo.

A la persona concernida o titular de los datos que puedan haberse automatizado, por el Convenio se le atribuyen unos derechos que le permitan comprobar que se han cumplido las condiciones de automatización de sus datos, exigidas por los artículos 5 y 6 del Convenio. Y también el derecho a disponer de recursos o acciones eficaces para obligar a cumplir las indicadas condiciones, si no se hubieren respetado.

En consecuencia, el titular de los datos tiene derecho:

1. A saber que existe o no un fichero con datos personales suyos.

   Y si lo hay, saber con que finalidad y quien es la autoridad que controla tal fichero.

2. También conocer periódicamente si aun existe tal fichero y su contenido.

3. A conseguir que se rectifique o a que se borre, según proceda, en defensa de sus derechos.

4. Y, finalmente tener protección Jurídica para hacer efectivos los derechos indicados.

De lo contrario supondría un vacío de contenido, es decir una falta protección efectiva.

Junto a estas garantías respecto al proceso de automatización de datos personales, el Convenio también prevé excepciones. Veamos el art. 9 del repetido Convenio.

Art. 9 Excepción y restricciones.

1. No se admitirá excepción alguna en las disposiciones de los artículos 5, 6 y 8 del presente Convenio, salvo que sea dentro de los límites que se definen en el presente artículo.

2. Será posible una excepción en las disposiciones de los artículos 5, 6 y 8 del presente Convenio cuando tal excepción, prevista por la ley de la Parte, construya una medida necesaria en una sociedad democrática:

a) 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;

b) para la protección de la persona concernida y de los derechos y libertades de otras personas.

3. Podrán preverse por la ley restricciones en el ejercicio de los derechos a que se refieren los párrafos b), c) y d) del art. 8 para los ficheros automatizados de datos de carácter personal que se utilicen con fines estadísticos o de Investigación científica, cuando no existan manifiestamente riesgos de atentado a la vida privada de las personas concernidas".

Se parte del principio de que las excepciones son tasadas o limitadas, debiendo prevalecer en general las condiciones establecidas en los artículos 5, 6 y 8, en cuanto garantes de las condiciones exigibles para la creación de ficheros automatizados de datos personales, así como para garantizar los correlativos derechos de las personas concernidas.

Una condición general para que sea legítima alguna excepción es la exigencia de que haya sido prevista por la Parte, al ratificar el Convenio y que constituya una medida necesaria en una sociedad democrática. Es importante para lo sucesivo de nuestra exposición, no perder de vista estas afirmaciones o principios. No nos sirven argumentos justificativos más o menos imprecisos o genéricos como utilidad general, interés general y otras vaguedades en las cuales cabe todo lo que se quiera meter.

Cumpliéndose esa condición general indicada en el párrafo anterior, las excepciones posibles se circunscriben las situaciones siguientes tres supuestos:

1. En defensa de Estado y/o de la sociedad, porque sea necesaria la medida para la seguridad dei Estado o para la seguridad pública.

2. En defensa de la persona física, para la protección del propio concernido o de los derechos y libertades de otras personas.

3. Cuando sean con fines estadísticos o de investigación científica, salvaguardando la vida privada de las personas concernidas (vid Ley de la función estadística).

En este último supuesto se requiere que la excepción se establezca por Ley, que, lógicamente deberá dar las garantías de anonimato necesarias, y el alcance de las restricciones

Como hemos visto, en este tercer supuesto, las excepciones pueden referirse a los derechos reconocidos en el art. 8 referidos a tener confirmación periódica y económica de la existencia de un fichero y su contenido, al derecho a rectificar o borrar tal fichero, según los casos, y a disponer de un recurso para hacer valer los derechos anteriores, si no son respetados. En tales casos quedarían suspendidos total o parcialmente los mismos.

Las razones parecen ser aceptables: la finalidad de utilidad común, como necesidad para conocer la situación real de determinados problemas, recursos, enfermedades, etc. Y la garantía de que no suponga en ningún caso perturbación de la vida privada de las personas.

Las normas que hemos contemplado ahora, junto con las propias normas constitucionales, deberemos tenerlas presentes para valorar los contenidos de la LORTAD, según vamos a intentar a continuación.

5. Principios sobre la protección de datos proclamados en la LORTAD.

5.1 Principios.

Como venimos señalando, la L. O. 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal, pretende ajustarse a los compromisos internacionales y a los principio constitucionales para la protección de datos personales que puedan afectar al libre

ejercicio de los derechos y libertades personales y, particularmente al derecho a la intimidad personal y familiar.

Sus fines nos parecen correctos. Pero ¿se cumplen? Empecemos por ver someramente cuales son los principios que se enuncian para alcanzar su propósito. Después veremos como se cumplen o no tales principios en la regulación del tratamiento automatizado de datos por parte de las Administraciones Públicas, en definitiva, si para los ficheros de titularidad pública se respetan tales principios y si las excepciones se ajustan a los principios internacionales y constitucionales para que sean licitas.

En la Exposición de motivos de la Ley, se hacen unas afirmaciones muy convincentes.

Se afirma que 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 inmunidad: aquella es más amplia que esta, pues en tanto la intimidad protege la esfera en que se desarrollan las facetas mas singularmente reservadas de la vida de la persona al 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 este tiene derecho a mantener reservado. r si la intimidad, en sentido estricto, esté suficientemente protegida por las previsiones de los tres primeros párrafos del artículo 18 de la Constitución y por las leyes que los desarrollan, la privacidad puede resultar menoscabada por la utilización de las tecnologías informáticas de tan reciente desarrollo. Declaración que suscribimos plenamente, si bien coincidimos con Emilio del Peso en su apreciación de que era innecesario introducir el barbarismo "privacidad", que, afortunadamente no se conserva en el texto de la Ley (vid. Peso, E. del, "Confidencialidad y seguridad de la información", Ed. Díaz Santos, 1994, intimidad y privacidad, pag 63 ss.).

La justificación de la protección ante la automatización de datos, queda justificada si tenemos en cuenta que hoy las modernas técnicas de comunicación permiten salvar sin dificultades el espacio y la informática posibilita almacenar todos los datos que se obtienen a través de las comunicaciones y acceder a ellos

en apenas segundos, por distante que fuera el lugar donde transcurrieron los hechos, o remotos que fueran estos. Los más diversos datos sobre la infancia, sobre la vida académica, profesional o laboral, sobre los hábitos de vida y consumo, sobre el uso del denominado «dinero plástico», sobre las relaciones personales o, incluso, sobre las creencias religiosas e ideologías, podrían ser, así, compilados y obtenidos sin dificultad. Ello permitiría a quien dispusiese de ellos acceder a un conocimiento cabal de actitudes, hechos o pautas de comportamiento que, sin duda, pertenecen a la esfera privada de las personas; a aquélla a la que sólo deben tener acceso el individuo y, quizás, quienes le son más próximos, o aquellos a los que el autorice. Aún más: El conocimiento ordenado de esos datos puede dibujar un determinado perfil de la persona, o configurar una determinada reputación o fama que es, en definitiva, expresión del honor, y este perfil, sin duda, puede resultar luego valorado, favorable o desfavorablemente, para las más diversas actividades públicas o privadas, como pueden ser la obtención de un empleo "a concesión de un préstamo o la admisión en determinados colectivos".

Para la recogida de los llamados "datos sensibles", se establece un reforzamiento de la protección. La ideología o creencias religiosas, está expresamente garantizada por la Constitución en su artículo 16.2, y la raza, la salud y la vida sexual, constituyen actualmente, datos de ese carácter. La protección reforzada de estos datos viene determinada porque los primeros de entre los datos mencionados;. los sólo serán disponibles con el consentimiento expreso y por escrito del afectado, y los segundos serán susceptibles de recopilación mediando dicho consentimiento o una habilitación legal expresa, habilitación que, según exigencia de la propia Ley Orgánica, ha de fundarse en razones de interés general; en todo caso, se establece la prohibición de los ficheros creados con la exclusiva finalidad de almacenar datos personales que expresen las mencionadas características .

Para la efectividad de la protección la persona frente a la informática, se reconocen los derechos de acceso a los datos, de rectificación y de cancelación. Y se afirma que no se establecen más excepciones que las derivadas de la puesta en peligro de bienes jurídicos en lo relativo al acceso a los datos policiales y a los precisos para asegurar el cumplimiento de las obligaciones tributarias en lo referente a los datos de esté carácter...., afirmando que se cumplen los preceptos constitucionales y los del Convenio suscrito por España. Veremos que no es así.

Como nuestro propósito actual se circunscribe a los principios generales para la creación, mantenimiento y utilización de los ficheros automatizados, y a las garantías de la persona, todo ello referido a ficheros de titularidad pública, hemos de prescindir de otros comentarios.

El objeto de la Ley (art. 18.4 CE) y su ámbito de aplicación, quedan perfectamente definidos (ficheros automatizados, y sus derivados, tanto de titularidad pública como privada), en los arts. 1 y 2 de la Ley. También se enumeran que ficheros quedan fuera de la protección de la misma, y aquellos otros que quedan regulados en otras leyes (electoral, de estadística del Registro Civil, etc.).

Los ficheros automatizados que quedan excluídos de la regulación de la LORTAD, parece razonable por su carácter de datos públicos, o por ser de uso exclusívamente privado. No parece tan razonable la exclusión de aquellos mantenidos por los partidos políticos, sindicatos e iglesias, confesiones y comunidades religiosas en cuanto los datos se refieran a sus asociados o miembros y ex miembros, en perjuicio de la cesión de los datos que queda sometida a lo dispuesto en el artículo 11 de esta Ley, salvo que resultara de aplicación el artículo 7 por tratarse de los datos personales en él contenidos. (art. 2.2.e). Supone una desprotección que nos parece injustificada, y, además, supone un agravio comparativo respecto a otras entidades como pueden ser las asociaciones culturales o las deportivas. De ello nos ocuparemos cuando tratemos de los ficheros de titularidad privada.

Especial interés tiene para nuestro propósito comparar los principios recogidos en la Ley sobre la Constitución, mantenimiento y utilización de los ficheros (art. 4 al 11), y que garantías tiene la persona para protegerse frente a la posible existencia de ficheros automatizados con sus datos (arts. 12 al 17).

En términos generales, como podemos comprobar, la LORTAD cumple con los principios de la Constitución y del Convenio, en cuanto se refiere creación del fichero y recogida do datos, así como en cuanto a las garantías para la persona concernida. De tal manera que si comparamos el texto de los artículos del Convenio con el de los de la LORTAD, a menudo coinciden a la letra.

5.2 Recogida de datos.

Art 4.- Calidad de los datos.

1. Sólo se podrán recoger datos de carácter personal para su tratamiento automatizado, así como someterlos a dicho tratamiento, cuando tales datos sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades legítimas para las que se hayan obtenido. .

En su clasificación sólo podrán utilizarse criterios que no se presten a prácticas ilícitas.

2. Los datos de carácter personal objeto de tratamiento automatizado no podrán usarse para finalidades distintas de aquellas para las que los datos hubieran sido recogidos.

Se corresponde con la exigencia del Convenio de que sean adecuados, pertinentes y no excesivos y que sus finalidades sean concretas y legítimas (vid. art. 5.a, b y c del Convenio).

3. Dichos datos serán exactos y puestos al día de forma que respondan con veracidad a la situación real del afectado.

Según el Convenio serán exactos y puestos al día (art. 5.d.).

4. Si los datos de carácter personal registrados resultaran ser inexactos, en todo o en parte, o incompletos, serán cancelados y sustituidos de oficio por los correspondientes datos rectificados o completados, sin perjuicio de las facultades que a los afectados reconoce el artículo 15.

5. Los datos de carácter personal serán cancelados cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados y registrados.

No serán conservados en forma que permita la identificación del interesado durante un período superior al necesario para los fines en base a los cuales hubieran sido recabados o registrados.

Contemplado en el art. 5.e) del Convenio.

Reglamentariamente se determinará el procedimiento por el que por excepción atendidos sus 9 valores históricos de acuerdo con la legislación especifica se decida el mantenimiento integro de determinados datos.

Supone una excepción por interés general de la sociedad, cuando los datos tengan un valor histórico. En cuanto puede afectar a derechos y libertades del Titulo I de la C.E., entendemos que debe regularse conforme con el art. 82 de la C.

6. Serán almacenados de forma que permitan el ejercicio del derecho de acceso por parte del afectado.

Reconocido el derecho de acceso en el art. 8.a) del Convenio.

7. Se prohibe la recogida de datos por medios fraudulentos desleales o ilícitos. (Conv. art. 5.a.).

El derecho a la información en la recogida de datos, creemos que está razonablemente recogido, con excepción de apartado último:

Art 5.- Derecho de información en la recogida de datos.

1.Los afectados a los que se soliciten datos personales deberán ser previamente informados de modo expreso, preciso e Inequívoco:

a) De la existencia de un fichero automatizado de datos de carácter personal de la finalidad de la recogida de estos y de los destinatarios de la Información.

b) Del carácter obligatorio o facultativo de su respuesta a las preguntas que les sean planteadas.

c) De las consecuencias de la obtención de los datos o de la negativa a suministrarlos.

d) De la posibilidad de ejercitar los derechos de acceso rectificación y cancelación.

e) De la identidad y dirección del responsable del fichero.

2. Cuando se utilicen cuestionarios u otros impresos para la recogida figurarán en los mismos en forma claramente legible las advertencias a que se refiere el apartado anterior.

3. No será necesaria la información a que se refiere el apartado 1 el contenido de ella se deduce claramente de la naturaleza de los datos personales que se solicitan o de las circunstancias en que se recaban.

En definitiva se establece la obligación de informar a la persona concernida de todos los aspectos que comporte la recogida de datos para incorporarlos a un fichero automatizado. En definitiva informar al interesado de sus derechos que le permiten facilitar o no los datos conseguidos voluntariamente u obligatoriamente. Con lo que no podemos estar conforme es con la afirmación de negar tal obligación cuando se deduce de la naturaleza de los datos o de las circunstancias en que se recaban. Tal excepción dada la inconcreción de los conceptos por los que se alega permite una discrecionalidad total, que podría dejar inoperante el derecho reconocido. El principio de seguridad Jurídica queda vulnerado, y por supuesto puede quedar desprotegidos los derechos reconocidos en el art. 18.4 CE. Entendemos debe ser suprimido por inconstitucional.

Art 6.- 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.

No nos parece ortodoxa la afirmación última, pues determinados datos personales sabemos que están protegidos por la Constitución de injerencias no consentidas. Por tanto no siempre se puede establecer una excepción en la exigencia del consentimiento del titular de los datos. Por tanto su vigencia o no, será según la naturaleza de los datos requeridos.

2. No será preciso el consentimiento cuando los datos de carácter personal se recojan de fuentes accesibles al público cuando se recojan para el ejercicio de las funciones propias de las Administraciones Públicas en el ámbito de sus competencias ni cuando se refieran a personas vinculadas por una relación negocial una relación laboral una relación administrativa o un contrato y sean necesarios para el mantenimiento de las relaciones o para el cumplimiento del contrato.

La facultad discrecional de que las Administraciones Públicas puedan, sin el consentimiento del interesado, recoger datos "para el ejercicio de funciones propias...en el ámbito de sus competencias", recogida en este apartado, supone la vulneración del Convenio, pues no es en virtud de necesidad en una sociedad democrática, sino pura arbitrariedad que atenta así mismo, contra el repetido art. 18 4. y, según la naturaleza de los datos, también puede atentar contra el art. 16.2. Que no se diga que en el ejercicio de sus competencias tiene una interpretación que puede llegar hasta tales límites.

Así se deja desprotegida a la persona que supuestamente se dice proteger. Consideramos que es inconstitucional.

3. El consentimiento a que se refiere el artículo podrá ser revocado cuando exista causa justificada para ello y no se le atribuya efectos retroactivos.

5.3. Protección de datos personales "sensibles".

Un concepto un tanto difuso que se vendrá repitiendo en relación con la protección de datos personales es el de datos sensibles. Por lo que conviene situamos conceptualmente para entendemos.

Son datos personales sensibles aquellos datos que pertenecen a la esfera privada íntima, que no son públicos, ni notorios y que su titular no esta obligado a facilitar. Son especialmente sensibles o reservados los referidos a las opiniones políticas, creencias religiosas y otras opiniones y creencias personales.

También son datos sensibles, aunque menos reservados, los referentes al origen racial, salud o vida sexual. Son protección legal, en consecuencia, debe ser menos estricta que si se tratase de los que hemos llamado datos especialmente sensibles. Pero también merecen una especial protección, por la que suele requerirse para recabarlos el consentimiento del concernido, o cuando este justificado para la protección social o de la persona, sustituido el consentimiento por ley que lo disponga adecuadamente (así, las razones de orden publico, de protección de la salud, prevención de enfermedades y epidemias, etc.). Los antecedentes penales, dado el daño que pueden suponer para la persona y su posible rehabilitación, son datos de cierta sensibilidad, que también merecen cierta protección, deben obtenerse de acuerdo con la ley y limitar su acceso y utilización a las esferas judicial y policial.

Según las circunstancias personales y sociales podrá variar el alcance de su contenido. La profesión o el cargo, el valor que el propio interesado de a determinados datos personales, y la propia conciencia social del momento histórico, costumbres y ambiente social, son factores que la ley y la jurisprudencia deben tener en cuenta para valorar el grado de protección que corresponda, y que pueden hacer variar las categorías protegidas. Si consideramos los tiempos previos a la difusión de la automatización de datos, vemos que las posibles agresiones a la intimidad personal eran menores, y por consiguiente la tutela de la ley ha tenido que variar.

La vida social y la importancia y cuidado que pone una persona concreta respecto a la publicidad o reserva de sus datos personales, hace que la línea divisoria entre intimidad y publicidad de sus datos pueda variar respecto a la regla general de protección.

Una clasificación de los datos personales sumamente sencilla y descriptiva, es la que hace el Prof. Miguel Angel Davara. Dentro de este campo empieza por distinguir entre datos públicos o conocidos, y datos privados. A continuación subdivide los datos privados en íntimos y secretos. Los primeros son reservados frente a particulares, pero pueden ser legalmente exigibles. Los secretos que equipara a sensibles, los subdivide a su vez, en dos categorías: a) datos profundos; supongo que equivalen a los que llamamos en nuestro trabajo datos sensibles, b) datos reservados, que equipara con datos sensibilísimos, los que nosotros llamamos reservados o muy sensibles (vid de dicho autor, Derecho Informático, Ed. Aranzadi, 1993, pag. 52 y ss)

El Convenio de Estrasburgo no incluye entre sus definiciones el concepto de "datos personales sensibles. Pero regula en su artículo 6, las "Categorías particulares de datos", incluyendo en dichas categorías las siguientes:

* origen racial,
* opiniones políticas,
* convicciones religiosas y
* otras convicciones. Se añade también como categoría datos personales a proteger:
* salud y
* vida sexual.

Todas ellas están excluídas del tratamiento automatizado de datos, salvo que haya garantías adecuadas en el derecho interno del Estado respectivo.

Finalmente en el mismo artículo se concede la misma protección respecto a los datos por condenas penales.

La Constitución española, como venimos diciendo protege absolutamente de la intromisión no consentida los datos que llamados muy sensibles (vid art. 16.2). También la LORTAD, aunque entre sus definiciones no incluye el concepto de "datos sensibles", en cambio como veremos a continuación, de acuerdo con el Convenio y con la Constitución reconoce como especialmente protegidos determinados datos personales, que define como "datos especialmente protegidos", si bien esa protección se resquebraja cuando se trate de datos contenidos en ficheros de titularidad pública, como veremos al analizar el articulado de la Ley.

En la Exposición de motivos de la LORTAD, a la que hemos aludido antes, tampoco se expone un concepto de datos sensibles para los que requiere un consentimiento consciente e informado. Se utiliza la vía de la enumeración de datos sensibles, incluyendo en su relato, "la ideología o creencias religiosas cuya privacidad esta expresamente garantizada por la Constitución.... y de otra parte, la raza, la salud y la vida sexual. La protección reforzada de estos datos...los primeros...solo serán disponibles con el consentimiento expreso y por escrito... Los segundos...mediante dicho consentimiento o una habilitación legal expresa....fundarse en razones de interés general" (Punto 2, párrafo 7 de la Exposición de Motivos).

Art 7.- 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.

En el art. 6 del Convenio, teniendo en cuenta las categorías particulares de datos, también exige para las categorías indicadas en la Ley española que el derecho interno prevea unas garantías apropiadas. Es decir se declara la protección de estos datos, en línea con lo que el Convenio exige.

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.

Las precedentes exigencias son correctas, se exige que el titular otorgue el consentimiento por escrito y que se le advierta de que no está obligado a facilitar dichos datos. Pero, como veremos más adelantes, por la vía de las excepciones se intenta dejar vacías de contenido las garantías indicadas.

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.

4. Quedan prohibidos los ficheros creados con la finalidad exclusiva de almacenar datos de carácter personal que revelen la ideología, religión, creencias, origen racial o vida sexual.

5. Los datos de carácter personal relativos a la comisión de infracciones penales o administrativas sólo podrán ser incluidos en ficheros automatizados de las Administraciones Públicas competentes en los supuestos previstos en las respectivas normas reguladoras.

Se establece aquí una limitación referida a órganos concretos de la Administración de Justicia y penitenciaria y para sus fines necesarios, conforme a las respectivas normas reguladoras. No siendo en estos supuestos información pública. Parece que se cumplen las garantías exigidas para tales supuestos por el propio Convenio (art. 6 final).

Art 8.- Datos relativos a la salud.

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 25/1990, 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.

Es conforme con el art. 6 del Convenio.

Art 9.- Seguridad de los datos

1. El responsable del fichero deberá adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración perdida 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.

2. No se registrarán datos de carácter personal en ficheros automatizados que no reúnan las condiciones que se determinen por vía reglamentaria con respecto a su Integridad y seguridad y a las de los centros tratamiento locales equipos sistemas y programas.

3. Reglamentariamente se establecerán los requisitos y condiciones que deban reunir los ficheros automatizados y las personas que Intervengan en el tratamiento automatizado de los datos a que se refiere el artículo 7 de esta Ley.

No nos gusta esta remisión a la vía reglamentaria (el subrayado es nuestro), para establecer las condiciones de ficheros y personas que intervengan en su tratamiento. Las exigencias de seguridad de los datos para evitar su alteración, pérdida y acceso, etc., no se concilian bien con la remisión a la vía reglamentaria de los dos puntos últimos del artículo. En el Convenio se exige esa seguridad contra la destrucción, acceso, modificación o difusión no autorizados (art. 7).

Art 10.- Deber de secreto.

El responsable del fichero automatizado y quienes intervengan en cualquier fase del tratamiento de los datos de carácter personal están obligados al secreto profesional respecto de los mismos y al deber de guardarlos obligaciones

que subsistirán aun después de finalizar sus relaciones con el titular del fichero automatizado o en su caso con el responsable del mismo.

Nos parece una medida adecuada y prudente.

Art 11.- Cesión de datos

1. Los datos de carácter personal objeto del tratamiento automatizado sólo podrán ser cedidos para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario con el previo consentimiento del afectado.

2. El consentimiento exigido en el apartado anterior no será preciso:

a) Cuando una Ley prevea otra cosa.

Reiteramos, lo ya dicho en otra ocasión, que hay supuestos perfectamente legitimados por ley, pero no basta que la ley lo establezca, depende también de la calificación o categoría de los datos, que pueden requerir el consentimiento del concernido por exigencia constitucional y/o del Convenio.

b) Cuando se trate de datos recogidos de fuentes accesibles al público.

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

Aun en estos supuestos, hay una aceptación libre aunque indirecta, por la relación Jurídica establecida, y se condiciona a que se utilice SOLO para la finalidad concreta propia de la relación Jurídica establecida.

d) Cuando la cesión que deba efectuarse tenga por destinatario el Defensor del Pueblo el Ministerio Fiscal o los Jueces o Tribunales en el ejercicio de las funciones que tienen atribuidas.

e) Cuando la cesión se produzca entre las Administraciones Públicas en los supuestos previstos en el artículo 19.

Este apartado puede estar afectado de inconstitucionalidad, en la medida que el art. 19 en el que se apoya para negar la necesidad del consentimiento, sea declarado inconstitucional. Lo cual es más que probable, pues podría significar una utilización del fichero para finalidades no contempladas en su creación.

f) Cuando la cesión de datos de carácter personal relativos a la salud sea necesaria para solucionar una urgencia que requiera acceder a un fichero automatizado o para realizar los estudios epidemiológicos en los términos establecidos en el artículo 8 de la Ley 14/1986 de 25 de abril General de Sanidad.

Tanto en el ámbito público como en el privado, esta permitido que las instituciones sanitarias y profesionales, con la finalidad de tener los antecedentes necesarios del enfermo, para su adecuada atención. Por otra parte, se contempla aquí la necesidad de que el sistema sanitario realice los estudios epidemiológicos necesarios para orientar eficazmente la prevención, la planificación y la evaluación sanitaria, por lo que necesita un sistema de información y vigilancia sanitaria para poder realizar las campañas epidemiológicas en favor de la salud.

En la propia Ley 14/1986 se reconoce a todos el derecho a "la confidencialidad de toda información relacionada con su proceso y con su estancia en instituciones sanitarias públicas y privadas que colaboren con el sistema público" (art. 10.3).

3. Será nulo el consentimiento cuando no recaiga sobre un cesionario determinado o determinable o si no constase con claridad la finalidad de la cesión que se consiente.

4. El consentimiento para la cesión de datos de carácter personal tiene también un carácter de revocable.

5. El cesionario de los datos de carácter personal se obliga por el solo hecho de la cesión a la observancia de las disposiciones de la presente Ley.

6. Si la cesión se efectúa previo procedimiento de disociación no ser aplicable lo establecido en los apartados anteriores.

Del art. 12 al 17 de la Ley se dedican a definir los derechos de los concernidos por los datos personales automatizados.

6. Derechos de las personas.

El Título III de la LORTAD dedica a definir los derechos personales y las vías reconocidas para hacerlos valer.

Art 12.- Impugnación de valoraciones basadas exclusivamente en datos automatizados

El afectado podrá impugnar 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.

Art 13.- Derecho de información.

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

Art 14.- Derecho de acceso.

1. El afectado tendrá derecho a solicitar y obtener información de sus datos de carácter personal incluídos en los ficheros automatizados.

2. La información podrá consistir en la mera consulta de los ficheros por medio de su visualización o en la comunicación de los datos pertinentes mediante escrito copia telescopio o fotocopia certificada o no en forma legible o inteligible sin utilizar claves o códigos convencionales que requieran el uso de dispositivos mecánicos específicos.

3. El derecho de acceso a que se refiere este artículo sólo podrá ser ejercitado a intervalos no inferiores a doce meses salvo que el afectado acredite un interés legítimo al efecto en cuyo caso podrá ejercitarlo antes.

Art 15.- Derecho de rectificación y cancelación.

1. Por vía reglamentaria se establecerá el plazo en que el responsable del fichero tendrá la obligación de hacer efectivo el derecho de rectificación o cancelación del afectado.

2. Los datos de carácter personal que resulten inexactos o incompletos serán rectificados y cancelado en su caso.

3. El los datos rectificados o cancelados hubieran sido cedidos previamente, el responsable del fichero deberá notificar la rectificación o cancelación efectuada al cesionario.

4. La cancelación no procederá cuando pudiese causar un perjuicio a intereses legítimos del afectado o de terceros o cuando existiese una obligación de conservar los datos.

5. Los datos de carácter personal deberán ser conservados durante los plazos previstos en las disposiciones aplicables o, en su caso, en las relaciones contractuales entre la persona o entidad responsable del fichero y el afectado.

Art 16.- Procedimiento de acceso.

1. El procedimiento para ejercitar el derecho de acceso, así como el de rectificación y cancelación será establecido reglamentariamente.

2. No se exigirá contraprestación alguna por la rectificación o cancelación de los datos de carácter personal inexactos.

Art 17.- Tutela de los derechos y derecho de Indemnización.

1. Las actuaciones contrarias a lo dispuesto en la presente Ley pueden ser objeto de reclamación por los afectados ante la Agencia de Protección de Datos, en la forma que reglamentariamente se determine.

No es constitucionalmente pertinente que las reclamaciones por derechos fundamentales amparados en el art 18.4 de la C.E, se regulen por reglamento, pues no se respeta el principio de reserva de ley que corresponde conforme al art. 53.1 de la Constitución.

2. Contra las resoluciones de la Agencia de Protección de Datos proceder recurso contencioso administrativo.

3. Los afectados que, como consecuencia del incumplimiento de lo dispuesto en la presente Ley por el responsable del fichero, sufran daño o lesión en sus bienes o derechos tendrán derecho a ser indemnizados.

4. Cuando se trate de ficheros de titularidad pública, la responsabilidad se exigirá de acuerdo con la legislación reguladora del régimen de responsabilidad de las Administraciones Públicas.

5. En el caso de los ficheros de titularidad privada la acción se ejercitará ante los órganos de la jurisdicción ordinaria.

Los derechos reconocidos a la persona afectada por la automatización de sus datos personales, con las salvedades que hemos apuntado y, particularmente en relación con el art. 17.1, en su conjunto está razonablemente regulado y se ajusta a las disposiciones del art. 8 del Convenio, el cual ya vimos antes: derecho a conocer la existencia, finalidad, y autoridad que controla el fichero, o de información; derecho de acceso al contenido, de rectificación de errores o de borrado del fichero cuando la finalidad se ha cumplido, y, por supuesto de posibilidad de defenderse cuando no es atendido en sus derechos, o cuando resulta perjudicado injustamente por el fichero.

El problema vendrá cuando tengamos que aplicar estos principios a determinados ficheros de titularidad pública.

7. Ficheros de titularidad pública.

7.1. Creación de ficheros y recogida de datos.

Ahora pasamos a tratar la parte final pero decisiva tratando de las excepciones que priman la normativa sobre los ficheros de datos personales de titularidad pública. Apreciaremos la impunidad de las Administración en este campo, dejando muy desprotegida a la persona respecto a sus datos personales. Creemos que en muchos supuestos vaciando el contenido de los derechos constitucionales en favor de una discrecionalidad casi absoluta.

Art 18.- Creación, modificación o supresión.

1. La creación, modificación o supresión de los ficheros automatizados de las Administraciones Públicas sólo podrán hacerse por medio de disposición general publicada en el Boletín Oficial del Estado o diario oficial correspondiente.

2. Las disposiciones de creación o de modificación de los ficheros deberán indicar:

a) La finalidad del fichero y los usos previstos para el mismo.

b) Las personas o colectivos sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos.

c) El procedimiento de recogida de los datos de carácter personal.

d) La estructura básica del fichero automatizado y la descripción de los tipos de datos de carácter personal incluidos en el mismo.

e) Las cesiones de datos de carácter personal que en su caso se prevean.

f) Los órganos de la Administración responsables del fichero automatizado.

g) Los servicios o unidades ante los que pudiesen ejercerse los derechos de acceso rectificación y cancelación.

3. En las disposiciones que se dicten para la supresión de los ficheros automatizados se establecerá el destino de los mismos o en su caso las previsiones que e adopten para su destrucción.

Resulta francamente aceptable la regulación para crear, finalidad, obligatoriedad o no de aportar los datos requeridos, autoridad responsable, derechos de acceso rectificación y cancelación.

No resulta tan claro que en disposiciones posteriores, en las disposiciones que se disten para la supresión pueda establecerse el destino de los mismos, sin contar con el consentimiento de los afectados.

Por lo demás, el conjunto de estas normas, se ajusta a los principios requeridos conforme a la Constitución y al Convenio.

Art 19 - Cesión de datos entre Administraciones Públicas.

1. Los datos de carácter personal recogidos o elaborados por las Administraciones Públicas para el desempeño de sus atribuciones no serán cedidos a otras Administraciones Públicas para el ejercicio de competencias diferentes o de competencias que versen sobre materias distintas salvo cuando la cesión hubiese sido prevista por las disposiciones de creación del fichero o por disposición posterior de igual o superior rango que regule su uso.

Este punto ya resulta muy conflictivo. Coinciden el Defensor del Pueblo y el Grupo Parlamentario Popular en tacharlo de inconstitucional; también el Prof. López Garrido lo considera inconstitucional. A nosotros no nos cabe duda de su inconstitucionalidad, pues son vulnerados múltiples principios constitucionales en favor de la arbitrariedad de las Administraciones Públicas.

El art. 18. a), esta en consonancia con el art. 5.b) del Convenio, pero la disposición que contemplamos ahora los deja vacíos de contenido ya que exige conocer la finalidad del fichero. También queda inoperante el art. 4.2. que antes vimos, que prohibe usar los datos para finalidades distintas para las que hubieran sido recogidos. Y no queda mejor el art. 11 de la Ley, que en su punto 1. establece que solo serán cedidos para el cumplimiento de los fines con el previo consentimiento de afectado

De tal manera que, según la LORTAD, los ficheros de titularidad pública, con los datos de carácter personal El serán cedidos a otras Administraciones Públicas, para finalidades diferentes, Sí una disposición posterior de igual o superior rango así lo dispone. Con lo cual el contenido esencial de los derechos reconocidos en el art. 18.4., que debe ser salvaguardado como dispone el art. 53.1, de la C.E., y, además, vulnera el principio de legalidad (art. 9.3 de la C.E.) y los Convenios internacionales sobre derechos y libertades, ratificados por España.

2. Podrán en todo caso ser Objeto de cesión los datos de carácter personal que una Administración Publica obtenga o elabore con destino a otra.

3. No obstante lo establecido Pn el artículo 11.2 b) la cesión de datos recogidos de fuentes accesibles al público no podrá efectuarse a ficheros de

titularidad privada sino con el consentimiento del interesado o cuando una Ley prevea otra cosa.

Según esté punto 19.3, seguimos con la inseguridad Jurídica sobre que se va ha hacer con nuestros datos, incluso respecto a ficheros de titularidad privada, si una ley puede disponer que se prescinda del consentimiento del interesado.

Otro tema muy grave es el referente a los ficheros de las Fuerzas y Cuerpos de Seguridad del Estado.

Art 20 - Ficheros de las Fuerzas y Cuerpos de Seguridad

1. Los ficheros automatizados creados por las Fuerzas y Cuerpos de Seguridad que contengan datos de carácter personal que, por haberse recogidos para fines administrativos, deban ser objeto de registro permanente, estarán sujetos al régimen general de la presente Ley.

La justificación de que puedan recogerse datos para fines administrativos no puede ser más inconcreta y arbitraria, y tampoco queda justificada por la necesidad de tales datos. Por lo que, discrecional e impunemente se podrían recoger cualesquiera datos, sin necesidad de consentimiento ni de justificación, convirtiendo en regla general de impunidad por parte de la Administración, lo que debe ser situaciones excepcionales y justificadas por la necesidad para una sociedad democrática. Las garantías del art. 18.4 de la C.E. quedarían vacías de contenido.

2. La recogida y tratamiento automatizado para fines policial de datos de carácter personal por las Fuerzas y Cuerpos de Seguridad sin consentimiento de las personas afectadas, tan limitados a aquellos supuestos y categorías de datos que resultan necesarios para la prevención de un peligro real para la seguridad pública o para la represión de Infracciones penales, debiendo ser almacenados en ficheros específicos establecidos al efecto, que deberán clasificarse por categorías, en función de su grado de fiabilidad.

Podríamos admitir la excepción, de acuerdo con el art 9.2 del Convenio si quedará definida la autoridad responsable del fichero.

3. La recogida y tratamiento por las Fuerzas y Cuerpos de Seguridad de los datos a que hacen referencia los apartados 2 y 3 del artículo 7, podrán

realizarse exclusivamente en los supuestos en que sea absolutamente necesario para los fines de una investigación concreta.

No es admisible por la naturaleza de los datos a que se refiere este punto, pues al tratarse de los llamados datos sensibles que tienen una protección reforzada requieren el consentimiento del afectado (vid. art. 7.2 y 3). También resulta sorprendente que se invoque "una investigación concreta, pues éstas se supone que no necesitan proceder mediante ficheros automatizados. Y en todo caso es difícil de justificar que determinados datos tengan personales íntimos tengan tal relevancia para una investigación. Consideramos que se trata de una norma contraria al art. 18.4 de la C.E, y por tanto inconstitucional.

Pero la impunidad de las Administraciones Públicas en estos supuestos se agrava, si tenemos en cuenta lo que se dispone en el art. 21.1, que por la vía de las excepciones se niega todo derecho a conocer, rectificar datos falsos o a cancelarlos.

4. Los datos personales registrados con fines policiales se cancelaran cuando no sean necesarios para las averiguaciones que motivaron su almacenamiento

A estos efectos se considerará especialmente la edad del afectado y el carácter de los datos almacenados, la necesidad de mantener los datos hasta la conclusión de una investigación o procedimiento concreto, la resolución judicial firme, en especial la absolutoria, el indulto, la rehabilitación y la prescripción de responsabilidad

7. 2 Excepciones en el ejercicio de los derechos personales.

En el Convenio se reconoce la posibilidad de excepciones y restricciones en el ejercicio de los derechos reconocidos a las personas concernidas, siempre y cuando se cumplan unas condiciones, que como hay examinábamos parten del principio de que se trate de una medida necesaria en una sociedad democrática y que se establezcan las excepciones o restricciones mediante una ley (art. 9.1.).

Art 21 - Excepciones a los derechos de acceso, rectificación y cancelación.

1. Los responsables de los ficheros que contengan los datos a que se refieren los apartados 2, 3 y 4 del artículo anterior podrán denegar el acceso, la rectificación o la cancelación en función de los peligros que pudieran derivarse para la defensa del Estado o la seguridad pública, la protección de los derechos y libertades de terceros o las necesidades de las investigaciones que se estén realizando.

Es decir que ni los datos sensibles protegidos por el art. 16.2 de la Constitución, según este apartado y el art. 20.3, quedan vacíos de derechos. La inconstitucionalidad no puede ser más rotunda.

2. Los responsables de los ficheros de la Hacienda Pública podrán, igualmente, denegar el ejercicio de los derechos a que se refiere el apartado anterior cuando el mismo obstaculice las actuaciones administrativas tendentes a asegurar el cumplimiento de las obligaciones tributarias y, en todo caso, cuando el afectado esté siendo objeto de actuaciones inspectoras.

Cabe admitirlo dentro de las excepciones contempladas en el Convenio para los intereses monetarios del Estado (art. 9.2.a).

3. El afectado al que se deniegue todo o parcialmente el ejercicio de los derechos mencionados en los apartados anteriores podrá ponerlo en conocimiento del Director de la Agencia de Protección de Datos o del Organismo competente de cada Comunidad Autónoma en el caso de ficheros automatizados mantenidos por Cuerpos de Policía propios de estos o por las Administraciones Tributarias Autonomías quien deberá asegurarse de la procedencia o improcedencia de la denegación.

Ya veremos después la incompetencia real de la Agencia de Protección de Datos para castigar las infracciones que se le prueben a las Administraciones Locales. Aquí tenemos una primera muestra de ello. No se cumple realmente el enunciado del art. 8.d) del Convenio, según el cual el afectado debe disponer de un recurso el si no es atendido.

Ponerlo en conocimiento del Director de la Agencia o del equivalente en cada Comunidad Autónoma, solo supone que este pregunte sobre la procedencia o improcedencia de la denegación, sin que ni el mismo pueda verificar la posible arbitrariedad de la respuesta. Vemos que la institución es viene dañada de origen, por su nombramiento, por su dependencia del Gobierno y por la nula

competencia efectiva en protección de datos personales, cuando de las Administraciones Públicas se trate.

Art 22 - Otras excepciones a los derechos de los afectados.

1. Lo dispuesto en los apartados 1 y 2 del artículo 5 no será aplicable a la recogida de datos cuando la información al afectado impida o dificulte gravemente el cumplimiento de las funciones de control y verificación de las Administraciones Publicas o cuando afecta a la Defensa Nacional a la Seguridad pública o a la persecución de infracciones penales o administrativas.

El derecho de información del concernido, reconocido en el art. 5.1 y 2. queda vacío de contenido con argumentos que no justifican conforme al Convenio una excepción al derecho invocado, y menos para perseguir las infracciones administrativas, que no entran dentro de las excepciones admitidas por el Convenio (art. 9).

Dificultar las funciones de control y verificación, no entran dentro de las necesidades para la protección de la seguridad del Estado democrático o de la seguridad pública, ni del orden monetario o para la represión penal. Ni siquiera los términos utilizados son suficientemente concretos, sino más bien conceptos difusos que pueden extender su campo tanto como los responsables de la Administración quieran. La arbitrariedad de la Administración para "el control y verificación" es completa. Con ello queda sin protección el contenido constitucional del art. 18.4.

2. Lo dispuesto en el artículo 14 y en el apartado 1 del artículo 15 no será de aplicación si ponderados los intereses en presencia resultase que los derechos que dichos preceptos conceden al afectado hubieran de ceder ante razones de interés público o ante intereses de terceros más dignos de protección Si el órgano administrativo responsable del fichero automatizado invocase lo dispuesto en este apartado dictará resolución motivada e instruirá al afectado del derecho que le asiste a poner la negativa en conocimiento del Director de la Agencia de Protección de Datos o en su caso del órgano equivalente de las Comunidades Autónomas.

Los argumentos de este punto son todavía mas insostenibles. El derecho de acceso a su propios datos automatizados (art. 14), y el derecho de rectificación o de cancelación, no es lícito que se pretenda anularlos como excepción

invocando "intereses, "razones de interés público", "intereses de terceros". Es decir que ya ni siquiera se invoca derechos, o razones de necesidad.

Los abstracto de los términos, y, ni siquiera cabe la relevancia de los "intereses, o de las "razones". ¿Pero que categorías son estas?. Corresponden al imperio de la arbitrariedad de los poderes públicos (art. 9.3) son contrarias al Convenio de Estrasburgo, y vulneran el arts. 18.4 y 53.1 de la Constitución, pues a los derechos protegidos no le quedaría ni su contenido esencial. La inconstitucionalidad es manifiesta.

8. Protección frente a las infracciones de las Administraciones Públicas.

Si fuera poco con la normativa de excepciones que deja casi impune los actos de la administración en el campo de la automatización de datos, incluso de los llamados sensibles, ante la hipótesis de que se le pueda atribuir alguna infracción, el Título VII, dedicado a las infracciones y sanciones, deja escasas garantías de objetividad y efectividad de las mismas.

Art 42 - Responsables.

2. Cuando se trate de ficheros de los que sean responsabilidad las Administraciones Públicas se estará en cuanto al procedimiento y a las sanciones a lo dispuesto en el artículo 45.

Art 45 - Infracciones de las Administraciones Públicas.

1. Cuando las infracciones a que se refiere el artículo 43 fuesen cometida en ficheros de los que sean responsables las Administraciones Públicas el Director de la Agencia de Protección de Datos dictara una resolución estableciendo las medidas que procede adoptar para que cesen o se corrijan los efectos de la infracción. Esté resolución se notificará al responsable del fichero al órgano del que dependa jerárquicamente y a los afectados si los hubiera.

2. El Director de la Agencia podrá proponer también la iniciación de actuaciones disciplinarias el procedieran. El procedimiento y las sanciones a aplicar serán las establecidas en la legislación sobre régimen disciplinario de las Administraciones Públicas.

3. Se deberán comunicar a la Agencia las resoluciones que recaigan en relación con las medidas y actuaciones a que se refieren los apartados anteriores.

4. El Director de la Agencia comunicará al Defensor del Pueblo las actuaciones que efectúe y las resoluciones que diste al amparo de los apartados anteriores.

Es decir que la Agencia y su Director no tienen fuerza alguna para imponer a las Administraciones Públicas unas medidas protectoras. Sólo puede "proponer", "notificar", y ser informado de lo que libremente, según su propia mecánica interna haya resuelto la Administración afectada.

Esa es la fuerza del "órgano de protección", y por si fuera poco, mediatizado desde su nombramiento por la propia Administración Pública.

9. Colofón.

Aunque no es el objeto principal de nuestro estudio actual, quede como muestra de la impunidad de la Administración prevista en la LORTAD, al dejar en manos del Gobierno excesivas potestades reglamentarias y una delegación legislativa (o también reglamentaria) que entendemos contraria a la Constitución.

La delegación reglamentaria de la Disposición final primera, se refiere a la libertad de dictar las disposiciones necesarias para regular la estructura orgánica de la Agencia de Protección de datos. Entendemos que si se pretende un órgano independiente no se puede dejar en manos del Gobierno las facultades indicadas. Mas bien corresponde regular la institución, conforme con el art. 53. 1, mediante una Ley ordinaria.

Disposición final primera.

Habilitación de desarrollo reglamentario.

El Gobierno dictará las disposiciones necesarias para la aplicación y desarrollo de la presente Ley y para regular la estructura orgánica de la Agencia de Protección de Datos.

Reiteramos el hecho de que se deja en manos del Gobierno el desarrollo reglamentario de un órgano teóricamente independiente como es la Agencia de

Protección de Datos y el Director de la misma. La supeditación gubernativa resulta evidente y descorazonadora. Cuando analicemos la institución en un próximo trabajo monográfico, estudiaremos a fondo el tema.

La delegación legislativa siguiente y /o reglamentaria, parece como justificación del aplazamiento de una de las exigencias del Convenio de Estrasburgo. Las Partes que lo suscriben, por consiguiente también a España, que lo ha ratificado, deben garantizar la protección de los derechos de las personas frente a la utilización de datos incluídos en ficheros automatizados o no. En la LORTAD por la Disposición final segunda, que reproducimos a continuación se trata de dar una respuesta a esta exigencia.

El convenio de Estrasburgo prevé que se "aplicara el presente Convenio asimismo a los ficheros de datos de carácter personal que no sean objeto de tratamientos automatizados" (art. 3.c). La LORTAD solo se refiere a los ficheros de "tratamiento automatizado". y respecto los ficheros no automatizados, solo aquellos que tengan por origen un fichero automatizado (art. 2.1). Pero la solución adoptada con esta Disposición transitoria nos parece contraria a la Constitución. Dice:

Disposición final segunda.

Extensión de la aplicación de la Ley a ficheros convencionales.

El Gobierno. previo informe del Director de la Agencia de Protección de Datos podrá extender la aplicación de la presente Ley, con las modificaciones y adaptaciones que fuesen necesarias, a los ficheros que contengan datos almacenados en forma convencional y que no hayan sido sometidos todavía o no estén destinados a ser sometidos a tratamiento automatizado.

El remate de nuestro comentario actual, es contemplar la ya citada antes, ilícita delegación legislativa o de potestad reglamentaria a favor del Gobierno que, por tratarse de derechos y libertades fundamentales, tiene que tener un tratamiento mediante Ley orgánica, conforme con los art. 81.1 y 82.1 de la C.E. También se vulnera la reserva de ley exigida por el art. 53.1 en relación con el principio de jerarquía normativa del art. 9.3 Pero además, si se trata de una delegación legislativa, tampoco se ajustaría a ley, ya que deberla concretarse un plazo para ejercitaría (art 82.3 C.E), por lo que parece más bien que se le atribuye

una potestad reglamentaria, por supuesto contraria a la jerarquía normativa y a la reserva de ley. Si inconstitucionalidad nos parece evidente.

Nos parece bien se protejan los datos personales aunque no vengan referidos en ficheros automatizados y por ello resulten probablemente menos nocivos, pero utilizando la vía legislativa correcta, y sin más aplazamientos. La indefensión de la persona frente a las Administraciones Públicas, en ficheros no automatizados, nos parece mucho mayor. invitamos al alumno a un esfuerzo contrario, mas constructivo, algo así como un anteproyecto de ley, en el que se tenga en cuenta la protección de los derechos y libertades y la protección de la Seguridad del Estado. Para ello puede tener en cuenta, aparte de la LORTAD, expurgada de sus desafueros, el repetido Convenio de Estrasburgo y, si está a su alcance, la Ley francesa de protección de datos, de 1978, que fue inspiradora de aquel Convenio, y aquellos documentos que puedan aportarle ideas, como el estudio del Prof. Mario G. Losano.

ANEXO: Artículos presuntamente inconstitucionales de la LORTAD.

Arts. inconstitucionales para el Defensor del Pueblo: 19.1, 22.1 y 2
Id. id. para el Grupo P. Popular: 6.2, 19.1, 20.3 y el 22.1 y 2.
Id. id. para la Generalidad de Cataluña: 24, 31, 39, 40.1. y 2.
Id. id. para el Parlamento Catalán: 24, 31, --- 40.1. y 2.
Id. id. según mi criterio: 5.3, 6.2, 17.1, 19.1, 20.2 y 3, 21.1, 22.1 y 2, y Disp. Final 2ª

No son a nuestro entender las únicas disposiciones inconstitucionales de la LORTAD, pero si las más importantes.

Aportación a la conferencia del Dr. Ull, por Dª Raquel Castaño Suárez, ex-alumna de Doctorado (Mérida, 18-9-97).

FICHEROS DE TITULARIDAD PUBLICA

Tribunal Constitucional:

Se regulan por la Orden de 16 de junio de 1.994, debiendo reseñarse simplemente respecto a ellos la previsión que se establece de un plazo de conservación de los datos.

En el fichero de ASUNTOS JURISDICCIONALES, los datos se conservan indefinidamente, si bien sólo se trata del nombre y apellidos de los recurrentes. Por otra parte, en el fichero de PERSONAL los datos se conservan hasta pasados 5 años desde el 30 de junio del año siguiente a aquél en que se haya causado baja el interesado. En el de SEGURIDAD, se cancelarán en un plazo de 2 años desde su obtención. Esta última disposición supera en mucho el plazo establecido por la Instrucción 1/96 de la Agencia de Protección de Datos, de 1 de marzo de 1.996.

Audiencia Provincial de Madrid:

Se regulan por el Acuerdo de 3 de diciembre de 1.996, de la Comisión Permanente del Consejo General del Poder Judicial.

Ministerio de Asuntos Exteriores:

Se encuentran regulados por las Ordenes de 22 de julio de 1.994, en la que se crean los mismos, de 26 de mayo de 1.995, en la que se establece la posible cesión de los datos contenidos en los ficheros al Instituto Nacional de Estadística a efectos estadísticos y de 18 de julio de 1.995, en la que se modifican los relativos a la Agencia Española de Cooperación Internacional, debido a la reestructuración de la misma.

Se observan las siguientes irregularidades:

-En el fichero de LICENCIADOS JUNIOR de la Agencia de Cooperación Internacional, se recogen como datos a incorporar las circunstancias sociales. ¿Cuáles son éstas? Podrán ser, como se recogen en el de Agenda del Instituto Cervantes, la pertenencia a clubes y asociaciones, lo cual es un modo de recoger datos sobre las opiniones personales que deberían ser tratados de modo especial, de acuerdo con lo señalado en el artº 20 LORTAD.

-En el caso de ACCESOS AL MINISTERIO, no se señala plazo de cancelación de los datos; debiéndose poner en relación con lo señalado en la Instrucción de la Agencia de Protección de Datos nº 1/96, que establece un plazo de cancelación de un mes (Norma Quinta).

-En el fichero de AGENDA INSTITUTO CERVANTES, se recaban también datos sobre las circunstancias sociales del afectado, mencionándose entre las mismas datos del alojamiento/vivienda, la pertenencia a clubes, asociaciones,

etc., debiéndose presentar la misma objeción que al fichero mencionado en primer lugar. Asimismo, se recogen datos con fines comerciales, a los que debería aplicarse lo señalado en el artº 29 de la LORTAD, referente a los ficheros de titularidad privada con fines de publicidad.

-Igual observación debe hacerse en relación con el fichero UNIVERSIDADES, en relación con los responsables de Departamentos de Español de Universidades extranjeras.

Como observaciones comunes, señalar que no se establecen plazos de cancelación de los datos, ni normativa que ampara el fichero, produciéndose la obtención de datos fundamentalmente a partir del propio interesado.

Ministerio de Justicia e Interior

Se encuentran regulados por las Ordenes de 26 de julio de 1.994, de 5 de diciembre de 1.994 , de 3 de abril de 1.995, y de 12 de julio de 1.996. Se pueden hacer las siguientes observaciones:

-El archivo de JUEGO está afectado por lo señalado en la Instrucción 2/96, de 1 de marzo de 1.996, que concreta la definición de responsable de los ficheros, correspondiendo la misma a los casinos explotadores del juego, estableciéndose, por otra parte, un plazo de cancelación de datos de 6 meses desde "*el último acceso*" (Norma quinta). Se supone que desde el último acceso a la sala de juego, pero la redacción es equívoca.

-El archivo ASILO, creado por la Orden de 26 de julio de 1.994, fue modificado por la Orden de 3 de abril de 1.995, incluyendo como posible cesionario de los datos a la Oficina Española del Alto Comisionado de la ONU para los refugiados. Asimismo, es uno de los afectados por el Convenio de Schengen (artículos 96 y 102).

-En el de VIGILANTES JURADOS, se establece como datos a recoger, las circunstancias sociales. ¿Cuáles? ¿No constituiría un dato sensible?

-El fichero de LICENCIA DE ARMAS, es otro de los afectados por el SISTEMA DE INFORMACION SCHENGEN.

-En el fichero PER, respecto al reparto de obras solicitadas y concedidas, al establecerse el órgano ante el que puede ejercitarse el derecho de acceso, se señala: "NINGUNO", lo que constituye una excepción a los derechos de los afectados muy importante; si este caso constituye uno de los supuestos de interés público que excepcionan el derecho de acceso, de acuerdo con lo señalado en el artículo 22 de la LORTAD, pocas materias quedarán fuera de él.

-En el fichero de CONDUCTORES (D.GRAL. TRAFICO), es curioso que se incluya un dato como el nivel de estudios.

-En el fichero CLA-GEN-OBJ (D. GRAL. DE OBJECION DE CONCIENCIA) se incluye la salud, como dato especialmente protegido.

-En los ficheros SANITARIOS y CASOSSIDA (D. GRAL. INST. PENITENCIARIAS) se recogen datos de salud, en un caso generales y en otro de afectados por HIV.

-En el fichero COMUNICACIONES (D. GRAL. INST. PENITENCIARIAS), se prevé como finalidad del mismo el control del sistema de comunicaciones de los internos, lo que supone un serio atentado al derecho de intimidad y de secreto de las comunicaciones. Lo mismo sucede con el de CONTROL DE VISITAS.

-En el fichero PERPOL no se alude al consentimiento del afectado, al recoger datos sobre la raza, salud, vida sexual, aficiones y estilo de vida, que es de suponer que se legitiman en el interés general que preside su recogida y tratamiento.

-En el fichero INVESTIGACIONES EN CURSO, se recogen todos los datos posibles de la vida de una persona, incluyendo algunos que no son usuales, examinando otros ficheros: "alojamiento y vivienda", "autorizaciones", "situación militar", etc. Lo mismo sucede en el caso del fichero de la Guardia Civil BASEFIS, que recoge como datos básicos, además de cualquier otro relevante: la formación, las titulaciones, etc.

-En la mayor parte de los ficheros de la Dirección General de la Policía, se establece como procedimiento de recogida de los datos *"la información es grabada por los gestores a partir de los asuntos tramitados"* . Esto NO es un procedimiento de

recogida de datos, sino la incorporación a un fichero de los mismos. En definitiva, no se especifica el procedimiento de recogida de los datos.

-En el fichero CONTROL PISOS ALQUILADOS, no se especifica si cualesquiera pisos arrendados pueden ser objeto de una investigación. En el capítulo de las cesiones, no se especifica nada, si se interconectara con ficheros tributarios podría constituir una fuente de información importante en materia fiscal.

-Se recogen datos sensibles en los ficheros de SALUD MENTAL e INOCULACION ACCIDENTAL.

-Los ficheros de visitas, tanto de la D. Gral. Policía y de la Dirección Gral. Guardia Civil, están afectados, como todos los de seguridad, por la Instrucción 1/96, de la Agencia de Protección de Datos.

Como sucede en la mayor parte de las disposiciones generales de creación de los ficheros, no se establecen plazos de cancelación de los datos, ni siquiera remisión a lo establecido reglamentariamente, ni la normativa reguladora que lo ampara.

En la Orden de 5 de diciembre de 1.994 se establece la cesión al Instituto Nacional de Estadística de los datos necesarios a los efectos de la Función Estadística Pública.

Ministerio de Defensa:

Los ficheros de este Departamento Ministerial se regulan en las Ordenes de 26 de julio de 1.994, 16 de enero de 1.995, que amplía la anterior, incluyendo los datos de infracciones administrativas respecto al personal civil, y de 15 de febrero de 1.996, en la que se establecen los ficheros de los Hospitales militares de Ceuta y Melilla, y del Laboratorio de Análisis Clínicos de Sevilla, señalándose en estos casos la necesidad de procedimientos de acceso restringidos, como sucede en el fichero de DATOS CLINICOS DE PACIENTES.

Son, en general, ficheros regulados de forma muy completa, dedicados en su mayoría a temas de personal, incluyéndose la normativa reguladora que los

ampara. Hay una remisión general a lo establecido reglamentariamente en lo relativo al plazo de cancelación de datos.

En el fichero SEGURO COLECTIVO DE ACCIDENTES, se establece la posible cesión de los datos personales a la entidad aseguradora adjudicataria del concurso anual, constituyendo por tanto una cesión a ficheros de titularidad privada, que plantean un problema de difícil justificación.

Los ficheros de control de visitas, como ya se ha señalado en los de otros Departamentos Ministeriales, están afectados por la Instrucción 1/96 de la Agencia de Protección de Datos.

Ministerio de Educación y Ciencia:

Regulados por Orden de 26 de julio de 1.994, y de 20 de febrero de 1.995, en esta última se establece la cesión de datos reclamados por el Instituto Nacional de Estadística con fines estadísticos. Se pueden formular las siguientes observaciones:

-En el de INVESTIGADORES (D. GRAL. INV. CIENTIFICA Y TECNICA), se incluye el "Personal en año sabático" y el "personal español en año sabático", previéndose cesiones a multitud de entidades públicas y privadas, sin excesiva concreción de los mismos.

-En el de ESPECIALIDADES EN CIENCIAS DE LA SALUD, se establece la posible cesión a asociaciones representativas en el ámbito científico, y "*terceros con intereses legítimos*". En este último caso se encuentran los de REGISTRO GENERAL DE CENTROS ESCOLARES, y REGISTRO ACTIVIDADES DE FORMACION Y MATERIAL NUEVAS TECNOLOGIAS.

-En los de GRADUADOS UNIVERSITARIOS, MATRICULADOS EN PRIMER Y SEGUNDO CICLO y MATRICULADOS EN TERCER CICLO, se prevén como datos a recabar las circunstancias sociales de los alumnos, ¿como cuáles? Es una circunstancia social los medios económicos, que no deben ser recogidos si no es en relación con petición de ayudas y becas; también lo es la pertenencia a clubes y asociaciones, pero sería absolutamente improcedente.

-Por último, en una gran cantidad de ficheros, no se indican los destinatarios de las posibles cesiones, ni siquiera negando su previsión. Así, el de

PROGRAMA ARION, PREMIOS FIN DE ESTUDIOS, PUEBLOS ABANDONADOS, PROGRAMAS DE GARANTIA SOCIAL, etc.

Instituto Astrofísica de Canarias:

Se regulan en las Resoluciones de 19 de julio de 1.994 y 7 de noviembre de 1.994 (en la que se establece la cesión al INE de los datos correspondientes a efectos estadísticos).

Consejo Superior de Investigaciones Científicas:

Se regulan en las Resoluciones de 21 de julio de 1.994 y 15 de noviembre de 1.994, que establece la cesión al Instituto de Estadística de los correspondientes datos.

Consejo Superior de Deportes:

Se regulan en las Ordenes de 20 de julio de 1.994 y 26 de octubre de 1.994, que establece la cesión al Instituto de Estadística de los correspondientes datos. Se recogen los datos médicos de los deportistas, debiéndose haber recogido la necesidad de restricciones de acceso.

Ministerio de Industria y Energía:

Fueron creados por la Orden de 26 de julio de 1.994. Se dividen entre los de servicios centrales y otros Organismos del Departamento.

En todos los ficheros, salvo en los de AYUDAS SOCIALES y SELECCION DE PERSONAL DEL CENTRO DE DESARROLLO TECNOLOGICO INDUSTRIAL, se establece la cesión "*a los órganos de las Administraciones Públicas para el desarrollo de las funciones que le encomienda el ordenamiento jurídico*" . En definitiva, para esto no era necesario que se incluyeran en las disposiciones de creación del fichero las cesiones que se previeran.

En el fichero de seguridad, que controla los accesos a los edificios públicos, ¿qué utilidad tienen las circunstancias sociales? También es aplicable la Instrucción 1/96 de la Agencia de Protección de Datos.

Muy escuetos, sólo se recogen los responsables de los ficheros, su estructura y datos, finalidades y usos y cesiones, no haciendo mención de las personas de quienes se van a obtener los datos ni el procedimiento de recogida de los mismos.

En los ficheros de la Escuela de Organización Industrial, "CLIENTES POTENCIALES" y "CONTACTOS PERSONALES", la no concreción de las personas sobre las que se deben recoger los datos, crea indeterminación.

Se recogen datos sobre la salud en los ficheros de PERSONAL DEL INSTITUTO TECNOLOGICO GEOMINERO DE ESPAÑA, SALUD LABORAL, y DATOS DOSIMETRICOS DE LOS TRABAJADORES PROFESIONALMENTE EXPUESTOS.

Ministerio de Agricultura, Pesca y Alimentación:

Se regulan por Ordenes de 26 de julio de 1.994 y de 24 de mayo de 1.997.

No se menciona la normativa que los ampara; se puede observar en primer lugar, la mención de recogida de los datos a partir de las Administraciones Públicas, no concretando si es por cesión, o por recogida de fuentes accesibles al público. Así sucede en los de ABANDONO DEFINITIVO DEL VIÑEDO, o REGISTRO VITICOLA COMUNITARIO.

Se producen transferencias internacionales de datos en lo ficheros de AYUDAS A ZONAS DESFAVORECIDAS, AYUDAS A LA INCORPORACION DE AGRICULTORES, AYUDAS A EXPLOTACIONES FAMILIARES, AYUDAS A INVERSIONES FORESTALES, CESE ANTICIPADO DE ACTIVIDAD AGRARIA, CAPITALIZACION DE EXPLOTACIONES AGRARIAS y RETIRADA DE TIERRAS DE PRODUCCION.

Ministerio de la Presidencia:

Regulados por las Ordenes de 26 de julio de 1.994 y de 14 de marzo de 1.997. Sin incluir plazo de cancelación de los datos, ni normativa reguladora, son bastante completos.

Ministerio de Administraciones Públicas:

Sus ficheros fueron creados y regulados por Orden de 22 de julio de 1.994, incluyéndose en la misma todas los requisitos legales, así como la normativa que los ampara, y la remisión al reglamento para los plazos de cancelación de los datos, etc.

Ministerio de Cultura:

Sus ficheros están regulados por las Ordenes de 22 de julio de 1.994 y de 25 de abril de 1.995, cumpliendo los requisitos legales, sino mayor información, como la normativa reguladora, ni el plazo de cancelación de los datos.

Ministerio de Sanidad y Consumo:

Se regulan por lo dispuesto en las Ordenes de 21 de julio de 1.994, 24 de noviembre de 1.995 y de 21 de octubre de 1.996. Como sucede en los ficheros de otros Departamentos Ministeriales y organismos, el procedimiento de recogida de los datos es poco claro. Así, en el fichero HISTORIAS CLINICAS se señala como procedimiento de recogida de los datos, además de los datos comunicados por el propio paciente y el personal del propio centro, por *"impresos generados por el centro"*. En algún soporte quedarán recogidas las informaciones proporcionadas por el propio paciente y el personal, pero el soporte no es un procedimiento.

En el fichero "REGISTRO DE DONANTES DE ORGANOS Y TEJIDOS", se hace la observación de que las cesiones a servicios públicos responsables de la producción de estadísticas oficiales se refieren a datos estadísticos globales y elaborados, en ningún caso, a datos particulares de un paciente o donante, lo que constituye una observación que no por obvia, es menos importante, y más tratándose de este tipo de datos necesarios de una especial protección.

Dentro de los correspondientes al Instituto Carlos III, el de GESTION DE PERSONAL, se recoge como procedimiento de recogida de datos, *"preimpresos e introducción manual de datos en el ordenador"*. Al igual que lo señalado en el de HISTORIAS CLINICAS del Mº DE SANIDAD Y CONSUMO, esto no es un procedimiento de recogida de los mismos, siendo ilógica la previsión de que el procedimiento previsto o posible en el futuro, será el mismo.

Ministerio de Asuntos Sociales:

Se regulan en la Orden de 22 de julio de 1.994 y de 22 de octubre de 1.996.

Asimismo, inciden en los mismos los Reales Decretos 758/96, de 5 de mayo, de reestructuración de Departamentos Ministeriales, que reagrupaba los Ministerios de Trabajo y Asuntos Sociales, y 1888/96, de 2 de agosto, de estructura orgánica básica.

El fichero de CONTROL DE ACCESO, está afectado por la Instrucción 1/96 de la Agencia de Protección de Datos.

En el fichero de GESTION DE PERSONAL, se prevé una especial protección a los datos de carácter personal sobre salud laboral, debiéndose haber formado un fichero independiente, para mayor garantía, con un control de acceso mínimo.

En el fichero del REAL PATR. DE PREVENCION Y ATENCION A PERSONAS CON MINUSVALIA, se establece la cesión de datos a ficheros de carácter informativo, lo que supone una indeterminación que ampararía una posible cesión a entidades de carácter privado.

Los ficheros de PERSONAL del Instituto de la Juventud, deberían tener carácter temporal en relación con los interesados, a medida que los empleados fueran jubilados, deberían ser cancelados los datos.

En el caso de los ficheros del Instituto de la Mujer de CURRICULUM DE MUJERES PROFESIONALES y de ASESORAMIENTO JURIDICO, se incluyen excesivos datos socioeconómicos, que no reúnen el principio de proporcionalidad de los datos de carácter personal, en relación con las finalidades que cumplen.

En el fichero SUBVENCIONES, se establece la cesión de los datos a Organismos públicos. ¿Cuáles?

Por último, queda señalar que la mayor parte de los ficheros del INSERSO contienen datos sensibles.

Ministerio de Comercio y Turismo:

Se encuentran regulados por la Orden de 26 de julio de 1.994.

En todos los ficheros, se relacionan como cesiones previstas, las procedentes a los órganos de la Administración Pública para el desarrollo de las funciones que les encomienda el ordenamiento jurídico.

Con excepción de los ficheros relativos a las Cámaras de Comercio, en los 22 ficheros restantes se establecen como personas o colectivos sobre los que se pretenden obtener los datos de carácter personal, o que resultan obligadas a suministrarlos, los "*funcionarios adscritos al Ministerio de Comercio y Turismo y personas relacionadas con la actividad administrativa que le compete*". Como parece obvio, pero no a juicio de los redactores de esta disposición, en los ficheros relativos a personal del Ministerio sí están obligados a proporcionar los datos los funcionarios del mismo, tanto de Servicios Centrales, como del ICEX, por ejemplo, pero no son los obligados a ello en un ejemplo tan claro como en el fichero de CONTROL DE VISITANTES. El obligado a proporcionar los datos, y sobre quien se pretenden obtener, es el tercero que accede a las instalaciones respectivas. Al igual que sucede con ficheros como el REGISTRO DE BECAS DE TURISMO, LOS ALUMNOS DE LA ESCUELA OFICIAL DE TURISMO, SUSCRIPTORES AL SERVICIO "BISE", o de las revistas del ICEX.

Por otra parte, contienen los datos imprescindibles y obligatorios en los ficheros de titularidad pública según la LORTAD.

Consejo de Estado:

Sus ficheros se regulan por la Orden de 22 de julio de 1.994.

Unicamente hacer constar que los datos relativos al fichero de DICTAMENES Y CONSULTAS se conservan indefinidamente, mientras que los relativos a nómina se conservan 5 años, como está establecido en la legislación tributaria.

Banco de España:

Se encuentran regulados en las Circulares de 22 de julio de 1.994, 25 de septiembre de 1.995, 30 de enero de 1.996, 27 de septiembre de 1.996 y 13 de junio de 1.997.

Se distinguen los ficheros que el Banco de España gestiona en atención a alguna de las funciones públicas encomendadas al mismo por la Ley 13/94, de 1 de junio, de Autonomía del Banco de España, de aquellos otros dirigidos a atender el propio funcionamiento operativo o interno de la Institución.

Pueden ser cedidos, además de lo que se establece en las disposiciones creadoras de los ficheros, a los organismos que se establecen en el artº 6 de la Ley 3/94, de 14 de abril.

Incluyen la normativa reguladora, pero no los plazos de cancelación de datos.

El fichero de GESTION DE PERSONAL contiene datos de circunstancias sociales, como pertenencia a clubes y asociaciones, lo que supone en cierto modo la inclusión de datos sobre la ideología o creencias de la persona. Asimismo, se incluyen en el de SELECCION y FORMACION, determinados datos económicos que no cumplen el principio de proporcionalidad y de adecuación al fin que deben cumplir los datos de carácter personal incorporados a un fichero.

Ministerio de Economía y Hacienda:

Se regulan por la Orden de 27 de julio de 1.994.

Encontramos un supuesto de flujo internacional de datos, en el fichero de INFORMACION DE INCENTIVOS ECONOMICOS REGIONALES, a la Comisión Europea.

El fichero de INFRACCIONES y EXPEDIENTES es un fichero con unas finalidades y usos tan genéricos, que podría englobar la información de otros muchos. Se consignan, en primer lugar, como finalidades del mismo, *"recoger los datos individuales de las personas objeto de expedientes disciplinarios o administrativos incoados por el incumplimiento de las obligaciones establecidas por la legislación vigente"*.
¿En materia de qué? En particular, se recogerán en el mismo, los médicos y psicológicos. También se recogerán datos del personal laboral expedientado, de los expedientes incoados por incumplimiento de la Ley de Estadística pública, y por la demora en la tramitación de expedientes.

Ahora bien, al recoger las personas o colectivos origen de los datos, se establece que podrán incluirse en el fichero, datos personales del personal destinado en el INE objeto de sanción administrativa y/o disciplinaria y que hayan incumplido las obligaciones de la Ley 12/89, de 9 de mayo.

Por último, señalar que se recogen datos sensibles en el fichero de reconocimientos médicos.

Agencia Estatal de Administración Tributaria:

Se regulan en las Ordenes de 27 de julio de 1.994 y de 4 de agosto de 1.995.

Hay varios casos de transferencia internacional de datos: en los ficheros de ADQUISICIONES REALIZADAS A OPERADORES INTRACOMUNITARIOS, ENTREGAS Y ADQUISICIONES A OPERADORES INTRACOMUNITARIOS, y CENSO DE OPERADORES COMUNITARIOS, con carácter parcial, a países de la Comunidad Europea, y en el caso de las DECLARACIONES DE NO RESIDENTES, a determinados Estados extranjeros en virtud de Convenios bilaterales o multilaterales de asistencia mutua. Esta cesión tendrá carácter parcial y bajo condición de reciprocidad. También se prevé la cesión de datos a órganos aduaneros internacionales de la base de datos de información SVA.

El fichero de CONTROL DE ACCESOS Y SEGURIDAD está afectado por la Instrucción 1/96, de 1 de marzo, de la Agencia de Protección de Datos.

Fábrica Nacional de Moneda y Timbre:

Se regulan en la Resolución de 22 de julio de 1.994

Ministerio de Obras Públicas, Transportes y Medio Ambiente:

Se regulan por las Ordenes de 27 de julio de 1.994 y 9 de enero de 1.996.

Se disgregarán entre el Ministerio de Fomento y de Medio Ambiente, siendo adscritos a este último los relativos a las Confederaciones Hidrográficas.

Son relativos en general a materias de personal e infracciones en materia de ley de aguas.

Es muy heterogénea la regulación en relación con los ficheros de puertos y aeropuertos. En el caso de los relativos a AUTORIDADES PORTUARIAS, casi todos son de gestión de personal, mientras que en el caso de AEROPUERTOS, en unos casos sólo integran datos de gestión de personal, mientras que en otros incorporan datos de salud laboral, y en otros se reducen a servir de justificante a las tarjetas identificativas del personal.

Sin otros problemas, no prevén plazos de cancelación de datos, agrupándose los ficheros por los órganos responsables de los mismos, y dentro de ellos, por los servicios ante quienes hacer ejercicio de los derechos de los afectados de acceso, rectificación o cancelación.

Ministerio de Trabajo y Seguridad Social:

Se encuentran regulados por las Ordenes de 27 de julio de 1.994, y 19 de mayo de 1.995, y determinadas disposiciones del Real Decreto 1.931/95, de 4 de agosto, y la Orden de 22 de febrero de 1.996.

Asimismo, inciden en los mismos los Reales Decretos 758/96, de 5 de mayo, de reestructuración de Departamentos Ministeriales, que reagrupaba los Ministerios de Trabajo y Asuntos Sociales, y 1888/96, de 2 de agosto, de estructura orgánica básica.

Aunque sin agrupar por entidades responsables de los mismos o por las unidades ante las que se podrían ejercer los derechos de acceso, rectificación o cancelación, su regulación es bastante completa.

Se diferencia en relación con las personas o colectivos personales, entre los afectados por los datos, y los obligados a suministrar los datos. Asimismo, y en relación con las cesiones, se diferencia entre las previstas a *"Departamentos, órganos, servicios de la propia Administración Pública; otras Administraciones Públicas y entidades privadas"*. A pesar de la positiva diferenciación, la terminología es inadecuada, debería haberse referido a los servicios del propio Departamento, o, como parece deducirse, a órganos del resto de la Administración del Estado.

Es elogiable asimismo la diferenciación establecida en relación con el procedimiento de recogida de datos, en el fichero de REGISTRO GENERAL, entre los afectados por los datos personales, los obligados a suministrarlos, y el procedimiento de obtención de los mismos.

Se recogen datos sensibles, sobre la salud, en el fichero de HISTORIAL CLINICO, en los relativos al SINDROME TOXICO, y los relativos a investigación de incapacidades laborales.

Comisión Nacional del Mercado de Valores:

Se regulan por Acuerdo de su órgano rector de 27 de julio de 1.994.

Consejo de Seguridad Nuclear:

Regulados por Resolución de 28 de julio de 1.994, incluyen en ellos su normativa reguladora.

En el de DATOS DOSIMETRICOS, no se prevén cesiones al tratarse de un banco de datos de acceso restringido, como corresponden a un fichero que contenga tales datos sensibles de carácter sanitario.

Respecto al de SEGURIDAD, se prevé la cancelación de los datos cuando los intereses dejen de estar en activo.

Agencia de Protección de Datos:

Se regulan en las Resoluciones de 18 de julio de 1.994 y de 7 de febrero de 1.995, no contienen previsión de cancelación de datos.

Junta Construcciones, Instalaciones y Obras:

Se regulan por Resoluciones de 29 de julio de 1.994, y 8 de noviembre del mismo año (en esta última, se contiene la cesión al INE de los datos necesarios a efectos estadísticos). Contienen los requisitos imprescindibles según la LORTAD.

Consejo Económico y Social:

Se crea un único sistema de información para su gestión, con usos múltiples, por Resolución de 31 de octubre de 1.994.

Congreso de los Diputados:

Se regulan por Acuerdo de la Mesa del Congreso de 8 de noviembre de 1.994. Como únicas notas que se deben destacar, el carácter permanente de los datos de las nóminas en el fichero de GESTION DE PERSONAL, y los datos sanitarios de HISTORIAS CLINICAS.

Defensor del Pueblo:

Se regulan por Instrucción del Defensor del Pueblo de 28 de marzo de 1.995.

Unicamente, resaltar que los datos de las QUEJAS se conservan indefinidamente, los de PERSONAL hasta pasados 5 años desde el 31 de diciembre del año en que la persona causa baja, y los de CONTROL ACCESO, se conservan durante 3 meses.

Administración de Justicia:

Regulados por Acuerdo del Consejo General del Poder Judicial de 7 de junio de 1.995, se establece la conservación indefinida de los datos, salvo en el fichero de SEGURIDAD.

Senado:

Son regulados por Acuerdo de la Mesa del Senado de 12 de julio de 1.995. Los datos en ellos incluidos se conservan con carácter permanente, salvo los relativos a GESTIONES ADMINISTRATIVAS EN RELACION CON LOS SENADORES, y el de OPOSITORES A UJIERES.

Universidades:

Se regulan en las Ordenes especificadas en el siguiente cuadro:

UNIVERSIDAD	RESOLUCION	UNIVERSIDAD	RESOLUCION
MALAGA	12-07-94	CANTABRIA	01-08-94
UNED	19-07-94	CORDOBA	27-07-94
POLIT. MADRID	27-07-94	OVIEDO	29-07-94
CARLOS III	20-07-94	LEON	31-07-94 y 28-10-94
MURCIA	27-07-94	SALAMANCA	14-09-94
EXTREMADURA	27-07-94	JAEN	26-07-94/03-02-1.997
VALLADOLID	19-07-94	SEVILLA	14-11-94
ISLAS BALEARES	22-07-94	ALMERIA	16-01-95
ZARAGOZA	27-07-94	NAVARRA	25-01-95
ALCALA HENARES	25-07-94	COMPLUTENSE	15-12-94
HUELVA	26-07-94	UN. AUT. MADRID	16-01-95
LA LAGUNA	05-08-94	VIGO	15 -08-95
CAST. LA MANCHA	29-07-94	PAIS VASCO	19-04-96
BURGOS	05-02-1.997	AUTON. BARCELONA	07-10-1.996

Refiriéndose la mayor parte de ellos a cuestiones académicas, su esquema se centra en datos de alumnado y de personal. La previsión de cesiones en las Universidades de Sevilla y Valladolid a empresas externas de grabación de datos, que no parece correcta, al entenderse que no se cede nada, sino simplemente los utilizan para incorporarlos a los ficheros universitarios.

La única transferencia internacional de datos está prevista en la Universidad de Zaragoza, en relación con el fichero de PROYECTOS DE INVESTIGACION.

Cumplen todos los requisitos legales, siendo los más completos los de la Universidad de Zaragoza, y la Complutense de Madrid.

ANEXO

TRIBUNAL CONSTITUCIONAL

-Asuntos jurisdiccionales
-Personal
-Seguridad

AUDIENCIA PROVINCIAL DE MADRID

-Personal
-Sentencias civiles

MINISTERIO DE ASUNTOS EXTERIORES

-Lista del Cuerpo Diplomático
-Becas D. Gral Relaciones Cult. y Científicas
-Archivo D. Gral Relaciones Cult. y Científicas
-Subvenciones a ONGDS
-Becas Agencia Esp. Coop. Internacional
-Nómina Agencia Esp. Coop. Internacional
-Reclutamiento licenciados expertos
-Licenciados junior
-Personal de Cooperación Exterior
-Registro de Investigadores
-Gestión de personal
-Nómina personal en España
-Nómina personal contratado en extranjero
-Control accesos
-Cuerpos de Seguridad
-Gestión de Visados
-Libro de Matrícula Consular
-Alistamiento de mozos
-Cursos Escuela Diplomática
-Participantes activ. cult. Inst. Cervantes
-Usuarios biblioteca Inst. Cervantes
-Agenda Inst. Cervantes
-Diplomas Español como Lengua Extr.

-Alumnos Instituto Cervantes
-Profesores Instituto Cervantes
-Asientos contables Inst. Cervantes
-Universidades
-Nómina Instituto Cervantes
-Consultas Instituto
-Control préstamo libros y revistas
-Inventario informático
-Españoles detenidos extranjero
-Examen intérpretes jurados
-Registros intérpretes jurados

MINISTERIO DE JUSTICIA E INTERIOR

SERVICIOS CENTRALES
-Nómina de personal
-Personal
-Consultas, quejas, recl. y suger.
-Juego
-Extranjeros
-Asilo
-N.SIS/Sirene (Schengen)
-Promotores part. políticos
-Título publicación

MUTUAL. GRAL. JUDICIAL
-Personal
-Nómina
-Afiliación
-Integradas

GOBIERNOS CIVILES
-Vigilantes jurados
-Medidas de seguridad establecimientos mercantiles e industriales
-Establecimientos Públicos
-Expedientes sancionadores
-Expulsión de extranjeros
-Infracciones Ley de Pesca

-Jurado de Expropiación Forzosa
-Personal Admón. Periférica
-Compatibilidades personal
-Administración local
-Protocolo
-Tasas de Viajeros
-Gestión Inundac. sept.-oct. 1.989
-Gestión Licencias de Armas
-Recursos situaciones de emergencia
-Drogas
-Damnificados presa de Tous
-Proveedores
-Concesión permisos y autor. extranjeros
-PER
-Explosivos
-Radioaficionados
-REMER (Red de Emergencia Provincial)
-INCENDIO
-BADARAL

D. GRAL. DE TRAFICO
-Base de datos de personas
-Base de datos de vehículos
-Escuelas de conductores
-Centros de Reconocimiento
-Expedientes de sanción
-Personal/Nómina
-Adjudicatarios
-Suscriptores Revista "Tráfico"
-Accidentes con daños personales
-Centro de Información de Tráfico
-Llamadas desde Postes SOS
-Visitas Centro de Gestión de Tráfico

D. GRAL. PROTECCION CIVIL
-Alumnos
-Profesores
-Personal
-Catálogo de recursos

-Subvenciones
-Emergencia y alerta

D. GRAL. OBJEC.CONCIENCIA
-Realiz. prest. soc. sustitutoria
-Solicitantes reconocimiento
-Incumplim. obl. prest. social
-Objetores denunciados
-Adscripción objetores
-Control objetores

D. GRAL. ADM. PENITENCIARIA
-Altos cargos
-Inventario parque informático
-Funcionarios y centros penit.
-Interinos
-Laborales
-Personal
-Prácticas
-Registro correspondencia
-Seguridad
-Compensaciones guerra civil
-Trienios
-Personal sanitario
-Libro de Servicios
-Nóminas y certificados
-Proveedores
-Biblioteca
-Protocolo y Mailing
-Gestión Oficina de Régimen
-Gestión de Ventanilla
-Vestuario
-Peculio
-Movimientos económicos internos

D.GRAL. INSTIT. PENITENCIARIAS
-Internos de especial significación
-Información población reclusa
-Prestación social sustitutoria

-Antecedentes personas que acceden a centros penitenciarios
-Alegaciones presentadas
-Comunicadores con internos
-Voluntarios y colaboradores
-Afectado virus del SIDA
-Seguimiento liberados por razones de salud
-Control enfermedades
-Autorizaciones de acceso
-Gestión de internos
-Control trabajo en talleres
-Control cursos a internos
-Salidas y permisos
-Reducciones y Cumplimiento de condena
-Comunicaciones
-Informes de Juzgados
-Contabilidad en Talleres
-Sanitarios
-Sistema de Información Penitenciario-Internos
-Sistema de Información Penitenciario-Personal
-Control de visitas
-Incursos

D.GRAL REGISTROS Y NOTARIADO
-Nacionalidad
-Registro Civil
-Actos de Ultima Voluntad
-Actas de Notoriedad

INSTITUTOS ANATOMICO-FORENSES
-Tanatológico-Forense
-Médico-Forense

CENTRO ESTUDIOS JUDICIALES
-Alumnos
-Nóminas

D. GRAL. POLICIA
-Antecedentes personas de interés pol.
-Asuntos de estudio de huellas

-Detenidos por delitos de drogas
-Tráfico drogas y blanqueo capitales
-Personal Servicio Estupefacientes
-Invest. en curso sobre drogas
-Archivo
-Inteligencia
-Prevención infracciones penales
-Balística
-Diligencias
-Documentoscopia
-Análisis
-Lofoscopia
-GRUMEN
-Prensa
-Archivo Serv. Inform. Exterior
-Ficheros Departamentales
-Solicitud nacional. española
-Control entradas por aeropurtos
-Temático documental
-Personal Comisaría Poder Jud.
-INTERPOL
-Falsificación de moneda
-Personal Brigada Delitos Monet.
-Fraudes Seguridad Social
-Delincuencia Económica
-Delitos patr. histórico-artístico
-Organizada
-Personal Servicio Central Pol. Jud.
-Desparecidos
-Invest. Servicio Central Pol. Jud.
-Bandas ADN
-Identific. cadáveres anónimos
-Documentoscopia
-Balística
-Personal Policía Científica
-Reseñas decadactilares
-Personas relación. con terrorismo
-Pisos alquilados
-Agendas telefónicas personas relacionadas con el terrorismo

-Titulares de teléfonos
-Objetos numerados de interés policial
-Titulares de permisos de conducción
-Gestión de visados de entrada en España
-Entradas súbd. extranj. por aerop. nac.
-Investigaciones Servicios de Información
-Gestión de dicha información
-Gestión archivo Servicio Inform. Ext.
-Control personas según Acuerdo España-EE.UU.
-Entradas y salidas extranj. no comunitarios
-Expedición pasaportes españoles
-D.N.I. Archivo óptico
-D.N.I. Archivo Magnético
-Permisos de residencia de extranjeros
-Solicitudes certificación de residencia
-Permisos de conducir
-Exped. acad. alumnos Centro de Formación
-Notas personal D.G.P.
-Prof. Centro Especialización
-Control armas particulares funcionarios
-Cursos del personal
-Gestión alumnos Centro Especialización
-Control armas D.G.P.
-Profesores Centro de Formación
-Gestión personal de cada centro
-Automatización ficheros manuales
-Revistas policiales
-Distintivos funcionarios
-Asistencia letrada a funcionarios
-Sanciones administrativas
-Personal adscrito a la D.G.P.
-Indemniz. por traslado
-Nómina funcionarios D.G.P.
-Control vehículos oficiales
-Documentación sanitaria
-Facultativos dependientes
-Datos reconocimientos médicos
-Informes psiquiátricos funcionarios
-Contactos de riesgo de salud

-Accidentes en acto de servicio
-Reclam. admvas de orden económico
-Liquidación y pago a S.S. y Hacienda
-Gastos cursos de especialización
-Calificaciones de estudios externos
-Registro documentos
-Control cursos especialización
-Cursos de idiomas
-Control de accesos
-Acceso a parkings
-Gastos de profesorado
-Informatización biblioteca
-Control uniformidad
-Actualización lista de alumnos
-Procesos selectivos
-Alumnos Centro Formación
-Méritos académicos
-Ayuda social
-Representantes con crédito horario
-Teléfonos intervenidos
-Control de detenidos
-Informes y gestiones
-Actuación unidades segur. ciudadana
-Personal plantillas periféricas
-Inmigración ilegal demarc. periféricas
-Personas de interés demarc. periférica
-Investigación delitos demarc. periférica
-Inv. movimientos sometidos a control

D. GRAL. GUARDIA CIVIL
-Indemnizaciones
-Dietas
-Horas nocturnas
-Conductores
-Tarjeta identificación profesional
-Patronato
-Mutua
-Sanidad
-Haberes

-Recursos Nómina
-Haberes Personal Civil
-Retenciones Judiciales
-Nómina Medallas
-Abonos
-Ayudas
-Residencias
-Visitas
-Exámenes
-Acción social
-Gastos comunes
-Gestión personal
-Revista
-Estudios
-Auxiliares
-Solicitudes
-Petición
-Asuntos internos
-Boletín Oficial del Cuerpo
-Deportes
-Destinos
-Expedientes Disciplinarios
-Socorros Mutuos
-Transportes
-Barcos
-Incidencias Artefactos explosivos
-Seguridad ciudadana
-Instalaciones
-Estrecho
-Fronteras
-Armas
-Helicòpteros
-Base de datos Señalamientos Nacionales
-BASEFIS (operaciones en prevención de blanqueo de dinero y narcotráfico)
-OPERFIS (investigaciones en relación con contrabando, blanqueo de dinero y narcotráfico)

MINISTERIO DE DEFENSA

-Personal militar Tierra
-Personal militar Armada
-Personal militar Aire
-Personal militar Fuerzas Comunes
-Personal civil
-Servicio militar y Militares Empleo
-INVIFAS
-ISFAS
-Pensiones militares
-Recursos
-Seguro colectivo accidentes
-Accidentes personal Defensa
-Datos clínicos de pacientes
-Gestión nóminas Organo Central
-Gestión nóminas Tierra
-Gestión nóminas Armada
-Gestión nóminas Aire
-Identificación personal Organo central
-Identificación personal Estado Mayor
-Ident. pers. Cuartel Gral. Tierra
-Ident. pers. Cuartel Gral. Armada
-Ident. pers. Cuartel Gral Aire
-Visitas Organo Central
-Visitas Estado Mayor Defensa
-Control visitas Ejército Tierra
-Visitas Cuartel General Aire
-Intervención Armas Ministerio
-Interv. armas ejército Tierra
-Interv. armas Armada
-Interv. armas ejército Aire
-Asoc. Mutua Benéfica Armada
-Suscriptores B.O.D.
-Suscriptores revistas Defensa

MINISTERIO DE EDUCACION Y CIENCIA

-Personal
-Becas y ayudas
-Títulos
-Concursos de traslados
-Concursos-oposición
-Direcciones provinciales
-Centros docentes
-Evaluación investigadores
-Investigadores D.Gral. Inv. Cient. y Técnica
-Colaboraciones y comis. serv. D. Gral. Invest.
-Especialidades en Ciencias de la Salud
-Personal Secr. Estº Univ. e Invesstig.
-Personal docente universitario
-Graduados universitarios
-Matr. univ. 1º y 2º ciclo
-Matr. univ. de tercer ciclo
-Investigadores Plan Nac. I+D
-Investigadores proyectos org. supranac.
-Altos cargos y expertos I+D
-Colaboradores I+D
-Contratistas transporte escolar
-Becas colaboración
-Reclamaciones de becas
-Verificación y control solicitudes de becas
-Ayudas para cursos de verano de idiomas
-Programa ARION
-Premios fin de estudios universitarios
-Premio Giner de los Ríos
-Pueblos abandonados
-Educación permanente y a distancia
-Form. Perm. Profesorado
-Directiva General
-Control presencia personal
-Recursos vía admva. y jurisd.
-Registro general centros escolares

-Intercambio profesores UE
-Cooperación bilateral
-Títulos
-Cooper. educativa con Iberoamérica
-Cooper. científica con Iberoamérica
-Rég. econ.-admvo. formación sobre nuevas tecnologías
-Actividades de formación nuevas tecnologías
-Programas de garantía social
-Licencias por estudios
-Becas programa LINGUA
-Personal centros
-Pagos de formación al profesorado
-Becas del Consejo de Europa
-Ayudas individuales formación profesorado
-Títulos extranjeros no universitarios

INSTITUTO ASTROFISICA CANARIAS

-Nómina de personal
-Pagos y cobros a terceros
-Compras

CONSEJO SUPERIOR DE DEPORTES

-Deportistas y técnicos de alto nivel
-Investigadores y centros de investigación
-Formación posgraduados
-Reconocimiento médico a deportistas
-Ayudas y subvenciones a la investigación deportiva
-Gestión de Recursos Humanos
-Dirección
-Biblioteca
-Nómina estándar
-Vida administrativa del personal
-Control horario

CONSEJO SUPERIOR INVESTIGACIONES CIENTIFICAS

-Base de datos corporativa
-Base de datos de Red de Area Local
-Sistema de gestión informatizada

MINISTERIO DE INDUSTRIA Y ENERGIA

SERVICIOS CENTRALES
-Personal
-Cursos informáticos
-Ayudas sociales
-Seguridad
-Gestión de concursos de traslado
-Caja Pagadora
-Registro de entrada/salida
-Control horario
-Tarjetas de identificación
-Incompatibilidades
-Isótopos radiactivos
-Registro de gasolineras

CENTRO DESARROLLO TECN.-IND.
-Recursos humanos
-Selección de personal
-Proveedores
-Proyectos CDTI
-Subvenciones
-Proyectos internacionales

INST. DIVERS. AHORRO ENERGIA
-Clientes-proveedores
-Control de presencia y visitas
-Retribuciones
-Servicios Generales
-Personal

-Control horario

OFIC. ESP. PATENTES Y MARCAS
-Personal

ESC. ORGAN. INDUSTRIAL
-Personal
-Colaboradores
-Alumnos
-Clientes potenciales
-Contactos personales

INST. TECN. GEOMINERO ESPAÑA
-Personal
-Ventas
-Pagos
-Registro
-Catastro Minero Nacional
-Datos bibliográficos

CENTRO INV. ENERG., MEDIOAMB. Y TECN.
-Recursos humanos del CIEMAT
-Control horario
-Nómina
-Becas
-Datos dosimétricos trabajadores expuestos
-Salud laboral
-Cursos Inst. Estudios Energía

INST. PEQUEÑA Y MED. EMP. INDUST.
-Nómina de personal
-Control horario
-Bases de datos SIBILA/SIE
-Solicitantes inform. bases de datos
-Organismos intermedios
-Solicitantes de información al IMPI
-Coordenadas empresariales
-Empresas afianzadas

MINISTERIO DE AGRICULTURA, PESCA Y ALIMENTACION

-Nómina
-Recursos humanos
-Personal
-Recursos administrativos
-Nómina Inst. Fomento Asoc. Agrario
-Sociedades agrarias de transformación
-Seguro colect. Inst. Fomento Asoc. Agrario
-Recursos Humanos Inst. Fomento
-Personal Cámaras Agrarias
-Directorio titulares explot. agrarias
-Nómina Agencia Aceite de Oliva
-Personal Agencia Aceite de Oliva
-Oleicultores
-Ayuda producción aceite de oliva
-Ayuda consumo aceite de oliva
-Información seguros agrarios
-Seguros agrarios
-Fichero oleícola informatizado
-Directorio industrias agroalimentarias
-Explotaciones ganaderas
-Red contable Agraria Nacional
-Personal INIA
-Becarios del INIA
-Registro vitícola comunitario
-Ayudas industrialización agraria
-Ayudas mejora transf. y comercial.
-Registro Oficial Maquinaria Agrícola
-Abandono definitivo viñedo
-Contratos semillas
-Productores plantas de vivero
-Productores de semillas
-Registro de variedades
-Contratos multiplicación de semillas
-Recursos sobre cuotas lecheras
-Asignación cuotas lecheras

-Indemn. por peste porcina africana
-Nómina SENPA
-Control visitas SENPA
-Cuotas producción agraria
-Tasas y producción láctea
-FEOGA-Garantía
-Ingresos y pagos SENPA
-Retenciones judiciales
-Ayudas estructurales pesqueras
-Censo y armadores y propietarios
-Titulaciones náutico-pesqueras
-Titulares y tripul. caladeros marroquíes
-Nómina Inst. Esp. Oceanografía
-Personal Inst. Esp. Oceanografía
-Gestión económica Inst. Esp. Oceanografía
-Nómina Inst. Nal. Reforma y Desar. Agrario
-RR.HH Inst. Nal. Reforma y Desar. Agrario
-Personal Inst. Nal. Reforma y Desar. Agrario
-Auxilio mutuo personal IRYDA
-Historiales médicos personal IRYDA
-Entidad colaboradora Seg. Social
-Reintegro préstamos IRYDA
-Subv. mejora de explotaciones
-Ayudas desarrollo rural integrado
-Ayudas medidas agroambientales
-Gestión de pagos ICONA
-Anilladores de aves de ICONA
-Pilotos ICONA
-Superficies sembradas de algodón
-Retirada tierras de producción
-Cese anticipado actividad agraria
-Capitalización explotaciones agrarias

MINISTERIO DE LA PRESIDENCIA

SUBSECRETARIA
-Control de Presidencia

SECRETARIA GENERAL

-Actividades

D.GRAL. SECRETARIADO
-Altos Cargos
-Miembros Consejos Administración
-Altos Cargos Comun. Autónomas
-Solic. acceso Archivo Central
-Publicaciones oficiales

D. GRAL. SERVICIOS
-Personal
-Condecoraciones
-Recursos
-Nóminas

JEFATURA DE SEGURIDAD
-Accesos complejo Moncloa

SECR. GRAL. PORTAVOZ
-Agenda de la Comunicación
-Acreditación

BOLETIN OFICIAL DEL ESTADO
-Control de presencia
-Gestión de personal
-Gestión económica personal
-Suscripciones
-Control anuncios B.O.E. y B.O.R.M.
-Compras y ventas de libros

CENTRO DE EST. CONSTITUC.
-Clientes
-Derechos de autor
-Gestión publicaciones periódicas
-SICAI
-Nómina de personal
-Badaral (gestión de personal)
-Profesores y alumnos
-Usuarios

CENTRO INVESTIG. SOCIOLOGICAS
-Gestión de personal
-Nómina de personal
-Pagos a entrevistadores
-Envío de boletines
-Peticiones de información
-Suscripción de publicaciones

Cº ADMON. PATRIM. NACIONAL
-Acceso Palacio Real
-Control horario personal
-Nómina
-Personal
-Terceros sujetos a retenc. IRPF
-SICAI
-Inmuebles
-Suscriptores
-Difusión

-Comunicaciones pendientes
-Respuestas a ciud. desde 16-05-1986
-Comunic. recibidas desde 16-05-1986
-Comunic. recibidas hasta 16-05-1986

MINISTERIO DE ADMINISTRACIONES PUBLICAS

-Directivos
-Permisos sindicales
-Funcionarios de Admón local con habilitación de carácter nacional
-Archivo óptico func. Admón. local con habil. de carácter nacional
-Altos cargos, directivos y predirectivos Admón. del Estado por videotex
-Idem sobre red de área local
-Expedientes de personal sobre soporte óptico
-Registro Central de Personal de jubilados y fallecidos
-Registro Central de Personal con fines estadísticos
-Ocupación de puestos de trabajo
-Participantes pruebas selectivas en Adm. del Estº, S.S. y A.E.A.T.
-Peticiones de destino en concursos unitarios

-Nómina jubilados AISS
-Gestión descentr. rec. humanos
-Directores Grales. Admón Gral.
-Registro Central de Personal con fines estadísticos
-Peticiones de destino func. nuevo ingreso
-Participantes pruebas select. Admón. Gral., S.S., y A.E.A.T. para inf. pública
-Registro Central de Personal
-Directivos, empleados publ. y empresas del sector de las comunic.
-Registro de intereses de altos cargos
-Incompatibilidades
-Archivo Central MAP
-Datos de visitantes
-Datos económicos del personal
-Formación y perfeccionamiento
-Datos de acción social de empleados públicos
-Concursos de funcionarios
-Relaciones de puestos de trabajo
-Control de asistencia de personal
-Datos BADARAL
-Datos incluidos en disco óptico
-Inventario b. inmuebles patronato Casas Func. Civiles
-Nómina personal MAP

INST. ADMON. PUBLICA
-Personal, colaboradores INAP y func. en prácticas
-Suscriptores revistas editadas por el INAP
-Personal INAP
-Opositores
-Usuarios centro estudios Peñíscola
-Alumnos cursos perfeccionamiento
-Visitantes

MUFACE
-Colectivo MUFACE
-Prestaciones MUFACE
-Cotizantes Fondo General MUFACE
-Fondo Especial MUFACE
-Cotizantes Fondo Esp. MUFACE
-Personal MUFACE

-Nóminas MUFACE

MINISTERIO DE CULTURA

GABINETE MINISTRO

-Personalidades relevantes
-Permanencia de personal
-Gestión económica

D.GRAL. SERVICIOS
-Retribuciones
-BARADAL
-Gestiones administrativas
-Contratos RD 1465/85 y D. 1505/74
-Control de expedientes
-Seguimiento obras
-Proyectos
-Seguridad. Control de visitas
-Historiales. Inf. médica

D. GRAL. BELLAS ARTES
-Usuarios Arch. Hco. Vizcaya
-Usuarios Arch. Gral. Admón.
-Usuarios Sección Guerra Civil
-Usuarios Arch. Hco. Nacional
-Usuarios Arch. Gral. Indias
-Usuarios Sección Nobleza
-Usuarios Arch. Gral. Simancas
-Usuarios Arch. Real Chancill. Valladolid
-Exportación bienes culturales
-Importación bienes culturales
-Salidas bienes culturales
-Compras bienes culturales
-Titularidad bienes culturales
-Donaciones
-Pago deudas trib. con bienes culturales
-Costes exposiciones
-Temporal.DBF

-Jubilados.DBF
-Arquitectos y aparejadores
-Asuntos propios
-Personal

D. GRAL. LIBRO Y BIBLIOTECAS
-Patr. Bibliogr. Español
-Traductores españoles
-Autores españoles

CINEMAT. Y ARTES AUDIOVISUALES
-Materiales Filmoteca Española
-Actividades cine Doré
-Ayudas a tramitación de expedientes
-Fichero técnico-artístico
-Expedientes administrativos
-Gestión económica
-Censo salas cinematográficas
-BADARAL
-Temas de cine en el País Vasco
-Relación de actores
-Retribuciones
-Abonos actuaciones Orquesta y Coro de España
-Boletín Compañía Nacional Teatro Clásico
-Abonados Teatro Zarzuela
-Personal Inst. Nal. Artes Escénicas

MUSEO DEL PRADO
-BARADAL

CENTRO ARTE REINA SOFIA
-Gestión de Recursos Humanos
-Actividad Org. Autónomo

BIBLIOTECA NACIONAL
-Lectores
-Personal

INST. NAL. ARTES ESCENICAS

-Recursos Danza en España
-Recursos Musicales en España

MINISTERIO DE SANIDAD Y CONSUMO

FICHEROS DE CARACTER SANITARIO

D. GRAL. SERVICIOS E INFORMATICA
-Usuarios Tarjeta Sanitaria

D. GRAL. FARMACIA Y PROD. SANIT.
-Import. y suministro medic.
extranjeros

INSTITUTO CARLOS III
-Morbilidad pacientes síndrome tóxico
-Enfermedades de Decl. Oblig.
-Registro Nacional de SIDA
-Registro Estatal de LEPRA
-FEDRA (Reg. reacciones diversas)
-Seguimiento de Clozapina
-Registro Nacional de de Enfermedad de Creutzfeldt-Jacob
-Casos de Haemophilus Influenzae

D.GRAL. SALUD PUBLICA
-Interrupción voluntaria del embarazo

D.GRAL. ASEG. Y PLAN. SANITARIA
-Altas hospitalarias

CENTRO NAC. DOSIMETRIA
-Banco Historiales Dosimétricos

INSALUD
-Población protegida
-Usuarios del sistema sanitario
-Historias clínicas
-Valoración de incapacidades

-Gestión de prestación farmacéutica
-Inc. Lab. Trans. e Invalidez Prov.
-Gestión y control de prestaciones
-Base de datos proyecto multicéntrico de Invest. sobre Tuberculosis

ORG. NAL. DE TRASPLANTES
-Registro de donantes

FICHEROS DE CARACTER ADMINISTRATIVO

D. GRAL. SERVICIOS E INFORMATICA
-Personal

D. GRAL. ORDENACION PROFESIONAL
-Residentes
-MIR
-Médicos generalistas
-Directivos

ESCUELA NAL. DE SANIDAD
-Gestión de personal
-MAILING

INST. CARLOS III
-Ayudas formación y perf. I+D
-Ayudas proyectos de investigación

D. GRAL. FARMACIA Y PROD. SANITARIOS
-Facturación de recetas
-Instalaciones farmaceúticas

INST. NAL. DE CONSUMO
-Gestión de personal

INST. NAL. CARLOS III
-Gestión de personal

D. GRAL. ASEG. Y PLAN. SANITARIA
-Contratos de servicios médicos

D. GRAL. ALTA INSPECCION
-Directivos Administr. Sanitaria

INSALUD
-Personal Instituciones Sanitarias
-Gestión de personal
-Personal Direcciones Provinciales
-Reclamaciones y Demandas
-Personal sanitario de Empresa

D.GRAL. SALUD PUBLICA
-Censo de Instalaciones de Radiodiagnóstico, Radioterapia y Medicina Nuclear

MINISTERIO DE ASUNTOS SOCIALES

DEPARTAMENTO
-Control de acceso de visitantes
-Personal Ministerio Asuntos Sociales
-Fichero de contabilidad
-Distribución instit. de publicaciones
-Suscriptores publ. periódicas
-Permisos de trabajo a extranjeros
-Permisos de trabajo extr. regularizados
-Contingente anual inmigrantes
-Excepciones de permisos de trabajo
-Solicit. participación viajes tercera edad emigrantes
-Pensiones asist. emigrantes esp. de ancianidad
-Asist. sanit. emigrantes y familias
-Registro demandantes empleo en exterior
-Subv. con cargo al 0.52 por 100 IRPF
-Subv. rég. gral. acción social
-Base de datos patronatos fundaciones
-Subv. área infancia y familia
-Menores deprotegidos y menores infractores
-Formación centro de estudios del menor
-Subv. rég. gral área de migraciones

REAL PATR. PREV. Y ATENCION MINUSVALIDOS

-Personas relacionadas con atención a discapaces

INSTITUTO DE LA JUVENTUD
-Datos personal Instituto Juventud
-Juventud y medio ambiente
-Servicio voluntario internacional
-Subv. INJUVE/Solicitud subvenc.

INSTITUTO DE LA MUJER
-Curriculum mujeres demandantes empleo
-Personal
-Asesoramiento jurídico
-Publicaciones
-Subvenciones

INSERSO
-Personal
-Prestaciones Ley 7/82, 13 de abril
-Beneficiarios prest. no contributivas
-Reconoc. condición minusválido
-Ingresos en resid. geriátricas
-Ingresos en resid. minusválidos
-Programa vacaciones 3ª edad
-Sorteos viajes a Canarias
-Gestión programa termalismo
-Beneficiarios ayuda a domicilio
-Oferta empleo público
-Suscripciones a public.
-Proveedores bienes y servicios
-Ingenieros y Arquitectos Superiores
-Fichero IRPF no incluidos en plantilla

MINISTERIO DE COMERCIO Y TURISMO

-Nóminas
-Nóminas personal exterior
-Nóminas personal Secr. Gral. Turismo
-Nóminas personal ICEX

-Gestión de personal
-Gestión de personal Secr. Gral. Turismo
-Gestión de personal ICEX
-Control visitantes
-Registro Directores Establ. Turísticos
-Registro de becas de Turismo
-Alumnos Escuela Oficial de Turismo
-Alumnos y personal docente del ICEX
-Personal colaborador ICEX
-Proveedores
-Biblioteca
-Control de presencia del personal
-Control de visitantes
-Usuarios base de datos empresas comercio exterior
-Suscriptores al servicio BISE
-Suscriptores revistas del ICEX
-Comunicación de novedades editoriales
-Censo empresas Cº Sup. Cámaras Oficiales Comercio, Ind. y Navegación
-Censo público empresas Cº Sup. Cámaras Oficiales Comercio
-Censo electoral
-Recaudación Recurso Cameral Permanente

CONSEJO DE ESTADO

-Consultas remitidas y dictámenes solicitados al Consejo de Estado
-Nóminas

BANCO DE ESPAÑA

FICHEROS GESTIONADOS EN VIRTUD DE FUNCIONES PUBLICAS
-Central de Información de Riesgos
-Balanzas y trans. econ. con el exterior
-Altos cargos de entid. inscr. en el Banco de España
-Reclamaciones
-Central anotaciones deuda pública

COMISION DE PREVENCION DEL BLANQUEO DE CAPITALES E INFRACCIONES MONETARIAS

-Control de actuaciones previas
-Datos correspondientes a las Declaraciones de Operaciones sobre Blanqueo de capitales
FICHEROS DE CARACTER INTERNO U OPERATIVO
-Operaciones cuentas corrientes
-Reg. y Libros aux. de sucursales
-Operaciones exteriores
-Cambios moneda extranjera
-Gestión personal
-Selección y formación de personal
-Personal residenc. y proveed. economato y residencias
-Servicios médicos de empresa
-Proveed. y clientes servicios no financieros
-Acceso físico a edificios
-Suscriptores del servicio de publicaciones
-Biblioteca

MINISTERIO DE ECONOMIA Y HACIENDA

SECR. ESTADO ECONOMIA
-Gestión de personal Gabinete
-Gestión de personal de la D. Gral. Defensa de la Competencia
-Gestión de expedientes
-Control de empresas
-Inversiones extranjeras en España
-Inversiones esp. en exterior (salvo valores negociables)
-Inv. valores negociables calificables como inv. esp. en el exterior
-Exp. sanc. inf. admvas en control de cambios
-Gestión de personal D. Gral. Incentivos Econ. y Region.
-Información de Incentivos Econ. Regionales
-Entidades de Seguros
-0101 y 0201 trimestral y anual
-Registros de corredores de seguros
-Sociedades de correduría de seguros
-Altos cargos de Entidades de Seguros
-Socios de sociedades de Correduría de Seguros
-Peritos tasadores, Comisarios averías y Liquidadores averías
-Fondos de pensiones, Entidades gestoras y Depositarias y Actuarios
-Documentación estadístico-contable fondos

-Expedientes sancionadores en seguros privados
-Consultas y reclamaciones
-Personal D. Gral. de Seguros
-Productividad
-Diario de Caja D. Gral. de Seguros
-Gestión de personal D. Gral del Tesoro
-Depósitos en metálico y valores
-Domicilios
-Publicidad de Deuda Pública
-Gestión de Deuda Pública
-Perceptores de transferencias
-Apoderados
-Multados por inf. defensa competencia
-Exped. Defensa Competencia
-Gestión de personal D. Gral. Defensa Comp.
-Distrib. gratuita, suscriptores y "mailing"
-Revista estadística española
-Asistentes cursos Escuela Estadística
-Encargados cursos Escuela Estadística
-Proveedores de bienes y servicios
-Personal I.N.E.
-Consejo Superior de Estadística
-Comité interterritorial de estadística
-Comisión Interministerial de Estadística
-Datos sanitarios y atención individualizada
-Infracciones y expedientes

SECR. ESTº DE HACIENDA
-Personal D. Gral. Pol. Tributaria
-Consultas
-Registro
-Imp. esp. sobre bienes inmuebles
-Publicaciones
-Personal D. Gral. Control Presupuestario
-SIGECA
-Personal D. Gral. de Servicios
-Opositores al CSIFE
-Opositores al Cuerpo de Gestión
-Declarantes del IRPF y Patrimonio

-Empresas declarantes
-Empresas
-Envío de publicaciones
-Colaboradores Inst. Est. Fiscales
-Datos personales Inst. Est. Fiscales
-Personal Inst. Est. Fiscales
-Personal Secr. Gral. Planif. y Pres.
-Colaboradores en formación
-Organos ejecutores
-Personal D. Gral. Planificación
-Autoriz. venta tabaco en estab. merc.
-Personal Interv. Gral. Adm. Estado
-Terceros de SICOP
-Sujetos pasivos de Deleg. de Hacienda
-Personal D. Gral. Presupuestos
-Personal D. Gral. Inf. Presupuestaria
-Centro de control de servicios
-Control horario
-Base de datos de direcciones
-Productividades del personal
-Recursos Area Jurídica Administrativa
-Datos personal actual Centro Direc.
-Datos personal pasado Centro Direc.
-Habilitados
-Gestión clases pasivas
-VIH
-Historiales Tribunal Médico
-Mutilados Clases pasivas
-Errores de nómina de Habil. Clases pasivas
-Indemnización por tiempo de prisión

SUBSECRETARIA
-Arrendamiento a inmuebles
-Personal D. Gral. Planificación
-Ayudas Acción social
-Reconocimientos médicos
-Adjudicatarios contratos
-Reclamantes y recurrentes
-Entrada y salida de documentos

-Seguridad
-Terceros
-Inquilinos
-Pacientes
-Personal Parque Móvil
-Caja de Socorro
-Nómina Parque Móvil
-Nómina
-Personal Instituto de Contabilidad
-Suscripciones
-Solicit. insc. Reg. Ofic. Audit. de Cuentas
-Registro Oficial Auditores de Cuentas
-Gestión económica
-Empresas ofertantes
-Registro de Contratos
-Empresas clasificadas
-Empresas suministradoras b. muebles
-Personal D. Gral. Patr. del Estado
-Inmovilizado material
-Red de ventas ONLAE
-Gestión de personal del Mº
-Personal Secr. Gral. Técnica
-Suscriptores Publ. Mº Econ. y Hac.
-Distribuidores publicaciones
-Recursos administrativos
-Indemnizaciones Ley 19/90

AGENCIA ESTATAL DE ADMON. TRIBUTARIA

-Rentas de capital mobiliario
-Transmisión valores mobiliarios
-Titulares de cuentas sin N.I.F.
-Adquisiciones a operadores intracomun.
-Entregas a operadores intracom.
-Fondos de inversión
-IBI-Rústica
-IBI-Urbana
-Transmisiones patrimoniales

-Altas, bajas y transfer. de vehículos
-Socios y consejeros de sociedades
-Autorizados en cuentas banc. de soc.
-Cuentas bancarias
-Planes y Fondos de pensiones
-Cesiones de crédito
-Seguros de prima única
-Letras del Tesoro
-Tráfico de divisas
-Fichas de inspección
-Titulares de cheques bancarios
-Pagos del Tesoro
-Anotaciones
-Censo de Actividades Económicas
-Decl. anuales operaciones con terceras personas
-Decl. anual retenc. trabajo personal
-Decl. de no residentes
-Actas de inspección
-Recursos
-Devolución de ingresos indebidos
-Autoliquidaciones
-Centro de contribuyentes en módulos
-Censo de contribuyentes
-Censo de obligados tributarios
-Sistema integrado de recaudación. Garantías
-Sist. integr. recaud. Exped. aplaz./fraccion.
-Sist. int. recaud. Diligencias de embargo
-Sist. integr. recaud. Deuda
-Sist. integr. recaud. Responsables
-Sist. integr. recaud. Deudores
-IVA. Exportadores
-Impuesto sobre el Patrimonio
-Impuesto sobre el Valor añadido
-Impuesto sobre la Renta de las Personas Físicas
-Imp. esp. determinados medios transporte
-Censo obligados de Impuestos Especiales
-Documentos de producción años 1.993 y 1.994
-Documentos producción años 1.986-1.992
-Censo de operadores comuntarios

-Garantías de importación
-DUA
-Base de datos información SVA
-Registro/ seguimiento de expedientes
-Actos Jurídicos documentados
-Procedimiento Inspector
-Fallecimientos
-Matrimonios

-Censo operadores INTRASTAT
-Personal AEAT
-Proveedores
-Censo de usuarios
-Control de accesos
-Seguridad
-Expedientes de compatibilidad

F.N.M.T.

-Persona
-Seguridad
-Terceros

Mº OBRAS PUBLICAS, TRANSPORTES Y MEDIO AMBIENTE

D. GRAL. PROGRAM. ECON. Y PRES.
-Estadística edific. viviendas
-Estadísticas autónomos construcción

SECRET. GRAL. TECNICA
-Títulos académicos
-Recursos
-Rec. contencioso-admvos
-Distribución de catálogos
-Suscriptores "MOPT"
-Suscriptores "Ciudad y Territorio"
-Suscriptores "Estudios del Transporte"

D.GRAL. RECURSOS HUMANOS
-Personal funcionario
-Personal laboral fijo
-Personal lab. eventual
-Personal caminero
-Acción social
-Concursos
-Gestión nóminas
-Datos bancarios
-Seguridad social
-Histórico general

D. GRAL. ADMON. Y SERVICIOS
-Proveedores a suministros
-Proveedores (gestión financiera
-Pagos por caja
-Cajeros
-Gestión Area Seg. Norte
-Gestión Area Seguridad Sur
-Reclamaciones y Recursos
-Tarjetas de acceso
-Incidencias de personal
-Prendas de vestuario
-Control de presencia

D. GRAL. VIVIENDA
-Apoyos bancarios a la vivienda
-Amortización de créditos
-Ayudas económicas a la vivienda
-Préstamos

D.GRAL. INST. NAL. METEOROLOGIA
-Gestión de personal

D. GRAL. ACT. CONCERT. EN CIUDADES
-Hogares-personas-viajes

SECR. GRAL. DE COMUNICACIONES
-Empleados

-Trienios
-Personal funcionario (registros públ.)
-Personal funcionario
-Tarjetas acceso
-Laboral
-Interinos
-Nóminas

SUBD. GRAL. ORDEN. COMUNICACIONES
-Registro de empresas con actividad postal
-Autorización servicios cartas y tarjetas postales

D. GRAL. TELECOMUNICACIONES
-Licencias radioaficionado
-Exped. sancionadores
-Infracciones televisión por cable
-Infrac. homologación terminales
-Reclamaciones serv. telefónico
-Personal
-Accionariado televisión privada
-Sistemas de telecomunicación
-Sistemas de gestión de recursos
-Personal funcionario rég. MUFACE
-Personal funcionario rég. gral.
-Personal laboral
-Personal interino

D. GRAL. MARINA MERCANTE
-Expedientes
-Empresas
-Titulados
-Proveedores

D. GRAL. AVIACION CIVIL
-Personal laboral
-Personal funcionario
-Personal adscrito
-Histórico de personal
-Aeronaves

-Identificación provisional
-Registro datos técnicos aeronaves
-Aspirantes
-Personal de vuelo
-Técnicos mantenimiento aeronáutico
-Reclama
-Compañía
-Licencias pilotos aviación deportiva

D. GRAL. INFRAESTR. TRANSPORTE FERROVIARIO
-Personal
-Licitadores
-Expropiaciones

CONFED. HIDROGRAFICA DUERO
-Nómina funcionarios
-Nómina laborales
-Registro de salida
-Registro de entrada
-Infracciones Ley de Aguas
-Regantes y Tasas
-Canon de regulación
-Vertidos

CONFED. HIDROG. EBRO
-Nóminas personal
-nóminas
-Dietas laborales
-Personal temporal
-Personal laboral
-Salud laboral
-Personal funcionario
-Nóminas funcionario
-Nóminas funcionarios (S.S.)
-Dietas funcionarios
-Aprovechamiento aguas superficiales
-Denuncias y sanciones
-Solicitudes aprovechamiento
-Aprovechamiento aguas subterráneas

-Tasas
-Proveedores
-Expropiaciones
-Indemnizaciones

CONF. HIDRO. SUR DE ESPAÑA
-Maestro de personal
-Maestro de cuentas
-Maestro de observaciones
-Regantes
-Fichas Ley de Aguas
-Inscripciones registro de agua

CONF. HIDRO. GUADALQUIVIR
-Censo de usuarios
-Tomas de agua en el Genil
-Usos de aguas
-Nómina

CONF. HIDRO. GUADIANA
-Aprovechamiento e instalaciones
-Lista cobratoria concesiones
-Liquidaciones concesiones
-Ensayos de laboratorio
-Lista cobratoria ensayos
-Liquidaciones de ensayos
-Certificaciones de obra
-Lista cobratoria certificaciones
-Liquidaciones de certificaciones
-Proyectos de comisaría
-Lista cobratoria proyectos
-Liquidaciones de proyectos
-Usuarios de informes
-Lista cobratoria usuarios de informes
-Liquidaciones de informes
-Canon de vertido
-Lista cobratoria canon
-Sanciones
-Lista cobratoria sanciones

-Liquidaciones sanciones
-Abastecimiento zona ind. Huelva
-Lista cobratoria zona ind. Huelva
-Liquidac. abastec. industr. Huelva
-Regadíos Palos de la Frontera
-Lista cobratoria regadíos Palos
-Liquidac. regadíos Palos
-Regadíos Cartaya
-Lista cobratoria regadíos Cartaya
-Liquidaciones regadíos Cartaya
-Regadíos Zújar
-Liquidaciones regadíos Zújar
-Regantes
-Lista cobratoria riegos oficiales
-Liquid. riegos oficiales
-Sueldos
-Datos mes
-Datos fijos funcionarios
-Transferencia
-Datos variables laborales
-Transferencia
-Propietarios de pozos
-Gestión de pozos
-Consulta propietarios
-Expediente de expropiación
-Consulta de fincas
-Consulta de propietarios

CONFED. HIDRO. JUCAR
-Devengos
-Expedientes
-Tasas
-Personal

CONFED. HIDRO. SEGURA
-Personal funcionario
-Personal laboral
-Apremios de pago
-Propietarios expropiados

-Ingresos
-Suministradores
-Registro aprovechamiento agua
-Vertidos
-Registro aprovechamiento
-Registro entrada-salida
-Captación aguas subterráneas

CONFED. HIDRO. NORTE
-Autorizaciones de vertido
-Aprovechamiento aguas
-Expedientes
-Ingresos
-Laboral-personal-hijos

CONFED. HIDRO. TAJO
-Recaud. en vía ejecutiva
-Beneficiados cheques bancarios
-Nómina
-Operaciones económico-patrimoniales
-Aprovechamientos (descentr.)
-Aprovechamientos (central)
-Bienes dominio público hidráulico
-Expedientes sanción
-Boletines denuncia
-Bienes dominio público hidráulico

MANCOMUNIDAD CANALES DEL TAIBILLA
-Proveedores
-Sección recreativa
-Ofertas y contratos
-Personal

CENTRO ESTUDIOS
-Datos personales

CENTRO NAL. INFORM. GEOGRAF.
-Nóminas

CENTRO ESP. METROLOGÍA
-Pagos baja cuantía
-Proveedores
-Nómina
-Personal
-Movimientos contables

O. A. CORREOS Y TELEGRAFOS
-Solicitudes de empleo
-Personal laboral
-Personal funcionario
-Personal

DELEG. GOB. EN TELEFONICA
-Reclamaciones tarificación telefónica
-Servidumbres servicio telefónico

RETEVISION
-Base de datos de personal

PUERTOS DEL ESTADO
-Nómina
-Nómina pensiones
-Personal

AUTOR. PORT. DE ALICANTE: Empleados
AUTOR. PORT. DE ALGECIRAS: Nóminas
AUTOR. PORT. DE ALMERIA MOTRIL: Personal
AUTOR. PORT. DE AVILES: Personal
AUTOR. PORT. DE BALEARES: Personal
AUTOR. PORT. DE BARCELONA
-Ficha médica
-Personal
-Multas
-Retenciones indirectas
AUTOR. PORT. DE BILBAO
-Personal
AUTOR. PORT. DE CADIZ
-Personal

AUTOR. PORT. DE CARTAGENA
-Personal
AUTOR. PORT. DE CASTELLON
-Personal
AUTOR. PORT. FERROL-SAN CIPRIAN
-Personal
AUTOR. PORT. GIJON
-Personal
AUTOR. PORT. HUELVA
-Personal activo
-Personal pasivo
-Demandas de empleo
-Usuarios
-Proveedores
AUTOR. PORT. LAS PALMAS
-Personal
AUTOR. PORT. MALAGA
-Personal
AUTOR. PORT. MELILLA
-Personal
-Usuarios
AUTOR. PORT. SEVILLA
-Personal
AUTOR. PORT. TARRAGONA
-Maestro de Personal
AUTOR. PORT. VIGO
-Personal
AUTOR. PORT. VILLAGARCIA
-Nómina
-Usuarios
AUTOR. PORT. CEUTA
-Personal
AUTOR. PORT. PASAJES
-Nóminas y liquidaciones
AUTOR. PORT. SANTANDER
-Nómina
AUTOR. PORT. MARIN-PONTEVEDRA
-Personal
AUTOR. PORT. VALENCIA

-Nóminas
-Usuarios
-Maestro de proveedores
AUTOR. PORT. SANTA CRUZ DE TENERIFE
-Nómina
-Incidencias de personal
-Nómina
AUTOR. PORT. LA CORUÑA
-Trabajadores
-Montepío
-Proveedores
-Usuarios

DEMARC. COSTAS CANTABRIA
-Gestión de personal
DEMARC. COSTAS ASTURIAS
-Funcionarios
DEMARC. COSTAS GALICIA
-Tramitación nóminas
DEMARC. COSTAS ANDAL. MEDIT.
-Nóminas
DEMARC. COSTAS ANDAL. ATLANTICO
-Gestión de personal
DEMARC. COSTAS MURCIA
-Personal
DEMARC. COSTAS VALENCIA
-Nóminas
DEMARC. COSTAS CATALUÑA
-Nóminas
DEMARC. COSTAS BALEARES
-Nóminas
DEMARC. COSTAS CANARIAS
-Nómina
DEMARC. COSTAS HUELVA
-Personal
DEMARC. COSTAS ALMERIA
-Nómina
SERVICIO COSTAS PONTEVEDRA
-Personal

SERVICIO COSTAS LUGO
-Personal

SOC. EST. PROM. Y EQUIP. SUELO
-Empleado
-Proveedores
-Clientes

AEROP. ESPAÑOLES
-Básico
-Archivo filiación
-Personal
-Incidencias mensuales en nómina
-Datos personales y económicos
-Generación fichero del mes
-Procesos anuales
-Pago de nómina en cinta magnética
-Resúmen anual ret. e ingresos a cuenta
-Nómina
-Personal (otras remuneraciones)
-Laboral
-Controla
-Persomto
-Personal trabajadores región balear
-Región canaria: turnos
-Región canaria: incidencias en turnos
-Región centro: datos administrativos y personales
-Región centro: archivo y control de pacientes

AEROPUERTO ALICANTE
-Personal
AEROPUERTO ALMERIA
-Personal
-Medicina laboral
AEROPUERTO ASTURIAS
-Trabajadores
AEROPUERTO BARCELONA
-Trabajadores
-Nóminas y altas

-Tarjetas identificativas
AEROPUERTO BILBAO
-Personal
-Histclin
-Seguridad
AEROPUERTO FUERTEVENTURA
-Personal
AEROPUERTO GERONA
-Confección de nóminas
AEROPUERTO GRANADA
-Personal
AEROPUERTO IBIZA
-Tarjetas personal fijo
-Tarjetas personal eventual
-Tarjetas visitantes
AEROPUERTO LANZAROTE
-Tarjetas
-Personal
AEROPUERTO BARAJAS
-Recursos Humanos
AEROPUERTO MALAGA
-Tarjetas acceso
-Nómina mes
-Plantilla
-Incap. lab. transitoria
-Coches
-Agencias
-Vehículos con conductor
-Vehículos sin conductor
AEROPUERTO MENORCA
-Tarjetas identificativas
-Cálculo nóminas
-Relación nominal empleados
AEROPUERTO PALMA MALLORCA
-Fichas audiométricas
-Asistencia sanitaria
AEROPUERTO PAMPLONA
-Control de presencia
-Control accesos

-Personal: uso administrativo
-Personal laboral
-Pago de nóminas
AEROPUERTO DE SALAMANCA
-Censo
-Direcciones
-Nombre y apellidos personal
AEROPUERTO DE TENERIFE SUR
-Seguridad
-Parking personal
-Control presencia personal
-Tarjetas de identificación
-Trabajadores
AEROPUERTO DE VALENCIA
-Servicio médico
-Pago nómina
-Control personal
-Control autorización personal
AEROPUERTO DE VITORIA
-Seguridad
AEROPUERTO DE ZARAGOZA
-Maestro de empleados

MINISTERIO DE TRABAJO Y SEGURIDAD SOCIAL

-MINIS
-NOVAL
-Gestión de Recursos
-Registro General
-Aparcamiento de vehículos
-Guía teléfonos
-Sistema de gestión del gasto
-Sistema de gestión integrada de personal
-FPN 156-A (Control de accesos)
-Historial clínico
-Control de recensiones
-Control de devolución de tasas
-Distrib. Bol. Inform. Sociolaboral

-Programa de Estudio
-Distrib. Revista Econ. y Sociología Trabajo
-A.G.C. Editoriales
-Gestión de bibliotecas. Lectores
-Gestión de bibliotecas. Proveedores
-Laboral
-Almacenamiento en disco óptico. Activos
-Base de datos BADARAL (Personal)
-Recursos
-Oposiciones
-Docente
-Concurso
-Cursos
-Sistema de inform. de personal
-Denuncias y reclamaciones
-Compatibilidades
-FOGASA
-Prestac. socioeconóm. síndrome tóxico. Reintegros
-Prestac. socioeconóm. síndrome tóxico.
-Prest. síndrome tóxico. Prestaciones
-Prest. síndrome tóxico. Ayuda domiciliaria
-Prest. síndrome tóxico. Fichero social familiar
-Prest. síndrome tóxico. Reinserción social individ.
-Prest. síndrome tóxico. Reinserción: estudio previo
-Sist. de inform. contable centros gestores
-Sistema informático FOGASA
-Datos personales trabajadores FOGASA
-AETP. Accidentes sin baja médica
-AETP. Altas o fallecimientos
-AETP. Enfermedades profesionales
-Apertura de centros de trabajo
-AETP. Accidentes con baja médica
-Permisos de trabajo a extranjeros
-Censo de afectados por el síndrome tóxico
-Proveedores de FOGASA
-Inspectores y controladores laborales
-Personal admvo. de Inspec. Prov.
-Sistema de gestión de personal
-Sistema de gestión de cajas pagadoras

-Expedientes de sanciones y liquidaciones
-Actas de liquidación
-Sistema de Gestión de Inspección MTS12.ACT
-Sistema de Gestión de Inspección MTS20. ACT
-Horas 94
-Reordenación minera
-Protocolo. Director
-Control de accidentes de trabajo
-Elecciones sindicales
-UMAC. Conciliaciones
-Direcciones secretaría particular
-ENRPROC. Ayudas equivalentes a jubil. en empresas no sujetas a reconversión
-Elecciones sindicales
-Mediación, arbitraje y conciliación.
-Sanciones Dirección General de Empleo
-Nómina Inst. Nal. de Fomento Econ. Social
-Revista Inst. Nal. de Fomento Econ. Social
-Subv. Desarrollo Economía social: jóvenes
-Subv. Desarrollo Economía social: gerentes
-Subv. Desarrollo Economía social: socios
-Préstamos concedidos por extinto Fondo Nacional de Prot. al trabajo
-Gestión control presupuestario cooperativo
-Personal IFES (Inst. Fom. Econ. Soc.)
-Personal y nóminas
-Publicaciones
-Compras
-Direcciones
-BADARAL
-Etiquetas
-Estibadores
-Nómina personal laboral trab. portuarios
-Nómina funcionarios trab. portuarios
-Sist. información lab. desempleo. Prestaciones
-Sist. inform. empleo. Empleadores
-Sist. inform. empleo. Oficinas de empleo
-Sist. inform. empleo. Demandas
-Sist. inform. empleo. Ofertas
-Recaud. cobros indebidos < 10.000 ptas.
-Recaud. cobros indebidos (salvo Desempleo)

-Sistema de Información de Pagos. Ficha de terceros
-SICAI. Subsistema de terceros
-Retenciones judiciales
-Contratación laboral. Contratos y prórrogas
-Contratación laboral. Subvenciones
-Personal Inst. Nal. de Empleo
-Gestión interna INEM
-Docentes y expertos INEM
-Alumnos INEM
-Profesores Escuelas Taller
-Nómina expertos
-Alumnos Escuela Taller
-Archivo-Registro
-Gasto contrato con Mutuas de Accidentes
-Cargos Mutuas de Accidentes
-Inspec. colaboradores mutuas

INSTITUTO NAC. SEG. SOCIAL
-Directivos INSS
-Pagos con retención a cuenta IRPF
-Personal INSS
-Gratificaciones y productividad INSS
-Serv. extra. funcionarios y horas pers. laboral
-Ejec. sentencias
-Productividad
-Control de presencia
-Personal
-Base de datos INSS
-Licencias
-Cursos realizados INSS
-Laboral fijo INSS
-Socorro fallecimiento
-Pluses familiares
-Recursos Acción Social
-AGORA
-Comisiones de servicio
-Exped. funcionarios
-Altos cargos provincias
-Personal eventual

-Traslados
-Resolución concursos.LARGO
-Resolución concursos.MATRIZ
-Resolución concursos. QUIENES
-Resolución concursos. QUE
-Personal
-Defunciones
-Pago de pensiones públicas
-Pago convenios internacionales
-Banco Pensiones públicas
-Gestión prestac. Seg. Social
-Inform. hca. IRPF
-Incap. lab. transitoria
-Protección familiar
-Pensiones públicas
-Pensionistas
-ILT personal INSS
-Productividad personal
-Expedientes de personal
-Reingresos personal
-Servicios previos
-Ayudas de acción
-Productividad tareas específicas
-Ciudad residencial vacaciones PERLORA
-Hojamar
-Gestión plantillas de personal
-Complem. pensión jubilados INSS
-Hist. sanitario trabajadores mar
-CM9 TDS1
-Afil. trabaj. e inscrip. empresas mar
-Nómina personal Inst. san. ISM
-Personal Instituciones san. ISM

-Funcionarios Intervención Seg. Soc.
-Afiliación trabajadores e insc. empresas
-Bases de cotización.
-Fichero general de recaudación
-Base de datos de terceros
-Situaciones administrativas del personal

-Datos de personal general
-Gestión de demandas en el Juzgado de lo Social
-Pago subsidio ILT
-Pago pensiones devengadas y no recibidas
-Convenios internacionales
-Mayores de cincuenta y dos años
-Control de presencia
-Direcciones provinciales INSS
-Gestión de personal Direcciones Provinciales
-Facturas proveedores Direc. Provinciales
-SERVIMED. Historiales médicos
-Registro de correo
-AGORA. Sistema informático
-Investigación accidentes
-Remuneración personal laboral Reino Unido
-Base de datos colonia español Reino Unido
-Familias y niños asistentes a guarderías infantiles en Londres

COMISION NACIONAL DEL MERCADO DE VALORES

-Cargos
-Personal sociedades y agencias, no público
-Proveedores, clientes, suscriptores C.N.M.V.
-Personal C.N.M.V.
-Selección de personal
-Reclamaciones
-Requerimientos
-Expedientes sancionadores

CONSEJO DE SEGURIDAD NUCLEAR

-Banco dosimétrico
-Licencias
-Personal

AGENCIA DE PROTECCION DE DATOS

-Gestión de recursos humanos
-Nómina estándar

JUNTA DE CONSTRUCCIONES, INSTALACIONES Y EQUIPO ESCOLAR

-Nómina de personal
-Pagos y cobros a terceros

CONGRESO DE LOS DIPUTADOS

-Documentación
-Biblioteca
-Archivo
-Publicaciones
-Nómina Cortes Generales
-Nómina Congreso
-Gestión administrativa parlamentarios
-Gestión de personal
-Acreditaciones Congreso Diputados
-Protección social
-Historias clínicas
-Acreditaciones medios com. Social
-Asuntos jurisdiccionales

DEFENSOR DEL PUEBLO

-Entradas
-Personal
-Control de entradas

ADMINISTRACION DE JUSTICIA

-Fichero carrera judicial
-Gestión de personal
-Nómina

-Seguridad
-Recursos
-Publicaciones
-Expedientes disciplinarios

SENADO

-Personal en nómina
-Proveedores
-Gestión de personal
-Acreditaciones del Senado
-Acreditaciones de prensa
-Fichero de Senadores para gestión administrativa
-Fichero de Senadores para gestión parlamentaria
-Fichero de iniciativas y expedientes parlamentarios
-Archivo
-Solicitudes documentación
-Solic. Docum. dirigidas al Dpto. de Documentación
-Solicit. documentación dirigidas al Servicio de Doc.
-Solicit. documentación al Dpto. Est. Comunitarios
-Biblioteca
-Personas presentadas a oposición de ujieres
-Control de entrada al Senado
-Historias clínicas
-Gestión de publicaciones

FICHEROS UNIVERSIDADES PUBLICAS:

UNIVERSIDAD DE MALAGA:
-Selectividad
-Preinscripciones
-Alumnos
-Becarios
-Personal
UNIV. NAL. EDUC. A DISTANCIA:
-Gestión de personal
-Gestión académica
-Gestión económica
UNIV. POLITECNICA DE MADRID:

-Alumnos
-Personal
UNIV. CARLOS III DE MADRID:
-HOMINIS: Gestión integral RRHH
-SIGMA: Gestión académica
-COU
-Becas
-SICAI (Gestión económica)
-SAVIA (Gestión de proyectos de investigación)
-EVALOS (Presencia personal)
-Tercer ciclo
-Biblioteca
-Competiciones deportivas
UNIVERSIDAD DE MURCIA:
-Personal
-Retribuciones
-Becas
-Alumnos
-Investigadores
UNIVERSIDAD DE EXTREMADURA:
-Personal
-Pruebas de acceso a la Universidad
-Admisión
-Matrícula (1º y 2º ciclo)
-Becas
-Títulos universitarios oficiales
UNIVERSIDAD DE VALLADOLID:
-Alumnos
-Personal
-Contabilidad
UNIVERSIDAD ISLAS BALEARES:
-Gestión de personal y nómina:
-Proveedores y clientes
-Títulos
-Alumnos
-Becas
UNIVERSIDAD DE ZARAGOZA:
-Estudiantes
-Profesores/ponentes

-Usuarios instalaciones deportivas
-Nóminas
-Personal
-Residentes en el CMU "Santa Isabel"
-Residentes en el CMU " Pedro Cerbuna"
-Personal, prfesionales y empresarios relacionados con proyectos de investig.
-Control de acceso
-Gestión administrativa de la investigación
-Alumnos extranj. de cursos de español
-Primer y segundo ciclos y títulos
-Tercer ciclo
-Estudiantes de estudios propios de la Universidad
-Estudiantes del Instituto de Idiomas
-Programa ERASMUS
-Programa LINGUA
-Programa EUROPEAN CREDIT TRANSFER SYSTEM
-Estudiantes extranjeros acogidos
UNIVERSIDAD ALCALA DE HENARES
-COU/PAU
-Alumnado 1º y 2º ciclo
-Tercer ciclo
-Estudios propios
-Gestión de recursos humanos
-Gestión económica
-Gestión de la investigación
-Gestión bibliotecaria
-Gestión de deportes
UNIVERSIDAD HUELVA:
-Profesorado y personal administración y servicios
-Alumnos matriculados
-Alumnos que pretenden acceder a estudios universitarios
-Alumnos que solicitan beca
UNIVERSIDAD LA LAGUNA:
-Gestión académica
-Personal
-Gestión económica
UNIVERS. CASTILLA LA MANCHA:
-Gestión académica
-Personal y nóminas

UNIVERSIDAD DE CANTABRIA:
-Alumnos y títulos
-Personal y nóminas
UNIVERSIDAD DE CORDOBA:
-Alumnos matriculados en primer, segundo y tercer ciclo
-Alumnos que han solicitado beca
-Alumnos que acceden a la Universidad
-Personal
-Proveedores
UNIVERSIDAD DE OVIEDO:
-Personal
-SIDRA (Gestión académica)
-Acceso
-Becas
-SICAI (Gestión económica)
-Investigación
-Tercer ciclo
-Biblioteca
-Estudios de Posgrado
-Departamento Biología funcional
-Escuela de Estomatología "ESTO"
-Escuela de Estomatología "GESCON"
-Escuela de Estomatología "DENTIBUS"
UNIVERSIDAD DE LEON:
-Personal
-Nóminas
-Estudiantes
-Becas
-Estudiantes 3° ciclo y Postgrado
-Tercer ciclo
-SICAI
UNIVERSIDAD SALAMANCA:
-Personal colaborador
-Alumnos
-Becarios
-Contratistas
-Acreedores
-Usuarios servicios universitarios
UNIVERSIDAD DE JAEN:

-Selectividad
-Preinscripción
-Alumnos
-Becarios
-Personal
-Terceros
UNIVERSIDAD DE SEVILLA:
-Alumnos
-Personal
UNIVERSIDAD DE ALMERIA:
-Personal docente
-Administración y servicios
-Alumnos
-Datos económicos e investigación
UNIVERSIDAD DE NAVARRA:
-Gestión recursos humanos
-SIGMA (Gestión académica)
-COU
-Becas
-Gestión económica
-Control de presencia
-Tercer ciclo
-Biblioteca
-Gestión retribuciones
UNIVERSIDAD COMPLUTENSE:
-Personal docente
-Personal administración y servicios (rég. admvo.)
-Personal administración y servicios (rég. laboral)
-Nómina
-Seguridad social y derechos pasivos
-Proveedores
-Gaceta complutense
-Retribuciones por asistencia a tribunales y comisiones de servicio
-Investigación
-COU y pruebas acceso
-Admisión distrito único Madrid
-Admisión distrito compartido
-Matriculación 1º y 2º ciclo
-Becas y ayudas al estudio

-Doctorado
-Títulos
-Usuarios biblioteca
UNIVERSIDAD AUTONOMA MADRID:
-SIGMA (Gestión académica)
-Personal/nómina
-SICAI: gestión económica
-COU
-Becas
UNIVERSIDAD DE VIGO:
-Alumnos
-Personal
-Contabilidad
UNIVERSIDAD PAIS VASCO:
-Arkhe Area académica
-Arkhe Area Personal
-Arkhe Area económica
-Arkhe Area Patrimonio
UNIVERSIDAD BURGOS:
-Alumnos
-Personal
-Contabilidad
UNIVERSIDAD LA RIOJA:
-Alumnos
-Personal
-Datos económicos
-Biblioteca

BIBLIOGRAFIA

Carrascosa López, V.: "La Ley Orgánica de Regulación del Tratamiento Automatizado de Datos de carácter personal", en "LA PROTECCION DE LOS DATOS PERSONALES. REGULACION NACIONAL E INTERNACIONAL DE LA SEGURIDAD INFORMATICA". Centre d'Investigació de la Comunicació i Universitat Pompeu Fabra. Barcelona,1.993.

Gay Fuentes, C.: "Intimidad y tratamiento de datos de las Administraciones Públicas". Madrid, 1.995. Editorial Complutense.

Herrero Tejedor, P.: "Honor, intimidad y propia imagen". Madrid, 1.990. Editorial COLEX.

Lucas Murillo de la Cueva, P.: "El derecho a la autodeterminación informativa". Madrid, 1.990. Editorial TECNOS.

Lucas Murillo de la Cueva, P.: "Informática y protección de datos personales". Madrid, 1.993. Centro de Estudios Constitucionales. Colección Cuadernos y debates.

Molina Mateos, J.M.: "Seguridad informática y poder: una perspectiva conceptual y jurídica de la criptología". Madrid, 1.994. Incipit Editores.

Pérez-Luño, Antonio E.: "La protección jurídica de los derechos personales en España". Volumen colectivo: "Estudios jurídicos en honor a José Gabaldón López". Madrid, 1.990. Edit. Trivium.

Ruiz Miguel, C.: "El derecho a la intimidad informática en el Derecho español", en REVISTA GENERAL DEL DERECHO. Abril-1.995.

Velázquez Bautista, R.: "Protección jurídica de los datos personales automatizados". Madrid, 1.993. Editorial COLEX.

Vilariño Pintos, E.: "La LORTAD ante el Derecho internacional", en"LA PROTECCION DE LOS DATOS PERSONALES. REGULACION NACIONAL E INTERNACIONAL DE LA SEGURIDAD INFORMATICA". Centre d'Investigació de la Comunicació i Universitat Pompeu Fabra. Barcelona,1.993.

Contratación Informática

EDUARDO RODRÍGUEZ DE CASTRO

Abogado, especialista en Derecho Informático. Profesor U.N.E.D. Mérida

I.- INTRODUCCION A LA CONTRATACION INFORMATICA

La Informática ha adquirido una importancia decisiva, no sólo en el mundo especializado de las grandes computadoras, sino también en nuestra vida cotidiana, lo que nos puede llevar a afirmar con ANTONIO MARTINO[1] que estamos ante la decadencia de la sociedad industrial en favor de la sociedad informatizada o sociedad de la información.

El Derecho, como regulador de la conducta social del individuo, no podía ser ajeno a esta realidad, viéndose por ello influenciado de una manera determinante por la Informática y demás avances tecnológicos.

De esta forma, la Informática ha ido calando en el mundo jurídico, no solo en sus aspectos prácticos, sino que como elemento determinante de nuestras relaciones, se presenta como una realidad a tratar por el Derecho.

■[1] ANTONIO MARTINO.- "La Informática Jurídica Hoy", citado por PEDRO MARTIN BARDI en su Ponencia "Derecho de la Informática. Contratos Informáticos".

Cuanto mayor es el avance tecnológico que vamos alcanzando, mayor es la ineficacia o insuficiencia de nuestra normativa para solventar los problemas jurídicos que van apareciendo. De esta forma, la informática ha creado una parcela, con características y necesidades propias, que nuestras viejas leyes no siempre satisfacen suficientemente.

Vemos pues, la conveniencia de que el Derecho Informático, como parte del Derecho que aborda todos los problemas jurídicos que se suscitan como consecuencia de la Informática, se estudie con la independencia y profundidad que exigen las actuales circunstancias.

Consideramos imprescindible para comenzar el tema de nuestra Ponencia "Los Contratos Informáticos", hacer una breve precisión terminológica sobre conceptos, que pueden llevar a confusión por la liberalidad con que en ocasiones se utilizan.

Como primer acercamiento al concepto de Derecho Informático, podemos definirlo como la rama del Derecho, o si se prefiere, la parte del Derecho, que trata problemas relacionados con la materia informática.

Pero nuestra precisión debe profundizar más y así compartimos la clasificación que EMILIO DEL PESO NAVARRO[2] hace al distinguir Derecho Informático o Derecho de la Informática ,de la Informática Jurídica. En el primer caso la propia Informática es el objeto del Derecho, mientras que con el término Informática Jurídica, estamos considerando la Informática como herramienta de nuestra actividad.

Dentro de esta faceta del Derecho, un aspecto clave es el que se refiere a la materia contractual. Así la contratación informática se presenta como una parte de este sector del Derecho, que merece especial consideración.

De nuevo, nos vemos obligados a hacer una precisión terminológica para poder determinar el objeto de nuestro estudio ya que también en el ámbito

■[2] EMILIO DEL PESO NAVARRO.- "Análisis Jurídico desde una perspectiva informática. La contratación Informática". Revista Actualidad Informática Aranzadi.Núm. 14. Enero 1.995.

contractual, la Informática se presenta en su doble aspecto de objeto y herramienta.

Se denomina contratación informática a los contratos de bienes y/o servicios informáticos, incluyendo los relativos a las bases de datos[3].

En contraposición a la llamada contratación informática en sentido estricto, tenemos la llamada contratación electrónica o por medios electrónicos que el Profesor DAVARA[4] define como aquélla que con independencia de cual sea su objeto, que puede también ser la Informática, aunque no necesariamente, se realiza a través o con ayuda de los medios electrónicos, que no tienen por qué ser siempre ordenadores.

Aún estando plenamente de acuerdo con los anteriores conceptos, compartimos la posición de SALVADOR DARÍO VERGEL[5], que pone de manifiesto la prudencia con que debemos acercarnos a estos contratos, ya que, por regla general, el término "contratación informática" se presenta en una doble acepción: en un sentido amplio, incluiría tanto la contratación sobre bienes o servicios informáticos, como la realizada a través de estos medios; y en un sentido estricto se limitaría al primero de estos grupos de contratos.

Nuestro estudio se centrará en la contratación informática en sentido estricto, cuya clave estará en el objeto sobre el que recae, que siempre serán bienes y/o servicios relacionados con la Informática, lo que nos obliga ineludiblemente a abordar estos conceptos.

Son bienes informáticos[6] todos aquellos elementos que forman el sistema

■[3] ISABEL HERNANDO.- "Contratos Informáticos (Consideraciones Generales)". Segundas Jornadas de la Abogacía e Informática. Barcelona 21-22 Abril 1.994. Ilustre Colegio de Abogados de Barcelona.

■[4] MIGUEL ANGEL DAVARA RODRIGUEZ .- Derecho Informático. Primera Edición. 1.993. Editorial Aranzadi..

■[5] SALVADOR DARIO VERGEL.- "Contratos Informáticos en el Derecho Privado". Revista Informática y Derecho 8. UNED Centro Regional de Extremadura. Mérida 1.995.

■[6] MIGUEL ANGEL DAVARA RODRIGUEZ.- Derecho Informático. Primera Edición 1.993.

-ordenador- en cuanto al hardware, ya sea la unidad central del proceso, o sus periféricos, y todos los equipos que tienen una relación directa de uso con respecto a ellos y que en su conjunto, conforman el soporte físico del elemento informático, así como los bienes inmateriales que proporcionan las órdenes, datos, procedimientos e instrucciones en el tratamiento automatizado de la información y que, en su conjunto, conforman el soporte lógico del elemento informático. Los servicios informáticos serían todos aquellos que sirvan de apoyo y complemento a la actividad informática, en su relación de afinidad directa con ella.

II.- CONCEPTO DE CONTRATO INFORMATICO.

Partiendo de la definición de GHERSI que concibe la contratación informática como aquellas operaciones jurídicas, por las cuales se crean, modifican o extinguen relaciones obligacionales sobre bienes o servicios informáticos, se plantea el problema de la razón de ser de esta categoría de contratos, o dicho de otra forma, de la diferencia entre la contratación informática y la contratación ordinaria y de las dificultades que presenta su estudio[7].

Ciertamente, como señala SALVADOR DARIO VERGEL[8], puede discutirse la categoría de contrato informático, pero no puede ponerse en tela de juicio la existencia de una problemática común que requiere una solución de conjunto. Podemos encontrar algunas notas propias de este tipo de contratos, y otras que, sin ser propias de éstos, se caracterizan por el hecho de referirse a la materia informática[9].

Editorial ARANZADI.

■[7] Consideramos contratación ordinaria aquella que independientemente de su naturaleza civil o mercantil, no recaiga sobre bienes y/o servicios informáticos.

■[8] SALVADOR DARIO VERGEL.- Obra ya citada

■[9] GOMEZ-ACEBO Y POMBO en su ponencia "Cómo protegerse de los riesgos derivados de las cláusulas abusivas en los contratos de hardware y software".- Institute for International Research España.- Madrid 1.994. Afirman que los contratos informáticos tienden a ser considerados una categoría autónoma de contratos, puesto que en virtud del principio de la autonomía de la voluntad, las partes intentan dar una regulación compleja al objeto de la transacción.

Con ello, no defendemos la total desconexión de estos contratos y el intento de una regulación que parta de cero, pero sí debemos ser conscientes de que, basándonos en nuestra legislación, hemos de ir más allá del mero intento de ajustarlos de una forma absoluta, a unos cánones que, en muchos casos, se alejan de su propia naturaleza. Una defectuosa regulación contractual, y así una imprecisa contratación, puede conllevar unas consecuencias económicas mucho más importantes que la mera reducción a sus propios costes. El ámbito negocial en materia informática debe ser objeto de una minuciosa precisión que las partes acaban solventando, en algunos casos, con un muy prudente ejercicio de la autonomía de la voluntad. Pero insistimos, la posición clave y fundamental que ocupa la Informática en la sociedad y todos sus aspectos contractuales, merecen una particular atención por parte de nuestro legislador, quien no debe desentenderse de sus peculiaridades, remitiéndose única y exclusivamente a la legislación vigente. Ciertamente nuestro ordenamiento jurídico es la línea de partida, pero en muchos aspectos contractuales que la moderna tecnología provoca, no puede ser la línea de llegada.

El jurista que accede al estudio de este tipo de contratación, se encuentra con importantes dificultades derivadas de la especificidad de sus aspectos técnicos, la particularidad de su vocabulario, y la estructura compleja que revisten muchos de ellos[10].

El estudio concreto de la contratación informática, nos exige partir del tratamiento de los tipos contractuales ya existentes en nuestra normativa, descubrir sus características, intentando dar respuesta a los problemas que plantean con nuestra propia legislación, ayudados de la interpretación jurisprudencial y doctrinal, y sólo en el caso en que sea absolutamente imposible, con los elementos señalados, dar respuesta a las nuevas necesidades, acudir a una legislación y práctica extranjera que deberá siempre ser respetuosa con la propia, y a su vez, exigir a nuestro legislador, que tomando conciencia de la nueva situación, regule de forma precisa, los extremos que aún así queden fuera de nuestro alcance.

■[10] ANDRE BERTRAND.- "Contrats Informatiques. Services et Conseils Ed. des Parques. París 1.983.

En ningún caso, podemos acudir a la fácil e incorrecta solución de suponer que, si nuestra normativa contractual es insuficiente o no se ajusta de forma absoluta e indiscutible a las necesidades de estos nuevos contratos, un "calco" del Derecho Comparado, sobre la base de la autonomía de la voluntad de nuestro art. 1.255 del Código Civil, puede ser la vía adecuada de solución, aún conculcando nuestros principios contractuales básicos, perfectamente reconocidos en nuestro ordenamiento jurídico.

III.- PRINCIPIOS Y CARACTERISTICAS FUNDAMENTALES DE LOS CONTRATOS INFORMATICOS. LA VOLUNTAD EN LA CONTRATACION INFORMATICA.

Como señala MIGUEL ANGEL DAVARA[11], los contratos informáticos como tales, con su tipicidad única y propia, no existen, no siendo posible un modelo único de contrato, lo que nos obliga a acudir a la teoría general de la contratación. Pero esta afirmación, sin dejar de ser correcta, no impide que haya una serie de características y circunstancias que impregnan la propia esencia de todo contrato informático.

Así, en primer lugar, debemos destacar las diferencias existentes entre ambos contratantes. El proveedor (como término genérico) de bienes o servicios informáticos, no solamente se encuentra, por regla general, en una posición económicamente más fuerte que la del usuario (también utilizado en término genérico), sino que además, y esta es una de las características propias de este tipo de contratos, sus conocimientos técnicos suelen estar muy distanciados.

Este desequilibrio evidente lleva con cierta habitualidad, a la creación de contratos de adhesión, en los que la colaboración negocial y bilateralidad propia de todo tipo contractual, queda muy mediatizada. El usuario no interviene en igualdad de condiciones en la gestación del contrato, sino que se limita a aceptar lo que el proveedor le ofrece-impone.

Por otra parte, observamos que este ámbito contractual se presenta como terreno abonado para la aparición de abusos, por acciones u omisiones, que

■[11] MIGUEL ANGEL DAVARA.- Obra ya citada

pueden llegar a viciar el contrato. El intentar ampararse en la autonomía de la voluntad, art. 1.255 del Código Civil[12], para justificar todo tipo de cláusulas contractuales, no sólo es una falacia, sino que en nuestra opinión, va en contra de la propia literalidad del artículo antes citado.

La situación de desigualdad entre las partes, propia de los contratos de adhesión, se ve agravada en los de naturaleza informática, ya que, al desequilibrio económico, se añade una menor preparación técnica[13].

En el ámbito contractual informático, debe asimismo destacarse la obligación de información consejo y asesoramiento, que adquiere una importancia decisiva.

Es obligación indiscutible de la parte más informada, esto es el proveedor del bien o servicio, poner de manifiesto al usuario todas y cada una de las características del entramado técnico que puede ser objeto de contratación. Pero no solamente debe informar en sentido estricto (poner de manifiesto una serie de hechos) sino que debe "aconsejar" la solución más beneficiosa y factible a las necesidades de la contraparte, lo que no debe suponer colocar al usuario en una posición de absoluta pasividad y privilegio, sino que, por el contrario, éste tiene el deber inexcusable de cooperar con el proveedor en la determinación de sus necesidades y de las mejores respuestas a las mismas.

Por otra parte, como en todo tipo de contratos, las posiciones de los contratantes son opuestas, pero concurrentes en su perfección (art. 1.262.1 del Cc[14]). El usuario parte de su intención de contratar un resultado, frente a la opinión del proveedor que oferta un funcionamiento en abstracto. Ciertamente, parece lógico inclinarse por la contratación con miras a un resultado. Se solicita un sistema informático, por unas necesidades que quieren solventarse, pero

■12 Art. 1.255 del Código Civil "Los contratantes pueden establecer los pactos, cláusulas y condiciones que tengan por conveniente, siempre que no sean contrarios a las leyes, a la moral, ni al orden público".

■13 CORREA Y OTROS.- Derecho Informático

■14 Art. 1.262.1 del Código Civil " El consentimiento se manifiesta por el concurso de la oferta y la aceptación sobre la causa y la cosa que han de constituir el contrato"

debemos ser conscientes, que en la materia que nos ocupa, la perfección indiscutible y la garantía absoluta de un resultado, se complican a medida que la solicitud es más compleja.

Entendemos por ello, que es característica propia de la contratación informática, buscar un resultado dentro de parámetros lógicos y naturales, sin permitir la exigencia del usuario de un resultado ideal e inalcanzable, ni al proveedor de una discreción y arbitrariedad que llevarían a la propia inexistencia del contrato (art. 1.256 del Código Civil[15]).

Otra de las notas características de este tipo de contratos es la diversidad de las prestaciones. Diversidad de prestaciones que se complica en el momento en que la contratación deja de centrarse en un bien o servicio, para incluir una pluralidad de prestaciones. Así nos encontramos, no sólo con la posibilidad, sino con la habitual presencia de múltiples prestaciones englobadas en un sólo contrato, o bien múltiples contratos, sobre prestaciones diversas, interconectados[16], que crean una relación de dependencia entre ellos. Todo ello obliga a que el objeto de la contratación informática esté precisado de una forma exquisita y con una terminología perfectamente detallada.

Como ya hemos señalado, las soluciones a las necesidades contractuales en materia informática, no pueden ser solventadas de ningún modo, por una mera traducción de los moldes provenientes de ordenamiento jurídicos ajenos. Sus planteamientos normativos y negociales pueden ser radicalmente diferentes a los nuestros, lo que supondrá o podrá suponer, la plasmación de cláusulas contractuales, que carezcan de todo sentido para nosotros, o incluso que adolezcan de nulidad por contravenir una normativa, ya vigente[17].

Como establece CATALA[18], la traducción literal de conceptos propios de

■[15] Art. 1.256 del Código Civil "La validez y el cumplimiento de los contratos no puede dejarse al arbitrio de uno de los contratantes".

■[16] ANA LOPEZ FRIAS.- "Los Contratos Conexos". Ed. J.M.Bosch S.A.. Barcelona 1.994.

■[17] Merece destacarse como ejemplo la cláusula de exclusión de responsabilidad propia de los contratos anglosajones y de difícil adaptación a nuestro ordenamiento jurídico.

■[18] P. CATALA.- "L'Informatique et l'evolucion des modelles contractuelles. V Congreso

un país que no guarda su correlato con otro, puede llevar a serios equívocos.

Se parte de una cooperación en la formación de un negocio por ambas partes contratantes, pero el tráfico masivo de mercancías, el comercio de las multinacionales y la complicación de los objetos y servicios intercambiados, coloca esta idea primigenia en una posición un tanto utópica, en un gran número de ocasiones.

IV.- NATURALEZA Y FORMA DE PRESENTACION DE LOS CONTRATOS INFORMATICOS.

El primer problema que plantean los contratos informáticos es la necesidad de acoplarlos a los tipos legales ya existentes, o bien, la posibilidad de identificarlos con otros típicos o acudir al concepto más genérico de atipicidad.

Los contratos atípicos surgen como respuestas a las cambiantes necesidades económicas que evolucionan con mayor rapidez que el contenido de nuestras leyes, y así cuando las nuevas necesidades no pueden ser solventadas por los contratos típicos, aparecen al amparo de la libertad contractual, nuevas formas que responden a un normal desenvolvimiento de la vida jurídico económica.

Lógicamente estos contratos habrán de regirse por los acuerdos de las partes, por las normas dispositivas de figuras afines, por las generales de la contratación y por la costumbre y principios generales del Derecho.

Hoy en día, la atipicidad absoluta es difícil de encontrar, pero por otra parte, en la materia que nos ocupa, más que en ninguna otra, la forma normal de presentarse un contrato es la mixta, que supone, como ya hemos dicho, que un solo acto negocial engloba diversas prestaciones características de otros contratos típicos.

No obstante, con todo lo dicho, tratamos una materia en la que predominan los llamados contratos de "atipicidad típica", o en palabras de

Informática e Acttivita Giuridica. Roma 1.993.

ROSELLO[19], "atipicidad estandarizada", que goza así de una tipicidad social individualizada por los usos negociales, doctrina, y en cierto modo, actuación jurisprudencial.

Problema diferente supone la aparición de los contratos conexos[20], que determinan una coordinación de distintos tipos negociales unidos por una misma finalidad económica.

En estos supuestos, encontramos un conjunto de contratos típicos, pero que están íntimamente relacionados, debiendo depender los resultados de uno, de los resultados de los demás.

La regulación aplicable, con la dependencia ya señalada, se presenta de una forma más sencilla. En cualquier caso, el principio base de nuestra contratación es la autonomía de la voluntad, y será sobre esta base, sobre la que los contratantes, comiencen y determinen el perfil de sus negocios, ahora bien, la ley (art. 1.258[21]) liga a los contratos unas consecuencias que no tienen por qué estar plasmadas en los mismos, y la autonomía de la voluntad no puede conculcar estas consecuencias, al igual que las obligaciones que de forma imperativa se establezcan por nuestra normativa.

Las conexiones que entre los contratos informáticos, se pueden apreciar, son indiscutibles. Debemos tener en cuenta cómo el hardware solo funciona cuando le es aplicable un software, al igual que éstos solo pueden ser útiles a través del ordenador. Por otra parte, la celebración de un contrato de asistencia técnica sólo tiene sentido si existe algo que cuidar y reparar. Así, todos estos contratos tienden a alcanzar una misma finalidad, consistente en hacer posible para un determinado sujeto, el uso de un sistema informático. Si los contratos

■[19] ROSELLO C.C..- "I Contratti dell'Informatici. Spunti di Reflesione in Comparazione con l'sperienza estatunitense e francese, en I. Contratti di utilizzacione del computer a cargo de G. ALPA. Giuffré. Milán 1.984.

■[20] ANA LOPEZ FRIAS.- Obra ya citada.

■[21] Art. 1.258 Cc.- "Los contratos se perfeccionan por el mero consentimiento, y desde entonces obligan no sólo al cumplimiento de lo expresamente pactado, sino también a todas las consecuencias que, según su naturaleza, sean conformes a la buena fe, al uso y a la ley".

antes mencionados son perfeccionados con un mismo proveedor, parece admisible la posibilidad de oponer la excepción de incumplimiento, en relación al precio de la máquina o al del software, cuando este software adolece de algún defecto, o viceversa[22].

Supuesto diferente, se plantea cuando los proveedores son distintos, en cuyo caso, el incumplimiento de un contrato por su inadecuación con el objeto de otro, sólo podrá ser excepcionado, cuando expresamente se haya hecho constar este requisito en el contrato. En otro caso, no pueden recaer sobre un proveedor que desconoce la existencia de un hardware o software, ajeno a su contrato, las consecuencias de una descoordinación de ambos.

V.- ELEMENTOS DE LA CONTRATACION INFORMATICA

El art. 1.261 del Código Civil, establece como indispensables para la existencia de un contrato[23] la concurrencia del consentimiento, el objeto y la causa.

Obviaremos la referencia a la causa, figura discutida y discutible, cuyo estudio sobrepasa los límites e intenciones de este trabajo.

Por lo que se refiere al segundo de estos elementos, el objeto, nos remitimos a lo señalado anteriormente, al concretar el concepto de contratación informática. Recordemos que es precisamente la peculiaridad del objeto (la prestación que recae sobre bienes y servicios informáticos) lo que va a calificar la propia naturaleza contractual. Pero hemos de poner de manifiesto la gran variedad de bienes y servicios informáticos que existen y que a su vez, darán su

■[22] ANA LOPEZ FRIAS.- Los Contratos Conexos. Estudio de supuestos concretos y ensayo de una construcción doctrinal. Ed. JOSE MARIA BOSCH.- Barcelona 1.994

■[23] Art. 1.261 del Código Civil.- "No hay contrato sino cuando concurran los requisitos siguientes: 1) Consentimiento de los contratantes, 2) Objeto cierto que sea materia del contrato y 3) Causa de la obligación que se establezca".

tinte particularizado a cada negocio en concreto, respetando siempre las exigencias que los arts. 1.271 a 1.273 del Código Civil, determinan en cuanto al objeto[24].

Merece especial mención el hecho de que en la negociación informática, la determinación del objeto puede alcanzar cotas de dificultad mayores que en la contratación ordinaria, lo que lleva consigo la necesidad de un exquisito examen de esta determinación para evitar posteriores problemas por el incumplimiento.

La multiplicidad y diversidad de las prestaciones objeto del contrato, llegan a calificar los propios pactos contractuales, como negocios de suma complejidad, cuya dificultad se verá agravada por los distintos tipos de derechos y obligaciones que ya se trate de hardware, de software o de servicios, determina nuestra legislación.

De forma meramente enunciativa, podemos citar[25]:

Como bienes informáticos:

1.- El equipo informático (unidad central de proceso y unidad periférica), equipo de transmisión de datos (módems, computadoras, multiplicadores...), equipo de telecomunicaciones, calculadoras programables, equipos y máquinas de contabilidad, equipo de proceso de palabras...

2.- Suministros informáticos: para registro de la información, de

■[24] Hablando con propiedad, afirma COLIN Y CAPITANT, un contrato no tiene objeto. El contrato es un acto jurídico que produce el efecto de crear obligaciones, ya a cargo de las dos partes, ya a cargo de una de ellas. Son estas obligaciones las que tienen un objeto, que puede consistir en una cosa material, o en un hecho, o en una abstención, por lo tanto, sólo de un modo elíptico, se puede hablar de objeto del contrato. En la misma línea, CASTAN afirma que el objeto inmediato de un contrato, en realidad, es la obligación que por él se crea, que a la vez tiene por contenido, una prestación de dar, hacer o no hacer, lo que nos lleva a considerar objeto del contrato, las cosas o servicios que son la materias de las obligaciones de dar, hacer o no hacer. En la misma línea, JULIO TELLEZ VALDES, en su ponencia "Contratos Informáticos", presentada en el Congreso de Guatemala, afirma que los contratos informáticos tienen por objeto regular la creación y transmisión de derechos y obligaciones, respecto a los bienes y servicios informáticos.

■[25] JULIO TELLEZ VALDES.- Los Contratos Informáticos.- Obra ya citada.

abastecimiento del equipo, auxiliares del equipo, auxiliares para programación...

3.- Programas de computación: sistemas organizadores de multiproceso, controladores de multiproceso, de aplicación específica...

4.- Equipo y suministro de apoyo y auxiliares a la información.

Como servicios informáticos:

1.- Relacionados con recursos humanos

2.- De acondicionamiento de locales e instalación de equipo de cómputo y auxiliares.

3.- De uso de equipos de cómputo por tiempo limitado

4.- De explotación de programas bajo licencia de uso, con o sin cargo

5.- De consultas de archivos y bases de datos

6.- De estudios de mercado en Informática

7.- De documentación técnica e informática

8.- De mantenimiento preventivo, correctivo o de conservación

9.- De manejo de datos

10.- De auditoría y diagnóstico

11.- De desarrollo de estudios de viabilidad, factibilidad, inversión o adquisición de bienes o servicios informáticos...

12.- Cualesquiera otros servicios de apoyo y auxiliares a la Informática....

Respecto al último de los elementos del contrato, el consentimiento, evidentemente las partes, tras haber determinado el objeto cierto del contrato, tendrán que alcanzar la coordinación de sus voluntades. De esta forma, partiendo de posiciones contrapuestas, llegará un momento en que tanto la oferta como la aceptación coincidan puntualmente, momento éste en que se entenderá

perfeccionado el contrato.

De forma genérica, las partes involucradas en un contrato informático, serían: el proveedor o suministrador, que será el encargado de realizar la prestación que sobre los bienes y servicios informáticos se esté pactando, y la persona natural o jurídica que reciba la antedicha prestación, que podemos denominar, usuario[26].

VI.- FASES DE LA CONTRATACION

Las fases de la contratación son las siguientes:

1) Periodo precontractual o de negociación.

2) Acuerdo de voluntades o perfeccionamiento del contrato.

3) Ejecución o cumplimiento de lo acordado.

A) FASE PRECONTRACTUAL

Ya hemos adelantado, que cuando la contratación informática recae sobre algo más que la sencilla compra de un ordenador personal o un disquete en una tienda especializada, requiere una importante fase precontractual en la que las partes pongan de manifiesto su intención de contratar, la finalidad perseguida, etc....

Esta fase precontractual adquiere una importante significación en este tipo de contratos, porque, en ocasiones, el llamado usuario, se presenta a la misma sin tener claras sus verdaderas necesidades, o si se prefiere, sin poder determinar

[26] EDUARDO RAMOS MENDEZ, LUIS EUGENIO OLIVER y FRANCISCO EUGENIO DIAZ.- Informática Jurídica. Educación Permanente. UNED, de una forma más desarrollada, hablan de los papeles a desempeñar por las personas que intervienen en la negociación de un contrato informático de cierto alcance, siguiendo a LOSANO, mencionando el papel del delegado de la alta dirección, el centro de cálculo a instalar, el experto en informática, ajeno a la empresa, el representante sindical de los trabajadores implicados y el jurista, encargado de preparar la documentación.

de una forma clara y precisa, qué soluciones pretende para esas necesidades.

En este periodo contractual, el suministrador o proveedor, deberá estudiar las necesidades o intenciones contractuales que el usuario ha puesto de manifiesto, gozando de la imprescindible colaboración de éste último. El proveedor tiene la obligación de asesorar y aconsejar al usuario, siendo nefastas las consecuencias que para una y otra parte se pueden dar si se escatiman esfuerzos y se mantienen actitudes suspicaces durante estas conversaciones.

Es conveniente que el usuario se asesore por técnicos ajenos al suministrador, si bien los límites de la obligación del primero respecto al análisis de sus necesidades, se encuentran en el deber de consejo y asesoramiento del proveedor[27].

Todas estas obligaciones y necesidades se verán modificadas y atemperadas, a tenor de la preparación técnica y negocial de ambas partes, teniendo en cuenta, con todo, las responsabilidades en que uno y otro podrán incurrir para el supuesto de una defectuosa coordinación de esfuerzos.

Es lógico pensar que, pese a lo establecido en nuestro Código Civil, en el art. 1.282[28], lo tratado en esta primera fase contractual será fundamental a la hora de interpretar los contratos, debiendo tenerse muy en cuenta el tenor literal del art. 1.288 del Código Civil respecto a las cláusulas oscuras[29].

Por último, hemos de advertir como señala ISABEL HERNANDO[30], que todos los estudios y conversaciones pueden no llegar a finalidad alguna, por causa de una actitud malintencionada y abusiva de una de las partes, encontrándonos ante la llamada "ruptura abusiva de los tratos preliminares".

■[27] ISABELLE DE LAMBERTERIE.- Obra ya citada.

■[28] Art. 1.282 del Cc.- "Para juzgar de la intención de los contratantes deberá atenderse principalmente a los actos de éstos, coetáneos y posteriores al contrato".

■[29] Art. 1.288 del Cc.- "la interpretación de las cláusulas oscuras de un contrato, no deberá favorecer a la parte que hubiese ocasionado la oscuridad".

■[30] ISABEL HERNANDO.- "Los Contratos Informáticos". Librería Carmelo. San Sebastián 1.996.

Al no estar regulada esta materia de forma expresa, podemos acudir a una doble solución. Si existen contratos de estudio y asesoría, las consecuencias de la ruptura deberán haber sido establecidas en los mismos. Si no es así, no tenemos más remedio que acudir al art. 1.902 del Cc, para la depuración de responsabilidades. Pero todo jurista es consciente que si bien se podría obtener una indemnización de daños y perjuicios, mucho más difícil será conseguir el resarcimiento por lucro cesante, que puede alcanzar en estos tipos contractuales, unas cotas importantísimas.

En la etapa precontractual, el usuario al determinar sus necesidades, deberá atender a su organización y los fines pretendidos, que comunicará al proveedor, quien a su vez, y como consecuencia de la imprescindible colaboración contractual, tiene la obligación de requerirle los datos y características necesarios, para poder ofrecer unas soluciones viables. Es conveniente, aunque no imprescindible, a efectos de evitar discusiones y responsabilidades postreras, plasmar por escrito estas necesidades, que firmarán ambos contratantes.

Una vez prefijadas con claridad, en la medida de lo posible, las necesidades del usuario, el proveedor propondrá las mejores soluciones, a su entender, informando y aconsejando al usuario, en evitación de soluciones excesivamente escasas o extensas.

En su propuesta de soluciones, el proveedor señalará los usos y tareas que el material está en condiciones de resolver, las características de la instalación, los diferentes elementos que permitan al usuario calcular la rentabilidad del sistema ofrecido, advirtiéndole de los riesgos inevitables que su adquisición puede conllevar[31].

En la fase de negociación, deberán discutirse sobre los presupuestos antedichos, todas las cláusulas que posteriormente se reflejarán en la firma del contrato, y que son determinantes, no solo de aspectos puntuales que redondean el contrato en su globalidad, sino que pueden perfilar de una manera sustancial, la propia viabilidad del contrato. Evidentemente, el proveedor puede encontrar en

■[31] DANIEL RICARDO ALTMARK.- La etapa precontractual en los contratos informáticos.

principio, soluciones a casi todos los problemas y necesidades que le plantea el cliente, pero su coste, el momento de entrega, o incluso la forma de pago, pueden resultarle, o inalcanzables o inaceptables a este último.

En todo el proceso negocial, debe primar la buena fe, colaboración y confianza mutua, pero desgraciadamente, la experiencia nos muestra cómo es conveniente que cada uno de los pasos, se refleje por escrito, no sólo para poder observar la evolución de todo el proceso, y facilitar la interpretación de las futuras cláusulas contractuales, sino y fundamentalmente, para garantizar la posición, tanto del proveedor, como del usuario. Esta documentación precontractual, en principio no obliga a la suscripción del contrato, pero sí crea un marco jurídico al que se podrá acudir, a efectos de exigir las posibles responsabilidades, por los perjuicios causados tanto por la ruptura de negociaciones, o la retirada prematura de la oferta, como por la divulgación de secretos o facetas empresariales que se hayan puesto en juego.

B) PERFECCIONAMIENTO DEL CONTRATO

Una vez finalizada la fase precontractual, se llega a la que podríamos llamar de perfeccionamiento del contrato, en la que se redacta éste y se procede a su suscripción por las partes.

Los contratos informáticos que en un primer momento no fueron más que un calco de los ya desarrollados por los países anglosajones, van adquiriendo en la actualidad, una forma más acorde y adecuada, con nuestro ordenamiento jurídico. En ellos, como señala BIGELOW[32] es muy importante que se determine de forma clara y precisa, qué se va a hacer, dónde se va a hacer, cuándo se va a hacer, cómo se va a hacer y quien lo va a hacer.

Las cláusulas contractuales, que deberán estar perfectamente redactadas y perfiladas, atenderán a todos los extremos que el objeto contractual precise, dependiendo, eso sí, la existencia de unas u otras, de la peculiar prestación que en cada momento se esté tratando.

■[32] ROBERT P. BIGELOW.- "Understanding computer system contracts". Data Center Operations Managements. Auerdach Publisher 1.991. WARREN GORHAM & LAMONT.

CLAUSULAS CONTRACTUALES

De una forma genérica, podemos determinar como cláusulas más representativas, las siguientes:

1.- Las partes. El contrato deberá reflejar quiénes son las partes contratantes, su naturaleza física o jurídica y la posición que ocupen en el contrato. Huelga decir que ha de precisarse el carácter representativo de la persona física que actúa en nombre de la jurídica, determinándose con meridiana claridad, los sujetos que vayan a quedar vinculados.

2.- El objeto del contrato, determinando los derechos y obligaciones que surgirán sobre los bienes y/o servicios contratados. Por otra parte, el objeto del contrato puede sufrir modificaciones dada la duración en el tiempo que el cumplimiento del mismo puede requerir, supuesto que deberá constar expresamente en el contrato.

3.- Duración, en la que se fijará el plazo de vigencia del contrato, y en su caso, la propia vida contractual, estableciéndose los ritmos mínimos de trabajo, y las fechas a partir de las cuales comenzarán las responsabilidades por mora. Debe tenerse en cuenta que el factor tiempo, en un contrato informático de cierta entidad, adquiere una importancia de primerísimo orden, ya que, por una parte puede suponer la paralización de una empresa o la suspensión parcial de sus actividades, y por otra, la obsolescencia de ciertos elementos pactados en el contrato. En supuestos contractuales como el del mantenimiento, la vida del contrato garantiza al cliente un periodo en que se le asegura el funcionamiento del sistema, pudiendo éste calcular su renovación empresarial o forma de trabajo, sobre unos parámetros de seguridad.

4.- Fijación del precio y forma de pago. Esta cláusula determinará la cantidad a pagar, las formas y plazos de pago, con sus respectivas garantías, debiendo calcular, dentro de unos márgenes, ciertos costes que en un primer momento, no pudieron preverse. Lógicamente la fijación del precio y modo de pago, variarán según el objeto del contrato, fijándose de forma diferente en una compraventa o en un arrendamiento de servicios. Pero indudablemente el precio debe ser cierto, bien por estar fijado de forma expresa en el contrato, o por haberse establecido los criterios para ser determinado. En ningún caso podrá dejarse al arbitrio de una de las partes la determinación del mismo, lo que

equivaldría a dejar en sus manos el cumplimiento o incumplimiento del contrato.

Tan importante como el precio, resulta el momento de pago o facturación, que pude posibilitar tanto la disponibilidad del dinero por parte del usuario, como el propio funcionamiento de la empresa proveedora, ya que en múltiples ocasiones los contratos informáticos se extienden en el tiempo con importantes costes, que no pueden posponerse en su totalidad hasta la finalización completa de la prestación.

5.- La entrega y pruebas de recepción. Todo contrato nace a la vida negocial para su cumplimiento, debiendo determinarse el plazo y el lugar de la entrega. Una vez realizada la entrega, se procederá a efectuar los controles y pruebas de recepción, para asegurar que las prestaciones realizadas son conformes a las necesidades del cliente. Las pruebas deberán estar sometidas a un calendario que formará parte del contrato. Una vez pasadas estas pruebas, el cliente procederá a aceptar el bien (o el servicio), lo que muestra claramente la diferencia entre entrega y recepción. Es conveniente establecer un periodo de prueba en que el usuario vaya comprobando la idoneidad del producto, a cuya finalización se producirá la aceptación definitiva[33].

6.- Cláusula de Confidencialidad. La información que entra en juego o puede aparecer y utilizarse en un contrato informático, hará pertinente la existencia de cláusulas que garanticen la reserva por ambas partes contratantes.

7.- La transmisión de derechos. Tanto sobre el hardware, como sobre el software se deberá especificar qué derechos y en qué amplitud adquiere el usuario, con las consiguientes garantías y responsabilidades. Especial significación adquiere esta materia, en el caso del software, que siempre habrá de respetar el marco establecido por nuestra Ley de Propiedad Intelectual.

8.- Cláusula de asistencia técnica y capacitación del personal del usuario, a la que se unirá, en cláusula aparte, la entrega de los manuales y documentos necesarios para el funcionamiento y utilización del hardware y del software.

■[33] Lógicamente, los contratos de servicios tienen unas características peculiares por la propia naturaleza de la prestación objeto del contrato.

9.- Cláusula de escrow[34].

10.- Cláusula de mantenimiento[35].

11.- Otras cláusulas. El contrato informático contendrá los supuestos de incumplimiento, los seguros concertados, fianzas a prestar, cláusula arbitral, y demás disposiciones que faciliten y determinen el contrato.

12.- Asimismo constarán las garantías y responsabilidades a que se comprometen unos y otros. Se puede observar una tendencia por parte de los proveedores, de excluir al máximo sus responsabilidades, cláusula que a nuestro entender, puede llegar a ser nula por ir en contra de nuestra propia legislación.

C) CUMPLIMIENTO DEL CONTRATO

Una vez suscrito el contrato, comienza la fase de ejecución o cumplimiento, en la que se harán las entregas, comenzarán a prestarse los servicios..., o en otras palabras, se empezará a cumplir lo acordado en el contrato firmado. Evidentemente, el cumplimiento ha de ajustarse estrictamente a lo acordado, que deberá, como ya hemos señalado, estar perfectamente detallado. Se respetarán los plazos de entrega y de asistencia, el pago del precio, las responsabilidades por vicios...

Las notas reseñadas son más características de los contratos de cierta entidad, dado que a nadie se le escapa que si alguien quiere comprar un ordenador personal, no necesitará una fase precontractual desarrollada; el consejo que recibirá será muy limitado, y el contrato se redactará en el mejor de los casos, como un contrato-tipo.

■[34] Nos remitimos al contrato de escrow, tratado específicamente en esta obra.

■[35] Nos remitimos al contrato de mantenimiento.

VII.- TIPOS DE CONTRATOS

La propia naturaleza de los contratos informáticos, el complejo mundo sobre el que recaen y la constante evolución de los mismos, hace que cualquier clasificación que propongamos, tienda a quedar, o desfasada, o cuando menos, no aporte la visión global que toda clasificación, para ser útil, debe proporcionar.

Una primera aproximación a la tipología de los contratos informáticos, nos indica, como ya hemos señalado en numerosas ocasiones, que son todos aquéllos que recaen sobre bienes y servicios informáticos, por lo que, indudablemente, el primer intento clasificatorio, nos llevará a distinguir entre aquellos que recaigan sobre bienes informáticos; y los que tengan por objeto un servicio relacionado con la informática.

Un segundo paso nos obliga a destacar la diversa naturaleza de los bienes informáticos. Naturaleza que conlleva un tratamiento diferenciado entre los bienes materiales y los inmateriales, por lo que, atendiendo al objeto sobre el que recae el contrato informático, podremos observar que existen los contratos sobre hardware, sobre software y sobre servicios informáticos.

Esta es la clasificación más básica y generalmente admitida. Cada contrato podrá localizarse dentro de alguno de estos tres grandes grupos, pero realmente esta clasificación carece de virtualidad práctica, ya que a nadie se le escapa que afirmar la complejidad del mundo informático, conlleva afirmar la complejidad del mundo contractual que se centra en esta materia. Los contratos de servicios en numerosas ocasiones se entremezclan con contratos que, en puridad, quedan englobadas en los otros dos grupos, mostrando un panorama mucho más interrelacionado que el que esta clasificación pueda, a primera vista, ofrecer.

Ello ha llevado a EMILIO DEL PESO[36] a afirmar que esta división no responde ya a la realidad, proponiendo la división de los contratos entre: contratos de hardware, contratos de software, contratos de datos, contratos de servicios y contratos complejos.

■[36] EMILIO DEL PESO.- La Contratación Informática.- Actualidad Informática Aranzadi.- núm. 14 Enero 1.995.

Clasificación esta que se acerca más al entramado real de las relaciones negociales que recaen sobre la Informática.

BONNEAU[37] propone una clasificación atendiendo al negocio jurídico que se celebre, distinguiendo entre: contrato de venta (que puede ser de equipo informático o de programas); contrato de leasing; contrato de locación sobre equipos o sobre programas; contrato de horas-máquina, que equivaldría a un contrato de cesión de uso; contrato de mantenimiento; contrato de prestaciones intelectuales que englobaría los estudios previos, el pliego de condiciones, la formación de personal, el contrato llave en mano y contrato de prestación de servicios.

Todas las clasificaciones expuestas y cualquiera otra que atendiese a criterios diferentes, a pesar de poder ser objeto de numerosas y fundadas críticas, no dejan de aportar una visión globalizante del aspecto negocial de la Informática, que ayudará a cualquier estudioso de esta materia a centrar en un primer acercamiento la figura contractual ante la que se encuentre.

FIGURAS CONTRACTUALES MAS REPRESENTATIVAS:

LA COMPRAVENTA INFORMATICA

1) INTRODUCCION

La compraventa, tal y como establece el art. 1.445 de nuestro Código Civil, es el contrato por el que una parte se obliga a entregar cosa determinada, y la otra a pagar por ella un precio cierto, en dinero o signo que lo represente.

Una primera aproximación a la figura de la compraventa informática nos

■[37] JACQUES-ROGER BONNEAU.- "La pratique du droit de l'Informatique dans l'enterprise. Les relations entre contructeurs utilisateurs et conseils, et de l'usine nouvelle.- París 1.984, citado por CORREA y otros en "Derecho Informático".

obliga en primer lugar a cuestionarnos su naturaleza, características y especificidad. ¿Es realmente la compraventa informática una figura negocial con características propias con relación a la compraventa ordinaria?.

La compraventa informática será aquélla que recaiga sobre bienes informáticos, lo que en principio no le confiere ninguna característica especial, o cuando menos no aporta ningún razonamiento de mediana entidad que justifique nuestro estudio. Por supuesto, puede haber una compraventa de coches, de mobiliario de oficinas, de libros... y por ello no se realiza un estudio pormenorizado específico de sus características, al coincidir básicamente con las generales de la compraventa.

Pero realmente el concepto de bien informático y sus propias características, sí que plantean una cualificación del contrato de compraventa que hace conveniente su tratamiento.

El bien informático puede abarcar al hardware y al software, lo que por pura lógica nos llevaría a afirmar, a tenor de la definición aportada, que el contrato de compraventa podrá recaer sobre el hardware y sobre el software.

BONNEAU[38] al clasificar los contratos informáticos, habla en primer término del contrato de venta, que subdivide en venta de equipo informático y venta de programas. Incluso este mismo autor, cuando habla de la compraventa de equipamiento, pone de manifiesto, cómo a menudo se incluye también el software asociado.

Por nuestra parte, consideramos que no es posible hablar de venta de software, salvo, como señalan GOMEZ ACEBO y POMBO[39] la venta de cosas específicas de un programa, venta del disquete o soporte; realizándose simultáneamente con esta venta, la obtención de una licencia de uso del programa

■[38] JACQUES ROGER BONNEAU.- La practique du droit de l'informatique dans l'enterprise, les relations entre constructeurs, utilisateurs et conseils. Ed. de l'USINE NOUVELLE. París 1.984.

■[39] GOMEZ ACEBO y POMBO.- Cómo Protegerse de los riesgos derivados de las cláusulas abusivas en los contratos de hardware y software". Institute for International Research España. 9 de febrero de 1.994.

que contiene, por lo que en puridad, el contrato de compraventa y su regulación, tanto en el Código Civil como en el Código de Comercio, según los casos, se aplicará exclusivamente al equipo informático

2.- ELEMENTOS PERSONALES Y REALES. EL OBJETO DE LA COMPRAVENTA INFORMATICA. EL CUMPLIMIENTO DE LAS OBLIGACIONES ASUMIDAS.

A) ELEMENTOS PERSONALES

Las partes que intervienen en una compraventa son el comprador y el vendedor, a las que se les exige capacidad para contratar, capacidad que se supone a toda persona a quien nuestras leyes autorizan para obligarse, siendo la incapacidad, la excepción a la regla.

B) OBLIGACIONES DEL VENDEDOR

Por lo que se refiere al vendedor o persona que se obliga a entregar un bien informático, deberá, como obligación más característica, dar toda la información necesaria para que el comprador conozca las posibilidades y utilidades del bien informático adquirido.

ISABELLLE DE LAMBERTERIE[40] afirma que la Jurisprudencia francesa establece que el vendedor asume una doble obligación: de puesta en guardia y de consejo, por un lado y de informar e informarse, por otro, si bien, como señala ANDRÉ BERTRAND[41] esta obligación no es la misma en cuanto al proveedor de microcomputadoras y el de grandes equipos, aunque ello no es óbice para presuponer la desaparición de esta obligación de informar completa y correctamente, que pesa sobre el vendedor.

■[40] ISABELLE DE LAMBERTERIE.- Les contrats en informatique, jurisprudence française. 3ª edición Librairie de la Cour de Cassation 1.983.-

■[41] ANDRE BERTRAND.- L'obligation de conseil et de renseignement en Droit de l'Informatique 1.986, "Expertises núm. 84 Mayo 1.986 París.

Debe entenderse que el término "información" que estamos empleando, engloba las obligaciones de prevenir y aconsejar la mejor y más útil adquisición para el comprador.

Obviamente, y dada la complejidad del objeto de esta compraventa, deberá el vendedor, entregar las instrucciones y documentación necesaria para su uso, siendo precisamente estas pautas, comprensibles para el adquirente.

Esta información debe ser clara y precisa, por lo que el vendedor ha de solicitar del comprador, los datos necesarios de su actividad o destino para el que va a emplear o al que va a dedicar su equipo informático.

La capacitación técnica del adquirente determinará la naturaleza y extensión de las explicaciones del vendedor que en todo caso, incluirá la compatibilidad con otros aparatos y/o sistemas, las posibilidades de expansión...

Asimismo, si bien el contrato queda perfeccionado al asumir por las partes sus respectivas obligaciones, entendemos que el vendedor ha de entregar el bien adquirido, y si fuese necesario por la importancia de dicho bien, será precisa además la instalación en el lugar que se haya convenido[42].

B.1 Entrega

Sin duda alguna, el vendedor está obligado a entregar la cosa en el estado en que se hallase al perfeccionarse el contrato (art. 1.458 Cc), por lo que en caso de venta de un sistema que precise una instalación, éste deberá responsabilizarse de su buen estado, encargándose asimismo de los seguros que fueran precisos, lo que no impide que en numerosas ocasiones, el vendedor trate de exonerarse de toda responsabilidad. Estimamos que hasta que el equipo no esté en funcionamiento o con posibilidades de estarlo, el comprador no asume ningún riesgo. El vendedor así, deberá demostrar la perfecta viabilidad del equipo instalado.

■[42] El art. 1.461 del Cc establece que el vendedor está obligado a la entrega de la cosa objeto de la venta.

Nuestro Código Civil, en el art. 1.453 admite la venta hecha en calidad de ensayo o prueba y la venta de las cosas que es costumbre gustar o probar antes de recibirlas, presumiendo que se hacen siempre bajo condición suspensiva. Así el llamado "test de aceptación" es el medio de que dispone el comprador de un equipo para revisarlo, a partir del cual comenzará un periodo de prueba opcional que deberá constar en el contrato[43].

Es lógico pensar que en caso de desacuerdo en cuanto al funcionamiento del equipo, se acuda a una peritación por un técnico informático que determinará si el equipo se ajusta a lo ofertado por el vendedor y a lo demandado por el comprador.

CORREA[44] afirma que es conveniente que después de la entrega e instalación, el vendedor certifique por escrito al adquirente que el equipo se halla listo para el test de aceptación, debiendo el usuario comprobar en un plazo prudencial, el funcionamiento del equipo con el software para el que está destinado y la inexistencia de vicios de fabricación.

Por último, debemos destacar la obligación del vendedor de garantizar al adquirente el funcionamiento correcto del equipo entregado durante un periodo de tiempo determinado, garantía que el vendedor tratará de eliminar, y que por el contrario es aconsejable que conste en todo contrato de forma clara y expresa, siendo de especial importancia la cuestión relativa a los repuestos, ya que al comprador le interesará un compromiso de suministro durante un periodo prolongado de tiempo.

B.2 Saneamiento.

Complemento de la obligación de entrega, según nuestra legislación, es la de saneamiento (art. 1.461 del Cc).

Así, tal como establece el art. 1.474 del Cc, en virtud del saneamiento a que se refiere el art. 1.461, el vendedor debe garantizar al comprador la posesión

■[43] ALFONSO NOGALES AGUIRRE.- Obra ya citada.

■[44] CORREA y otros.- Obra ya citada.

legal y pacífica de la cosa vendida y responderá de los vicios o defectos ocultos que tuviera.

El art. 1.475 del Cc dispone que tendrá lugar la evicción cuando se prive al comprador por sentencia firme y en virtud de un derecho anterior a la compra, de todo o parte de la cosa comprada.

El vendedor responderá de la evicción aunque nada se haya expresado en el contrato. Los contratantes sin embargo podrán aumentar, disminuir o suprimir esta obligación del vendedor.

Consciente el legislador de la puerta que se abre para un posible abuso de derecho, con el último párrafo del artículo antes citado, se establece en el art. 1.476, la nulidad de todo pacto que exima al vendedor de responder de la evicción siempre que hubiera mala fe por su parte.

En cuanto a la licencia de uso de un software, que puede ir unida a la adquisición de un equipo, indudablemente el vendedor deberá garantizar la legalidad de ese uso, a tenor de lo dispuesto en la Ley de Propiedad Intelectual (materia que será objeto de tratamiento más adelante).

Asimismo, el vendedor estará obligado al saneamiento por los defectos ocultos que tuviera la cosa vendida si la hacen impropia para el uso al que se destina o si disminuyen de tal modo este uso que, de haberlo conocido el comprador, no lo habría adquirido, o habría dado menos precio por ella, pero no será responsable de los defectos manifiestos o que estuvieran a la vista, ni tampoco de los que no lo estén, si el comprador es un perito que, por razón de su oficio o profesión debe fácilmente conocerlos (art. 1.484 Cc).

Téngase en cuenta que a pesar del último párrafo, la complejidad técnica de la compraventa informática hace que la interpretación del mismo, deba hacerse de forma restrictiva.

El art. 1.485 del Cc determina que el vendedor responde al comprador del saneamiento por los vicios ocultos de la cosa vendida, aunque los ignorase. Esta disposición no regirá cuando se haya estipulado en contrario y el vendedor ignorara los vicios o defectos ocultos de lo vendido.

La Jurisprudencia ha venido interpretando extensivamente el art. 1.484 en

el sentido de considerar que cuando los defectos de la cosa sean de tal entidad que la hagan impropia para su uso, se equipararán a la entrega de una prestación diferente a la prometida, con la posibilidad de aplicación de los arts. 1.101 y 1.124, lo que protege mejor los intereses del comprador, a quien la cosa comprada le resulta inhábil para el fin previsto.

Asimismo esta dirección Jurisprudencial llega a considerar de aplicación en dichos casos, el plazo de quince años del art. 1.964 del Cc, superándose los limitados periodos temporales previstos en el art. 1.490 del Cc y 342 del Código de Comercio[45].

La Ley 7/1.996 de 15 de Enero de Ordenación del Comercio Minorista, establece en su art. 12 que el vendedor responderá de la calidad de los artículos vendidos en la forma determinada en el Código Civil y Mercantil[46], así como en la Ley General para la Defensa de los Consumidores y Usuarios y normas concordantes y complementarias. El citado artículo dispone un plazo mínimo de garantía en caso de bienes de carácter duradero, de seis meses a contar desde la fecha de recepción del artículo que se trate, salvo cuando su naturaleza lo impidiere, y sin perjuicio de las disposiciones legales o reglamentarias para bienes o servicios concretos.

El productor, o en su defecto, el importador, debe garantizar frente a los compradores la existencias de un adecuado servicio técnico para los referidos bienes de carácter duradero, así como el suministro de piezas de repuesto durante un plazo mínimo de cinco años, a contar desde la fecha en que el producto deje de fabricarse. Para facilitar el ejercicio del referido derecho, el vendedor, al entregar el bien, extenderá, por cuenta del fabricante o importador, o en nombre propio, el documento de garantía, proporcionándole las instrucciones suficientes para el correcto uso e instalación del objeto, así como para la formulación de las posibles reclamaciones.

■45 Debe tenerse presente lo dispuesto en la Ley de Daños Causados por Productos Defectuosos Ley 22/94 de 6 de Julio.

■46 El ART. 345 del Código de Comercio dispone que en toda venta mercantil el vendedor quedará obligado a la evicción y al saneamiento en favor del comprador, salvo pacto en contrario, determinando en su art. 342 un límite de 30 días desde la entrega para que el comprador pueda reclamar contra el vendedor por los vicios internos de la cosa vendida.

C) OBLIGACIONES DEL COMPRADOR

El comprador está obligado a pagar el precio de la cosa vendida, en el tiempo y lugar fijados en el contrato (art. 1.500 primer inciso del Cc).

El precio deberá constar claramente en el contrato, fijándose la forma y condiciones del pago.

El pago del precio normalmente se hará efectivo, una vez transcurrido el periodo de prueba de forma satisfactoria. El art. 1.466 del Cc afirma que el vendedor no está obligado a entregar la cosa vendida, si el comprador no le ha pagado el precio o no se ha señalado en el contrato un plazo para el pago. Entendemos que el vendedor no podrá exigir el pago hasta que no haya conformidad en cuanto a las características y utilidades del bien objeto de la venta por el comprador.

Las peculiaridades de la compraventa informática hacen inapropiada la aplicación de este artículo o si se prefiere, exige su propia naturaleza, el establecimiento de un cierto plazo para el pago que como mínimo, vendrá a coincidir con el periodo de prueba, lo que implica en los grandes equipos, lógicamente, la previa instalación y puesta en funcionamiento.

Asimismo el adquirente de un bien informático está obligado a colaborar con el vendedor, colaboración que viene a ser la otra cara de la moneda del deber de informar y aconsejar del vendedor, debiendo seguir las instrucciones de este último en cuanto a la preparación de los locales, la utilización del bien y los cuidados que precise.

Al comprador también le interesará establecer en el contrato una serie de cláusulas sobre confidencialidad, garantías, estipulación penal en caso de incumplimiento y capacitación y formación de su personal en el manejo del bien adquirido...

CONTRATOS SOBRE EL SOFTWARE

Cuando se plantea el estudio de la contratación informática, muchas son las perspectivas, clasificaciones y estructuras sobre las que se puede trabajar, todas ellas conllevan el riesgo de acentuar la importancia de ciertos aspectos, olvidando otros, que desde el punto de vista de un determinado autor, pueden tener menor incidencia. En cualquier caso, y con independencia de otros planteamientos de indudable acierto, hemos considerado conveniente adentrarnos en un estudio global de los contratos sobre el software, haciendo hincapié en la protección que al mismo se otorga, y de la que dependerá el planteamiento, amparo y características, en cierto modo, de los distintos tipos contractuales.

Es indudable que el software es el elemento más peculiar y caracterizador de lo que hemos venido llamando contratación informática. La mayor brecha entre la contratación ordinaria y la contratación informática, la abre precisamente la especial naturaleza y regulación de la que goza el software.

El software puede ser objeto de múltiples figuras negociales, desde su creación, comercialización, instalación, modificación y mantenimiento. En este apartado haremos mención de las figuras más específicas y utilizadas en la práctica, sin que ello suponga un estudio exhaustivo de todas las que existen o pudieran existir, según vayan naciendo o modificándose las necesidades del usuario.

El Software como objeto contractual

Un primer paso indispensable para el tratamiento de los contratos sobre el software, es precisamente perfilar este concepto.

JAVIER RAMIREZ IGLESIAS[47] define el software, desde un punto de

■[47] JAVIER RAMIREZ IGLESIAS.- "El status negocial de los programas de ordenador: contratos sobre software".- Revista Informática y Derecho número 12,13, 14, y 15 Volumen II.- UNED Centro Regional de Extremadura, Mérida 1.996.

vista estricto, como esos programas que cuando se conjugan con la "máquina", son capaces de procesar información al objeto de ejecutar o alcanzar una determinada función, tarea, o resultado.

Nuestra Ley de Propiedad Intelectual, cuyo Texto Refundido fue aprobado por RD Legislativo de 12 de Abril de 1.996, núm. 1/96, define en el art. 96, a los efectos de la protección de la referida ley, como programa de ordenador, 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 o fijación.

Pero el R.D. 1/96, a los efectos de proyectar su cobertura, establece, en el segundo párrafo del mismo punto del art. 96, que la expresión "programa de ordenador" comprenderá también su documentación preparatoria. La documentación técnica y los manuales de uso de un programa gozarán de la misma protección que el Título VII del referido R.D. 1/96 dispensa a los programas de ordenador.

De esta forma, nuestro legislador se inclina por una concepción amplia de programa de ordenador, como producto de la capacidad creadora del hombre que ha de ser protegido de forma minuciosa[48].

El proceso de creación[49] del programa, parte de la idea de su autor de solventar un problema o cumplir una función. Todo programa pretende, en términos generales, dar solución a un problema circunscrito en una actividad, pudiendo tener una aplicación general para un determinado sector, o incluso para una persona en concreto. En esta primera fase, deberán establecerse los objetivos, concretando los problemas y determinando las especificaciones funcionales.

■ [48] El punto segundo del artículo 1 de la derogada Ley sobre Protección Jurídica de Programas de Ordenador, incluía también dentro de la expresión programa de ordenador, la denominada documentación preparatoria.

■ [49] Explicación de RACICOT sobre el proceso de creación de programas, citado por GUILLERMO OROZCO PARDO.- "Informática y Propiedad Intelectual".- Actualidad Informática Aranzadi, núm. 19.- Abril de 1.996

El analista elabora un documento que contiene una serie de funciones que el programa deberá realizar, logrando así el objetivo previsto, con la consiguiente solución del problema planteado. El análisis de esta forma, constituye el eje del futuro programa, pero aún así no son las ideas en sí mismas, objeto de protección a través de la propiedad intelectual, sino la forma de expresarlas, por lo cual, el análisis funcional no es objeto de protección[50].

Seguidamente, en el proceso de creación del programa, se procede a segregar la obra en módulos, que a su vez, se subdividen y se determinan las relaciones, los "interfaces" entre los componentes, lo que constituye la etapa de "arquitectura del programa"[51].

Con posterioridad el autor determina el método de solución del problema, siendo esta fase, la de la lógica o algoritmo del programa, donde se describe gráficamente la lógica del programa por unidades interrelacionadas, que desarrollan las diferentes etapas y los flujos de datos. El autor, una vez elegido el lenguaje de programación, codifica el programa en ese lenguaje, creando el programa fuente.

El programa, en lenguaje fuente, ha de ser traducido a lenguaje objeto para que se adapte al ordenador.

El llamado lenguaje máquina suele estar compuesto por una sucesión numérica de dos valores (0 y 1), es por lo tanto un lenguaje binario, (ya que todos los dispositivos del sistema y los medios de almacenamiento de datos disponen únicamente de dos estados[52]). El lenguaje máquina, puede asimismo estar compuesto por un lenguaje hexadecimal, formado por combinación de números y letras. En cualquier caso, las series de unidades de tales códigos se representan en

■50 XAVIER RIBAS.- "Protección Jurídica de los Programas de Ordenador". Institute for International Research España 1.994.

■51 XAVIER RIBAS.- Obra ya citada.- conceptúa el análisis orgánico, como la fase de elaboración del programa en la que se determinan los métodos, lenguajes y sistemas operativos a utilizar, se diseña el algoritmo, se realizan los diagramas de flujo y se describen los menús y el display gráfico de las pantallas.

■52 JAVIER RAMIREZ IGLESIAS.- Obra ya citada

el ordenador en dos estados, como ya hemos señalado, que suponen la existencia o inexistencia de corriente eléctrica o un alto o bajo voltaje de corriente.

El programa traducido al lenguaje máquina se insertará en un soporte material, que ya puede ser leído por el ordenador, y de esta forma, llegamos al soporte físico de la obra creada por un autor.

Una vez finalizadas estas fases, se procede a la comprobación del mismo elaborándose la documentación necesaria para su utilización.

Protección Jurídica del software

La protección jurídica del software, viene determinada fundamentalmente por la Ley de Propiedad Intelectual, Texto Refundido aprobado por RD Legislativo de 12 de Abril de 1.996, núm. 1/96, que supone una importante garantía, dadas las características técnicas del software y la facilidad para vulnerar los derechos de su legítimo titular.

El referido Texto Refundido viene a sustituir y unificar la dispersa normativa que sobre esta materia y como respuesta al acuciante empuje de las nuevas necesidades, se había venido promulgando en nuestro país[53].

El R.D. 1/96 determina en su art. 1 que la propiedad intelectual de una obra literaria, artística o científica, corresponde al autor, por el solo hecho de su

■[53] La Disposición Derogatoria Unica de la Ley 1/96 deroga las siguiente leyes: 1) Ley 22/1987 de 11 de Noviembre, de Propiedad Intelectual; 2) Ley 20/1.992 de 7 de Julio de Modificación de la Ley 22/87 de 11 de Noviembre de Propiedad Intelectual; 3) Ley 16/1.993 de 23 de Diciembre de Incorporación al Derecho Español de la Directiva 91/250/CEE de 14 de Mayo, sobre la Protección Jurídica de Programas de Ordenador; 4) Ley 43/1.994 de 30 de Diciembre de Incorporación al Derecho Español de la Directiva 92/100/CEE de 19 de Noviembre sobre derechos de alquiler y préstamo y otros derechos afines a los derechos de autor en el ámbito de la propiedad intelectual; 5) Ley 27/1.995 de 11 de Octubre de Incorporación al Derecho Español de la Directiva 93/98/CEE del Consejo, de 29 de Octubre, relativa a la armonización del plazo de protección del derecho de autor y de determinados derechos afines; y 6) Ley 28/1.995 de 11 de Octubre de Incorporación al Derecho Español, de la Directiva 93/83/CEE del Consejo de 27 de Septiembre sobre coordinación de determinadas disposiciones relativas a los derechos de autor y derechos afines a los derechos de autor, en el ámbito de la radiodifusión vía satélite y de la distribución por cable.

creación, considerando en su art. 5, punto primero, como autor, a la persona natural que crea alguna obra literaria, artística o científica, no obstante, dispone este mismo artículo en su punto segundo, que de la protección que esta ley concede al autor, se podrán beneficiar personas jurídicas en los casos expresamente previstos en la misma.

Concretamente, y por lo que se refiere a los programas de ordenador, la Ley, en su art. 97, considera autor a la persona o grupo de personas naturales que lo hayan creado, o a la persona jurídica que sea contemplada como titular de los derechos de autor en los casos expresamente previstos por esta ley[54]. Cuando se trate de una obra colectiva, será considerado autor, salvo pacto en contrario, la persona natural o jurídica que la edite y divulgue bajo su nombre[55].

Cuando el programa de ordenador sea resultado de la colaboración entre varios autores, la propiedad será común, correspondiendo a todos ellos en la proporción que determinen[56].

Si el creador es trabajador asalariado y crea el programa en el ejercicio de las funciones que le han sido confiadas o siguiendo las instrucciones de su empresario, la titularidad de los derechos de explotación corresponderán exclusivamente al empresario, salvo pacto en contrario.

Exige por lo tanto el anterior supuesto, que el creador sea un trabajador asalariado, y que el programa sea fruto de su relación laboral, presumiéndose que

■[54] Uno de estos casos es el del art. 97 punto 5 para los programas de ordenador, que dice "que la protección se concederá a todas las personas naturales y jurídicas que cumplan los requisitos establecidos en esta ley para la protección de los derechos de autor.

■[55] El art. 8 del R.D. 1/96 define la obra colectiva como la creada por la iniciativa y bajo la coordinación de una persona natural o jurídica, que la edita y divulga bajo su nombre, y está constituida por la reunión de aportaciones de diferentes autores, cuya contribución se funde en una creación única y autónoma, para la cual haya sido concebida, sin que sea posible atribuir separadamente a cualquiera de ellos, un derecho sobre el conjunto de la obra realizada.

■[56] El art. 7 del R.D. 1/96, al referirse a las obras de colaboración establece en el último inciso de su punto 4, que en lo no previsto en esta Ley, se aplicarán a estas obras, las reglas establecidas en el Código Civil, para la comunidad de bienes (art. 392 y ss. Cc).

aquel cede los derechos de explotación del programa a quien le ha empleado, salvo que haga constar lo contrario en su contrato de trabajo.

Problema diferente al anteriormente planteado, se presenta en los programas realizados por encargo, para los que la Ley de Propiedad Intelectual guarda silencio, por lo que tendremos que acudir al art. 43 de la citada Ley, que regula la transmisión inter vivos de los derechos de explotación.

A pesar de todo lo dicho, el art. 100 de nuestra LPI establece que no se necesitará autorización del titular salvo disposición contractual en contrario, para la reproducción o transformación de un programa de ordenador, incluida la corrección de errores, cuando dichos actos sean necesarios para la utilización del mismo por parte del usuario legítimo, con arreglo a su finalidad propuesta, incluso la realización de una copia de seguridad por parte de quien tiene derecho a utilizar el programa, no podrá ser impedida por disposición contractual, en cuanto resulte necesaria para dicha utilización.

Asimismo, el citado art. 100 del T.R. de la Ley de Propiedad Intelectual, dentro de los límites a los derechos de explotación, faculta al usuario legítimo de la copia de un programa para estudiar o verificar su funcionamiento, sin autorización del titular, para determinar las ideas y principios implícitos en cualquier elemento del programa, estableciéndose como requisito para ello, que se haga durante cualquiera de las operaciones de carga, visualización, ejecución, transmisión o almacenamiento del programa.

Tampoco podrá el autor, salvo pacto en contrario, impedir que el cesionario titular de derechos de explotación realice o autorice la realización de versiones sucesivas de su programa y de programas derivados del mismo. No será necesaria la autorización del titular del derecho para la reproducción total o parcial, la traducción, adaptación, arreglo o cualquier otra transformación de un programa de ordenador y la reproducción de los resultados de tales actos, cuando sean indispensables para obtener la información necesaria para la interoperatividad de un programa, creado de forma independiente con otros programas, siempre que tales actos sean realizados por el usuario legítimo, o cualquier otra persona facultada para utilizar una copia del programa, o en su nombre por parte de una persona debidamente autorizada; que la información necesaria para conseguir la interoperatividad no haya sido puesta previamente de una forma fácil y rápida a disposición de las referidas personas, limitándose dichos actos a las partes del programa original que resulten necesarias para

conseguir la interoperatividad. La información así obtenida, se utilizará de forma exclusiva para conseguir la interoperatividad del programa creado de forma independiente, pudiendo comunicarse a terceros únicamente cuando sea necesario para la referida interoperatividad, no pudiéndose utilizar para el desarrollo, producción o comercialización de un programa similar en su expresión o para cualquier otro acto que infrinja el derecho de autor.

En cualquier caso estas disposiciones de nuestra LPI no podrán interpretarse de forma que perjudiquen injustificadamente los legítimos intereses del titular de los derechos o sean contrarios a la explotación normal del programa informático.

De esta forma, se recoge la idea de la Comisión de la CEE, en cuanto al fomento de la interoperatividad entre los programas, como la capacidad de los mismos para intercambiar información y utilizar mutuamente la información así intercambiada[57].

No debemos olvidar que el programa de ordenador únicamente será protegido si fuese original, aplicándose la protección prevista en la LPI a cualquier forma de expresión del mismo, extendiéndose a sus versiones sucesivas y programas derivados, excepto, lógicamente, aquellos que tengan como finalidad ocasionar efectos nocivos en un sistema informático.

Lo que indudablemente, como establece la Ley, no queda protegido por los derechos de autor, son las ideas y principios en los que se basan los elementos de un programa de ordenador.

La protección que otorga nuestra Ley diferencia la autoría de persona natural, de la de persona jurídica. En el primero de estos casos, la duración de los derechos de explotación en los términos del art. 99 del T.R., se extenderá a la vida del autor y sesenta años después, desde su muerte o declaración de fallecimiento, con las particularidades que para las obras realizadas en colaboración y las

■[57] La posibilidad de comunicarse se localiza en el interface que contiene unos protocolos de acceso que deben coincidir con los de otro programa que vaya a entrar en comunicación con él, tal como señala XAVIER RIBAS ALEJANDRO, en su ponencia "Protección Jurídica de los Programas de Ordenador", antes reseñada.

colectivas dispone el art. 28. Cuando se trate de persona jurídica, la duración de los derechos será de sesenta años a contar desde el uno de enero del año siguiente a la divulgación lícita del programa, o al de su creación si no hubiera sido divulgado.

El art. 101 posibilita la inscripción en el Registro de la Propiedad Intelectual, de los derechos sobre programas de ordenador, sus sucesivas versiones, y programas derivados.

La infracción de los derechos es tratada en el art. 102 del TR de la Ley, dedicándose el art. 103 a las acciones y procedimientos del titular de los derechos, con remisión al título I, Libro III, de la LPI, y concretamente al art. 137. 3ª, párrafo segundo y al art. 136.3, en relación con el art. 134.2 del referido T.R.

La protección del software viene dada fundamentalmente por la LPI, o si se prefiere, a través de los derechos de autor, pero no es la única vía que se puede utilizar. La propia LPI, en el párrafo segundo del punto 3 del art. 96, determina que cuando los programas de ordenador formen parte de una patente o modelo de utilidad, gozarán, sin perjuicio de lo que dispone esta Ley, de la protección que pudiera corresponderle por aplicación del régimen jurídico de la propiedad industrial, estableciendo el art. 114, que el contenido del Título VII dedicado a los programas de ordenador, 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. Obviamos la normativa general del derecho de obligaciones y contratos, cuyo estudio sobrepasaría los objetivos del presente apartado, y que no supone más que una remisión a la regulación común.

Contratos sobre el software

Muchas son las formas o criterios que la doctrina ha utilizado para la clasificación de los acuerdos comerciales que tienen por objeto al software. Se habla de esta forma, de distintos contratos según la función del software, según el grado de estandarización del mismo, por la vinculación o no del hardware con el software en el acuerdo, por la naturaleza jurídica de los acuerdos contractuales,

por las partes contratantes, o incluso, por los aspectos del contrato "librados a la negociación"[58].

Pero a pesar del indiscutible valor de todos los criterios anteriormente reseñados, creemos más conveniente hacer un breve estudio de los distintos contratos sobre el software, atendiendo a su propia vida, esto es, partiendo de su creación hasta los contratos relacionados con su utilización y mantenimiento.

De esta forma, debemos iniciar este estudio, atendiendo a la EMPRESA CREADORA DEL SOFTWARE.

Estas empresas cuentan con una plantilla de trabajadores asalariados que individualmente, o de forma colectiva, intervendrán en la elaboración del software. Asimismo las citadas empresas pueden contratar a personal ajeno a la misma, para la realización de un software concreto, e indudablemente puede existir una colaboración entre distintas empresas de software.

Antes de contratar con una empresa de software el desarrollo de un programa concreto, es posible, incluso conveniente, acudir a un **CONTRATO DE CONSULTORIA**, con el fin, tanto desde una perspectiva de arrendamiento de servicio como de arrendamiento de obra, de asegurarse un estudio previo de las necesidades y posibles soluciones del cliente en particular.

Asimismo, el consultor podrá incluir dentro de este contrato, la supervisión de la actividad que realice la empresa de software, actuando como intermediario entre cliente y desarrollador. Debe insistirse que quien requiera los servicios de una empresa de software para el desarrollo de un programa que solvente sus necesidades informáticas, no tiene por qué tener los conocimientos técnicos necesarios para un eficiente control del servicio u obra contratada, por lo que, el asesoramiento del consultor le garantizará el buen resultado de su contratación con la empresa de software.

Nada impide que la consultoría sea contratada por la propia empresa de software, para realizar alguna fase del contrato de desarrollo del software, como en la práctica ocurre con cierta habitualidad.

■[58] CORREA Y OTROS.- 'Derecho Informático".

Con independencia de los servicios de consultoría que en términos generales o sobre cuestiones específicas, se pueden concertar, tanto por la empresa-cliente, como por la propia empresa de software, existe el llamado contrato de **DESARROLLO DE SOFTWARE**, por el cual se encarga a alguien técnicamente cualificado, la creación de un programa que solvente las necesidades concretas de un cliente.

Dentro de los contratos de desarrollo, se podrá acudir a un programador autónomo o a una empresa de software (que será lo más habitual), o que sean varias empresas de software las que decidan el desarrollo, de forma conjunta, de un programa.

Indudablemente, es un contrato de resultado que participa de la naturaleza del arrendamiento de obra, exigiéndose una precisión en la determinación de sus cláusulas, que en la práctica, conlleva las máximas dificultades, dado que las partes en principio, definirán el objeto de la prestación, en términos generales, quedando los criterios de calidad y conformidad, en cierto modo poco seguros, pudiendo evolucionar la necesaria colaboración entre las partes contratantes, a medida que se produce el desarrollo pactado, lo que se reflejará en la difícil redacción del documento contractual.

XAVIER LINANT DE BELLEFONDS y ALAIN HOLLANDE[59] aconsejan una particular atención en el momento de negociar estos contratos, a la solidez financiera y reputación del proveedor, dado que estos pactos, por su propia esencia, suponen una cierta duración que exige eliminar al máximo la incertidumbre de una posible extinción de la empresa de software. Indudablemente, la reputación de la empresa de software debe conllevar la imprescindible competencia intelectual y técnica que un contrato de esta envergadura exige.

Por otra parte, los citados autores advierten al cliente sobre las garantías que debe adoptar para evitar que el proveedor no considere su empresa como un área de ensayo y experimentación, prefijándose de manera detallada los plazos de

■[59] XAVIER LINANT DE BELLEFONS y ALAIN HOLLANDE.- Contrats Informatiques et télématiques.- J. DELMAS et Cie.- 2ª Edición.

entrega y el pago de las prestaciones.

En esta misma línea, JAVIER RAMIREZ IGLESIAS[60] insiste en el "documento de especificaciones" como uno de los elementos esenciales en el contrato de desarrollo del software (que no suele formar parte del contrato propiamente dicho), que recogerá en detalle el objeto del contrato, conteniendo información de lo que va a realizar el software, sin entrar a determinar la forma o el modo en que lo va a llevar a cabo.

El documento de especificaciones normalmente incluirá la descripción funcional del software; la descripción del equipo en el que el software va a operar; así como las especificaciones de los sistemas operativos, los lenguajes de programación y otros programas con los que se interconectará; los informes sobre rendimiento del software; las normas de programación y documentación[61].

La principal diferencia entre el contrato de desarrollo de software y el de consultoría, se centra en que el primero se dará cuando el cliente tenga unos requerimientos concretos para la creación de uno o varios programas; mientras que en la consultoría entrarán en juego un conjunto amplio de servicios solicitados, sólo alguno de los cuales serán posteriormente incluidos en el desarrollo del software[62].

JAVIER RAMIREZ IGLESIAS, en su trabajo "El status negocial de los

■[60] JAVIER RAMIREZ IGLESIAS.- "El status negocial de los programas de ordenador. Contratos sobre software". Revista Informática y Derecho 12, 13, 14 y 15. Actas Volumen II.- UNED Centro Regional de Extremadura.- Mérida 1.996.

■[61] XAVIER LINANT DE BELLEFONDS y ALAIN HOLLANDE distinguen entre las siguientes fases del análisis y realización de un programa: análisis funcional, análisis orgánico, programación e integración en tiempo real. Una vez concluido el desarrollo del programa, se procederá a la recepción del mismo que conllevará una previa recepción provisional, y la postrera recepción definitiva, en la que se manifestará la conformidad del trabajo realizado, en respuesta a la demanda formulada.

■[62] JOSE MARIA AGUIANO JIMENEZ.- Aguiano & Asociados.- "Problemática en la contratación de desarrollo de programas a medida". Ponencia presentada en las Jornadas del Institute for International Research España S.A..- Madrid 1.995

programas de ordenador contratos sobre el software" (Obra ya citada), incluye, como caso particular de los contratos de desarrollo del software, el contrato de transformación del software, en el que partiendo de un programa preexistente, resulta un programa derivado, fruto de la modificación del primero. Dentro de éstos hace referencia a los que denomina acuerdos de migración del software, que tienen por objeto la adaptación de determinado programa de ordenador a un sistema operativo o para un tipo de ordenadores determinados, que suelen suscribirse entre las empresas creadoras del software y los fabricantes del hardware, asumiendo unos u otros, según los casos, la adaptación objeto del contrato. Por último el citado autor plantea el problema de los contratos de transformación suscritos entre el usuario del mismo y un tercero, en los que deberá atenderse a los términos del contrato de licencia en relación con los arts. 99 y 100 de nuestra LPI.

Con independencia del contrato de desarrollo del software, al que acabamos de hacer referencia, la creación de un software por una empresa o particular que se dedique a estos menesteres, tiene lógicamente y por lo que a nuestro trabajo se refiere, una proyección en el ámbito comercial.

La empresa de software, titular de los derechos sobre un programa de ordenador, pretenderá por su propia naturaleza mercantil, beneficiarse de su creación. De esta forma, acudirá a las figuras contractuales que le permitan obtener los legítimos beneficios que un bien de tan especiales características, pueda reportarle.

La empresa de software puede ceder la totalidad de los derechos de explotación de que es titular, excluyendo los derechos morales, que son irrenunciables. Si esta cesión carece de límites temporales y territoriales, con carácter exclusivo y permitiendo la negociación y cesión de los derechos de explotación a terceros, estaremos ante una figura contractual que se asemeja a la compraventa. Pero a pesar de que existen autores partidarios de calificar esta cesión de derechos como una verdadera compraventa, entendemos que nuestro sistema jurídico impide este tipo contractual, referido a los programas de ordenador, aunque hemos de reconocer que la apariencia jurídica tiende a equiparar ambas figuras.

En cualquier caso, lo habitual, es que el titular de los derechos opte por la licencia como figura contractual más típica, en este ámbito.

Con el término contrato de licencia, englobamos cualquier tipo de cesión de los derechos de explotación, si bien, ordinariamente se viene empleando para referirse a la cesión de los derechos de uso sobre el software. No obstante, podemos hablar de **LICENCIA DE DISTRIBUCION DEL SOFTWARE**, como el contrato por el que el titular de los derechos de explotación, cede los derechos de distribución del software, con el alcance y las limitaciones que en el acuerdo contractual se determine.

Nada impide que el creador del software sea quien asuma, como titular de los derechos de explotación, la distribución de los programas de ordenador, pero a menudo y por una lógica especialización de las funciones en el mercado, el creador firmará un contrato de distribución para que sea el distribuidor quien se encargue de licenciarlo al usuario final, según lo recibe, o adaptándolo a un determinado hardware.

El contrato de distribución tendrá unas características diferentes dependiendo de los distintos tipos de software, que vendrán a determinar los diversos canales de distribución y el propio contenido del contrato, en el que se deberán fijar aspectos de tal importancia, como si la licencia es en exclusiva, o no; si el distribuidor puede valerse de otros distribuidores; si se le entrega el código fuente...

Especial importancia merece el **CONTRATO DE LICENCIA DE USO DEL SOFTWARE,** por ser el más característico de los contratos sobre el software.

Por la licencia de uso, el titular de los derechos de explotación de un programa de ordenador, autoriza a otro a utilizar este programa, a cambio de una retribución, pero conservando el licenciante la propiedad del mismo, por lo que el contenido del contrato se centra en la autorización para el referido uso, sin que por regla general, se transfiera ningún otro derecho.

La cesión de uso puede ser exclusiva o no exclusiva, si bien, normalmente tendrá este último carácter, presumiéndose que la licencia se refiere exclusivamente a la satisfacción de las necesidades del propio usuario licenciatario[63].

■[63] El art. 99 de la L.P.I., en su último párrafo, establece: "..., cuando se produzca la cesión del

Si bien, en puridad, el objeto de este contrato, se limita al programa de ordenador, creemos que se debe incluir la documentación complementaria, que habrá de reflejarse en el contrato, a pesar de las dificultades que surgen en esta materia al estar dominado este ámbito contractual, por los contratos de adhesión.

Realmente el sentido de este acuerdo responde al interés de los titulares del derecho sobre el software, de mantener esta titularidad, y obtener al mismo tiempo, importantes beneficios, lo que lógicamente conllevará, como ya hemos adelantado, la no exclusividad que caracteriza a la cesión, contenido del contrato.

Todo lo anteriormente expuesto nos lleva a la obligación lógica del titular de los programas, de garantizar el derecho que le asiste, para conceder la licencia, así como que los materiales del programa carecen de defectos de diseño o fabricación[64].

De esta forma, la naturaleza del contrato de licencia se presenta con un carácter sui generis, que ha provocado distintas opiniones doctrinales, como la de FEDERICO TERRADO, que lo califica de arrendamiento de servicios, o la de EDUARDO RAMOS MENDEZ[65] que considera que es un contrato que sin ser propiamente, ni una compraventa, ni un arrendamiento, participa de ambas figuras negociales.

El problema de la naturaleza, a nuestro entender, se minimiza al tener una regulación perfectamente determinada por la Ley de Propiedad Intelectual, si bien consideramos muy acertadas las afirmaciones de EDUARDO RAMOS MENDEZ, al señalar esa mixtura de naturaleza.

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...."

■[64] FEDERICO TERRADO SANCHEZ.- "La diversidad contractual en la generación y explotación de bases de datos".- Revista Informática y Derecho, núms. 9,10 y 11, Actas Volumen I.- UNED, Centro Regional de Extremadura, Mérida 1.996.

■[65] EDUARDO RAMOS MENDEZ, LUIS EUGENIO OLIVER y FRANCISCO EUGENIO DIAZ.- "Informática Jurídica. Educación Permanente".- UNED.

No queremos terminar, sin hacer mención a distintos tipos de licencia de uso, que concretan de esta forma, el objeto propio del contrato de licencia[66], y así puede existir una licencia de sistema, por la cual el cliente está capacitado para hacer uso del software, cuando así lo precise, en un procesador cualquiera (licencia de SISTEMA BASICA), en un ordenador perteneciente a una única clase (licencia de CLASE), o bien en un ordenador perfectamente individualizado y registrado (licencia de NODO); licencia de uso concurriente, por la cual el cliente, aún pudiendo hacer uso del software en cualquier momento, éste solo podrá ser utilizado al mismo tiempo por un número máximo de usuarios identificados; licencia temporal, mediante la que el usuario podrá utilizar el software durante un periodo determinado de tiempo; licencia runtime, en la que el cliente podrá utilizar el software, únicamente, en cuanto a sus prestaciones de ejecución, pero no en lo relativo a las prestaciones de programación.

Los referidos contratos de licencia (cuya enumeración no debe considerarse exhaustiva) presuponen un contacto directo entre el suministrador y el usuario, que conlleva una negociación más o menos amplia. Pero existe la llamada licencia de uso no personalizada[67], "shwrink-wrap license", para aquellos paquetes de amplia distribución que por el gran consumo, hace que sea imposible un trato directo y personalizado entre el suministrador y el usuario final, por lo que el software se entrega dentro de un paquete sellado, en cuyo envoltorio aparece un aviso en que se concretan las condiciones de la licencia de uso. La simple fractura del sello, presupone una aceptación de dichas condiciones. Esta figura de licencia puede plantear dudas en cuanto a su validez, o cuando menos, en cuanto a la validez de alguna de sus cláusulas, lo que no impide que sea una fórmula muy habitual.

Este elenco de contratos no cubre todas las posibilidades negociales que con relación al software se presentan en la actualidad y que indudablemente podemos presumir, aparezcan en un futuro, pero en nuestra opinión, son los más característicos. A ellos añadimos otras figuras que por su complejidad e

■[66] JAVIER RAMIREZ IGLESIAS.- Obra ya citada.

■[67] XAVIER RIBAS.- "Protección Jurídica de los Programas de Ordenador".- Revista Informática y Derecho 9, 10 y 11. Actas Volumen I.- UNED Centro Regional de Extremadura.- Mérida 1.996

importancia hemos querido tratarlas en apartados específicos y que sequidamente pasamos a estudiar.

EL LEASING INFORMATICO

1.- Introducción.

Las necesidades empresariales de importantes inversiones en bienes de equipo y los constantes avances tecnológicos exigen al empresario grandes desembolsos de capital, y con ello la búsqueda de sistemas de financiación que permitan y racionalicen un desarrollo económico, que de otro modo se vería, o bien paralizado, o bien sujeto a unos riesgos mucho mayores de lo que la propia actividad empresarial exige.

Todo ello ha llevado a la creación de unas nuevas formas de financiación, origen de nuevos contratos, que suplan las carencias hasta ahora existentes, faciliten el tráfico jurídico y económico y con ello posibiliten un desarrollo más acorde con las necesidades actuales.

En el campo informático y ante la perspectiva de las mismas necesidades, tiene una rápida acogida, siendo cada día más utilizado[68], y adquiriendo, dentro del volumen de operaciones de las sociedades de leasing, una importancia destacada, y todo ello por ser el modo de financiación ideal para los equipos informáticos, lo que no impide grandes resistencias, e incluso negativas a la hora de financiar el software.

Todo ello hace que en el estudio del leasing informático se unan a los problemas comunes de estas operaciones, los que surgen por las características especiales del nuevo objeto financiado.

2.- Concepto y Caracteres. La operación de leasing.

Leasing o arrendamiento financiero, es definido por la Corporación

■[68] ISABELLE DE LAMBERTERIE "Contratos en Informática".- Derecho y Tecnología Informática. Mayo 1.989.

Financiera de HISPAMER[69] como "un contrato mercantil, en que una de las partes, mediante precio determinado, se obliga a adquirir una cosa cierta y ceder su uso a la otra parte, por un periodo de tiempo, al término del cual, ésta deberá devolverla, o, a su elección, comprársela por un precio adicional".

Es necesario distinguir como conceptos diferentes, la operación de leasing y el contrato de leasing.

El desarrollo de una operación de leasing supone en primer lugar que el usuario (A), necesitado de un bien, del que puede equiparle un vendedor (B), elige y conviene con éste las condiciones de su adquisición, incluyendo el precio. Una vez determinados el comprador y vendedor, el usuario solicita la intervención de una Compañía de Leasing o entidad de depósito (C), quien previo examen de la solvencia del usuario y de las características del bien a financiar, adquiere del vendedor (B) con las condiciones convenidas entre A y B, el referido bien. Pero si la Compañía de Leasing es quien adquiere la propiedad del bien, éste es entregado directamente al usuario (A), con quien la sociedad ha convenido cederle con carácter irrevocable, el uso y aprovechamiento durante un periodo de tiempo que coincidirá en principio con la vida económica del bien. Por su parte, el usuario-arrendatario se compromete a pagar a la referida sociedad de leasing, una renta que se habrá calculado para que cubra, durante la vida del contrato: la inversión de la Compañía de Leasing, los gastos financieros y el margen de beneficio.

Al finalizar el contrato de leasing, el usuario puede optar por: adquirir el bien por un precio que supone el valor residual del mismo; o devolverlo a la sociedad de leasing; o prorrogarlo por nuevo plazo y renta menor.

En la práctica, el leasing supone una operación de crédito, garantizada con una reserva de dominio[70]

■[69] Corporación Financiera de HISPAMER.- Cívitas 1.991.

■[70] Fórmula de A. CHARLIER, citada por M. GIOVANOLI.- "El crédit bail (leasing) en Europe: dévelopement et nature juridique" París 1.980.

3.- Naturaleza y Marco Normativo

La naturaleza jurídica del contrato de leasing es una materia que ha sido muy discutida por la Doctrina, si bien la tendencia mayoritaria en la actualidad coincide en su calificación de contrato complejo y mixto.

Hay quien ha considerado al leasing como una venta-arrendamiento, atemperado por una reserva de dominio, lo que vendría a encuadrarlo dentro de un arrendamiento con opción de compra.

Otra tesis, encabezada por GIOVANOLI[71], asimila el leasing a un préstamo de dinero que hace el intermediario financiero al usuario, pero como señala CABANILLAS[72], en realidad la sociedad de leasing no presta dinero al usuario, sino que con dinero de ella, compra al proveedor los bienes designados por el usuario, conserva su propiedad y los cede en uso a éste; si fuera préstamo, sigue diciendo este autor, el usuario compraría directamente los bienes.

Para otro sector doctrinal, el leasing es un contrato de compraventa a plazos con reserva de dominio, con la finalidad para el usuario de llegar a ser dueño del objeto de este contrato, al cabo de un cierto tiempo, ejercitando la opción de compra, pagando durante este periodo de tiempo un canon que lleva incorporada una parte alícuota del precio de la cosa, tesis mantenida por el Tribunal Supremo en Sentencia de 28 de Marzo de 1.978.

Entre otros, CABANILLAS[73] defiende la naturaleza del leasing como arrendamiento, por la cesión temporal del uso de una cosa, a cambio de una renta periódica, y al que se añade como accesoria la opción de compra (que no es exclusiva del leasing). Sin duda, el arrendamiento presta al leasing sus

■[71] GIOVANOLI.- Obra ya citada.

■[72] CABANILLAS SANCHEZ.- "La Naturaleza del leasing o arrendamiento financiero y el control de las condiciones generales", en ADC 1982, II.

■[73] CABANILLAS SANCHEZ.- Obra ya citada.

mecanismos, pero es precisamente su finalidad, la que los diferencia. El objetivo del leasing no es que se pague una renta por el uso de un bien, sino garantizar el reembolso por un tercero de una serie de pagos por la adquisición de un bien puesto a su disposición[74].

ISABELLE DE LAMBERTERIE[75] afirma que el leasing es ante todo una operación financiera, concebida como instrumento de crédito que busca financiar equipos de uso profesional.

Por su parte, GERARDO NIETO BRIZUELA[76] dice que el arrendamiento financiero no es otra cosa que un producto financiero destinado a sociedades, profesionales y empresarios, configurándose como un negocio mercantil complejo, de objeto exclusivo.

FERNANDO GARCIA SOLE[77] considera que a la vista de nuestra legislación, el arrendamiento financiero, debe encuadrarse como un contrato financiero propio de determinadas entidades de crédito, y distinto tanto de la compraventa a plazos, como del arrendamiento, dado que su finalidad es la estrictamente financiera de posibilitar el uso y en su caso, la adquisición de la propiedad, a cambio de un beneficio, que la ley denomina "cargas financieras"[78].

■[74] EMMANUELLE DE CANNART D'HAMALE Y GUY VANDERBERGHE.- El contrato de Leasing y la Informática.- Le droit des contrats Informatiques, principes applications.- Societé d'etudes morales, sociales et juridiques.- Namur 1.983.

■[75] ISABELLE DE LAMBERTERIE Obra ya citada.

■[76] GERARDO NIETO BRIZUELA.- Despacho Jurídico Gaudeamus.- "Cuales son los aspectos jurídicos más relevantes del arrendamiento financiero de hardware y software" Institute for International Research España S.A. Madrid Febrero 1.994.

■[77] FERNANDO GARCIA SOLE.- Obra ya citada.

■[78] La finalidad financiera, dice CABANILLAS (defensor de la naturaleza arrendaticia del leasing) simplemente determina que tenga el carácter de arrendamiento especial, pues la misma se superpone a la causa del contrato: la cesión onerosa del uso y disfrute de bienes durante el plazo estipulado.

LACRUZ BERDEJO[79] lo califica de contrato atípico, sui generis y no homologable a otro de los tradicionales, necesitado de una propia y peculiar disciplina[80].

Nuestro legislador únicamente se ha ocupado del leasing en el art. 128 de la Ley 43/1.995 de 27 de Diciembre sobre el Impuesto de Sociedades, y la Disposición Adicional Séptima de la Ley 26/88 de 29 de Julio sobre Disciplina e Intervención de las Entidades de Crédito[81], cuyo número primero dice: "tendrán la consideración de operaciones de arrendamiento financiero, aquellos contratos que tengan por objeto exclusivo la cesión del uso de bienes muebles o inmuebles, adquiridos para dicha finalidad, según las especificaciones del futuro usuario, a cambio de una contraprestación consistente en el abono periódico de determinadas cuotas. Los bienes objeto de cesión habrán de quedar afectados por el usuario únicamente a sus explotaciones agrícolas, pesqueras, industriales, comerciales, artesanales, de servicios o profesionales. El contrato de arrendamiento financiero incluirá necesariamente a su término, una opción de compra, a favor del usuario"[82].

Compartimos la crítica que hace GARCIA SOLE[83] a la denominación de "arrendamiento" que utiliza nuestro legislador, ya que no nos parece correcta para el contrato de leasing, que es de carácter eminentemente financiero, si bien hemos de reconocer que el término "arrendamiento financiero" está ya consagrado.

En todo caso y ante la carencia de una legislación específica suficiente, hemos de aplicar la Ley de Venta de Bienes Muebles a Plazos de 1.965 con

■[79] LACRUZ BERDEJO.- Obra ya citada.

■[80] Se inclinan también por esta teoría BROSETA, GARRIGUES Y SANCHEZ CALERO.

■[81] La Disposición Derogatoria Unica de la Ley 43/1.995 en su núm. 19 establece que a la entrada en vigor de la referida Ley quedarán derogados los apartados 2, 3, 4, 5, 6 y 7 de la Disposición Adicional Séptima de la Ley 26/1.988 de 29 de Julio sobre Disciplina e Intervención de las Entidades de Crédito.

■[82] Sustituye a la anterior definición del art. 19 del RDL 15/77 de 25 de Febrero.

■[83] GARCIA SOLE.- Obra ya citada.

carácter subsidiario[84].

4.- Elementos Contractuales del Leasing

4.A Elementos Personales

Partiendo del concepto de operación de leasing, debemos establecer como elementos intervinientes en todo el proceso que estamos estudiando, en primer lugar, al vendedor del objeto sobre el que va a recaer el arrendamiento financiero. Por otra parte, la Compañía de Leasing que tiene una función evidentemente financiera y que vincula de alguna forma al vendedor con el usuario-locatario, que ha solicitado su intervención. Es la propia naturaleza de la operación financiera la que determina la posición e interrelación de estos tres elementos personales.

4.B Objeto del Leasing

Como ya se ha señalado, el objeto del leasing es la financiación de un bien mueble o inmueble, que se verá afecto a una actividad empresarial o profesional. Concretamente en materia informática, el objeto se centrará sobre el hardware en su sentido más amplio, o sobre el software, como soporte lógico y conceptuado como algo más que un simple programa de ordenador, y así, teniendo en cuenta las disposiciones-tipo de la Organización Mundial de la Propiedad Intelectual (OMPI), debemos considerar en el software, tanto el programa como su descripción y sus instrucciones[85].

V.- Cláusulas y condiciones generales de un contrato de leasing.

Partiendo del carácter complejo con que se presentan las operaciones de

■[84] La Sentencia de 28 de Marzo de 1.978 calificó el negocio como venta de bienes muebles a plazos y aplicó su régimen, por apreciar simulación relativa de venta bajo la apariencia formal de arrendamiento financiero, según deducía de las condiciones particulares del contrato.

■[85] FERNANDO GARCIA SOLE.- Obra ya citada.

leasing y más concretamente, atendiendo a la diferenciación ya hecha, el contrato de leasing, en la práctica, se manifiesta como contrato de adhesión. La colaboración por parte del usuario en la determinación de las cláusulas y condiciones del mismo, se reduce al máximo, limitándose en la mayoría de los casos a una simple aceptación de los modelos que la compañía de leasing le propone. Por ello, aparecen una serie de condiciones o cláusulas que, en ocasiones, pueden rayar la ilegalidad y que plantean problemas no sólo en cuanto a su aceptación, sino también en cuanto a las posibles soluciones jurídicas que pudieran adoptarse en un supuesto de incumplimiento.

En este momento, no podemos pretender hacer un estudio exhaustivo y pormenorizado de todas las cláusulas y condiciones que pudieran aparecer en un contrato de leasing, pero sí relacionar las más representativas:

1) Asesoramiento adecuado al usuario y devolución de los riesgos.

2) Entrega y Propiedad del bien objeto de leasing.

3) Duración y Opción de Compra.

La duración del contrato de leasing viene en principio determinada por la vida económica del bien, pero en nuestro ordenamiento no podrá ser inferior a dos años, cuando los bienes tengan carácter de muebles[86], para evitar así una amortización excesivamente acelerada. No obstante, la referida amortización puede repartirse en varios contratos de leasing a través de la subrogación contractual[87].

Pero los contratos de leasing cuentan por lo general con una cláusula que

■[86] El art. 128.2 de la Ley 43/1.995 dice que los contratos a que se refiere el apartado anterior (contratos de arrendamiento financiero), tendrán una duración mínima de dos años, cuando tengan por objeto bienes muebles y de diez años cuando tengan por objeto bienes inmuebles o establecimientos industriales. No obstante, reglamentariamente, para evitar prácticas abusivas se podrán establecer otros plazos mínimos de duración de los mismos en función de las características de los distintos bienes que puedan constituir su objeto.

■[87] GERARDO NIETO BRIZUELA.- Obra ya citada.

faculta a la compañía de leasing a poner fin al contrato anticipadamente en un cierto número de hipótesis, entre las cuales merece especial mención la del impago de rentas por parte del usuario, lo que en materia informática puede afectar a la vida de la empresa misma, cuando se refiere a todo un sistema informático.

Este derecho de rescisión se asimila por regla general a una cláusula penal, por lo que la falta de pago de algún canon, dará lugar a la resolución del contrato, y pago inmediato de los cánones no vencidos, siendo de aplicación el art. 1.152 y ss. del Cc. Debe tenerse en cuenta que la cláusula penal no puede tener carácter abusivo, en cuyo caso será de aplicación (cuando menos analógicamente)la Ley de Consumidores y Usuarios de 1.984.

Para concluir, debemos hacer referencia a la esencial cláusula de opción de compra que permite al usuario adquirir el bien financiado por su valor residual, si bien se ha venido afirmando que especialmente en materia informática, esta opción adquiere un carácter ilusorio, ya que el valor para el ejercicio de la referida opción, se establece muy por debajo del efectivo valor residual, dadas las características y rápida evolución de la materia informática. Lo que en ningún caso puede llevarnos a confundir el contrato de leasing, con la esencial cláusula de opción de compra, con el contrato de compraventa a plazos con reserva de dominio.

VI.- Leasing sobre el hardware.

Las operaciones de leasing que recaen sobre el material informático o hardware como componente de un sistema, de principio no tienen por qué plantear especialidad alguna, si bien es cierto que adquiere por su propia naturaleza, notas peculiares.

Por todo ello, reiteramos en este punto todas y cada una de las notas que venimos considerando sobre el contrato de leasing.

Unicamente queremos destacar una serie de caracteres que especifican este tipo de operaciones financieras cuando recaen sobre el hardware.

En primer lugar, ya adelantamos en su momento, que el valor residual por el que el usuario ejercita la opción de compra, al terminar el periodo por el

que se le cedió el uso del bien (característica esencial en los contratos de leasing) es "excepcionalmente bajo"[88], y ello se justifica por el rápido envejecimiento de este material. Ciertamente todo el material informático ha venido sufriendo una vertiginosa evolución que hace que lo que hoy es nuevo, mañana resulte anticuado. Esta situación hará que la opción de compra inherente a los contratos de leasing sea raramente ejercitada por el usuario, lo que supondrá un riesgo añadido para la compañía de leasing. Para evitar esta duplicidad de riesgos, la sociedad de leasing además de reducir al máximo el valor residual, incitando así al usuario a adquirir los bienes en propiedad, suele pactar la posible recompra del material con el vendedor, para el caso de que el usuario no ejercitase la tan repetida opción. Así el vendedor podrá adquirir los bienes que en su momento enajenó por el valor residual fijado en la operación de leasing.

Por otra parte, ha de tenerse en cuenta que si existen limitaciones que recaigan sobre la transmisión del material informático, estas afectan al contrato de leasing, obligando a la compañía de leasing a restringir su oferta. Si el suministrador del material impusiese algún tipo de obligación que afecte al mantenimiento del mismo[89], entendemos, deberán ser asumidas por la compañía de leasing que es la única con la que el vendedor se relaciona, salvo en lo que se refiere a la elección del material por el usuario. Téngase en cuenta, que el vínculo contractual de la compraventa existe exclusivamente entre el vendedor y la compañía de leasing.

El problema que se plantea es similar a la exención de responsabilidades de la compañía de leasing respecto al saneamiento por vicios ocultos. En este caso la compañía de leasing se encargará de incluir en el clausulado del contrato de leasing, la obligación de mantenimiento a cargo del usuario, que ella en principio, no puede realizar por no tener contacto directo con el bien financiado, pero de la que sí responderá ante el vendedor. Otra solución podría ser que el usuario firmase las condiciones de transmisión asumiendo estas obligaciones, lo que quedaría reflejado de una forma expresa en dicho contrato.

■[88] GARCIA SOLE.- Obra ya citada.

■[89] Piénsese en una operación en que existe un pacto de recompra por parte del vendedor, al que lógicamente le interesa garantizar el buen estado del bien.

En cualquier caso, es lógico imaginar que el leasing no recaiga sobre elementos materiales aislados, sino que se contrate sobre un sistema informático en general, en que la evolución de los distintos elementos será diferente, lo que lleva a mezclar componentes comprados y alquilados, por lo que el usuario procurará agrupar distintos contratos que expirarán, a ser posible en el mismo momento y con la misma compañía de leasing[90].

Lo cierto es que los verdaderos problemas del leasing informático se centran en el leasing sobre el software, o si se prefiere, en la parte inmaterial del sistema, que pasamos a exponer.

VII.- Leasing sobre el software.

Partiendo de un concepto amplio de software que incluye, no sólo los programas de ordenador, sino también sus instrucciones, descripciones, documentación auxiliar, etc...[91], debemos poner de manifiesto que si bien jurídicamente puede reconducirse el contrato de leasing a su aplicación sobre el software, no es esta operación el procedimiento más adecuado para su financiación.

Se plantean así, múltiples problemas que requerirán un importante esfuerzo para encontrar soluciones que puedan encuadrarse en este tipo de operaciones, llevándonos a planteamientos que suponen una excesiva laxitud de la propia estructura del leasing.

Como señala GERARDO NIETO BRIZUELA[92], el leasing sobre el software, suscita amplias dificultades que exigen una solución a través del "condicionado" que se pacte entre el proveedor y la entidad de crédito que realiza la operación de leasing, llegando a drásticas consecuencias que harán muy infrecuentes este tipo de operaciones. Este mismo autor señala la posible

■[90] ENMANUEL DE CANNART D'HAMALE y GUY VANDENBERGHE.- Obra ya citada

■[91] Concepto global del software expuesto por el Profesor GARCIA SOLE partiendo de las disposiciones-tipo de la Organización Mundial de la Propiedad Intelectual (OMPI)

■[92] GERARDO NIETO BRIZUELA.- Obra ya citada.

situación de que el usuario no cumpla sus obligaciones financieras, lo que llevaría a la compañía de leasing a optar por la resolución del contrato o exigir el cumplimiento del mismo mediante el vencimiento anticipado, sobre la base del art. 1.124 del Cc. En cualquiera de ambos supuestos, la solución chocará con los derechos que por ley, corresponden al titular del software, lo que llevará a la compañía de leasing a negar una financiación del mismo, contratar exclusivamente con empresa de absoluta solvencia, o a exigir al proveedor compromisos de recompra del bien en el precio de la inversión pendiente de recuperar por parte de la empresa financiadora.

ENMANUEL DE CANNART D'HAMALE y GUY VANDENBERGHE[93] consideran que es dudoso que el software pueda ser objeto de una operación de leasing de una forma independiente del hardware, al que pudiera ir unido. Los citados autores parten de los propios requisitos de una operación de leasing para cuestionar la viabilidad del arrendamiento financiero sobre el software, señalando que éste, al ser un bien incorporal, es difícil equipararlo a los bienes de equipo.

Por otra parte, no se debe olvidar que el software no puede ser objeto de compraventa, sino de mera licencia de uso, en la que se transfiere un derecho limitado o ilimitado, pero normalmente intransferible, por lo que en una operación de leasing, el software se encontrará excluido, tanto por no poder ser comprado, como por no poder ser cedido.

A ello se unen las dificultades que supone la estimación del valor residual del software a los efectos de ejecutar la opción de compra intrínseca en toda operación de leasing, teniendo en cuenta que dado lo rápidamente que evoluciona y se transforma, su valoración no puede limitarse al coste de fabricación ni incluso al de adquisición.

Por todo ello, los referidos autores deducen que el software no puede ser objeto de leasing, y así la financiación y puesta a disposición del mismo, deberá interpretarse como un contrato de licencia o sublicencia. El titular del citado software, se presumirá que admite esta licencia o sublicencia desde el momento en que la compañía de leasing le informa que la licencia de uso por ella adquirida, forma parte de un contrato de leasing.

■[93] ENMANUEL DE CANNART D'HAMALE y GUY VANDENBERGHE.- Obra ya citada.

En definitiva, y dado que lo más habitual será la negociación sobre un sistema informático y no sobre sus componentes independientemente, la respuesta a la posibilidad de concertar una operación de leasing, sería negativa, pues en realidad estaríamos ante un leasing sobre el hardware, unido a un contrato de licencia o sublicencia sobre el software.

Pero hay importantes sectores doctrinales que admiten, sin ningún género de dudas, la posibilidad de una operación de leasing sobre el software. Así el Profesor GARCIA SOLE[94], parte de la distinción entre software de base o de sistema, software útil, y software específico y de aplicación.

El primero de ellos es el que aparece unido al hardware y que no plantea problema alguno, dado que la operación de leasing lo incorporará como parte del ordenador.

Por lo que se refiere al software útil, que es el creado para un sector determinado, y que puede ser aprovechado por un número más o menos amplio de usuarios, debe plantearse la posibilidad de realizar una operación de leasing sobre los derechos de explotación o sobre la licencia de uso. En el primero de estos supuestos, el usuario encargará a la compañía de leasing que adquiera los derechos de explotación y se los ceda en régimen de arrendamiento financiero, explotándolos éste durante un tiempo determinado, pudiendo ejercitar la opción de compra, convirtiéndose así en titular de los derechos de explotación, o no, pudiendo, en este segundo caso, la compañía de leasing, concertar con otros usuarios diferentes operaciones de leasing, o negociarlas directamente. Para todo ello, se requerirá el consentimiento del titular del software, de forma expresa o tácita.

Por lo que se refiere al leasing sobre la licencia de uso del software, normalmente serán las propias casas comercializadoras de los programas de ordenador, las que explotarán por sí mismas los contratos que crean. Si bien, y dado que se permite el arrendamiento de los mismos, no parece haber ningún inconveniente jurídico para su admisión como objeto de la operación de leasing.

■[94] GARCIA SOLE.- Obra ya citada

CAMINO DE MIGUEL[95] admite la posibilidad de este acuerdo financiero, sobre la base de que la compañía de leasing, al adquirir la licencia de uso, adquiere un derecho de usufructo de la misma.

En cualquier caso GARCIA SOLE destaca la necesidad de que aunque se admita que el usufructo es la figura en la que encajar la relación para la formalización de una operación de leasing sobre el software, es necesario que haya sido autorizada la compañía de leasing por el titular del derecho de explotación, de una forma tácita o expresa, teniendo en cuenta que hay una presunción iuris tantum de que la cesión del uso es intransferible, lo que hará que la solución más habitual sea un pacto tripartito entre el titular del derecho de explotación, el usuario, y la compañía de leasing.

Por último este mismo autor estudia el leasing de elaboración de un programa informático o específico para un usuario. En este supuesto se pactará en el contrato de elaboración una cesión de los derechos de explotación en exclusiva a la empresa contratante. Aquí la compañía de leasing encargará la elaboración del programa y será la titular de los derechos de explotación del mismo. Una vez elaborado el mencionado programa, lo cederá en régimen de arrendamiento financiero, con la correspondiente autorización de quien lo elaboró, debiéndose pactar en estos casos minuciosamente las condiciones de la esencial opción de compra.

Con todo lo dicho, no podemos por menos que manifestar que si bien cabría la posibilidad jurídica de realizar una operación de leasing sobre el software, no parece que sea este el procedimiento más adecuado para obtener la financiación requerida por profesionales y empresas en cuanto al referido objeto. No existe, en nuestra opinión, ningún inconveniente jurídico insalvable para admitir la viabilidad de esta operación, si bien los requisitos, estructura y características de este tipo contractual y del software como objeto del mismo, parecen no coordinarse de una manera óptima.

CONTRATO DE MANTENIMIENTO.

1).- CONCEPTO Y NATURALEZA.

■[95] JOSE RAMON CAMINO DE MIGUEL.- "El Leasing de los Programas de Ordenador".- La LEY 1.989

Uno de los contratos más característicos del mundo informático es precisamente el de mantenimiento. En él se reúnen y destacan las notas más específicas del entorno negocial referido a la Informática. Cuando se ha instalado un sistema informático, se ha adquirido un hardware, se ha celebrado un contrato de licencia, de arrendamiento..., una de las partes cuya característica tantas veces mencionada, es el desconocimiento técnico del complejo mundo de la informática y sus procesos, se encuentra dependiendo del óptimo funcionamiento de sus instalaciones informáticas para que su vida negocial sea próspera y beneficiosa. Así, un servicio de mantenimiento que optimice los recursos informáticos, se hace imprescindible.

La paralización de una empresa por un defectuoso funcionamiento de su sistema informático, produciría enormes pérdidas que pueden llegar a ser irreparables, por lo que el empresario ha de contar con un servicio que prevenga este evento o lo corrija en caso de que se produzca.

La complejidad de todo un sistema exigirá que este mantenimiento se extienda tanto al hardware como al software, presentando así este contrato múltiples facetas, posibilidades y versiones.

EMILIO DEL PESO define el contrato de mantenimiento como aquel que se pacta para asegurar la perfecta utilización del bien adquirido, realizar las adaptaciones que sean precisas según las circunstancias e introducir mejoras que se consideren oportunas[96].

MIGUEL ANGEL DAVARA, sin embargo no incluye dentro de los contratos de mantenimiento, la actualización de los programas o la implantación en los mismos de nuevas rutinas que permitan potenciar su utilidad[97].

■[96] EMILIO DEL PESO NAVARRO.- "Cómo analizar los aspectos jurídicos y técnicos más importantes en el contrato de mantenimiento para conseguir el máximo rendimiento de la relación cliente proveedor" Institute for International Research España S.A. III Jornadas sobre contratos Informáticos.

■[97] MIGUEL ANGEL DAVARA Derecho Informático. Aranzadi 1.993.

Pero a pesar de ello, los conceptos dados por la Doctrina del contrato de mantenimiento, tienden a mostrar un carácter más amplio y englobador de diversas actividades, no limitándose a un simple mantenimiento del sistema.

XAVIER LINANT DE BELLEFONDS y ALAIN HOLLANDE[98] afirman que el contrato de mantenimiento puede tener diversas causas que no pueden reducirse a un esquema único, como son: el envejecimiento del sistema, programas mejores que van apareciendo en el mercado, evolución del equipo complementario del sistema, elementos externos...

Asimismo ALBERTO MARCHILI[99] considera que el contrato de mantenimiento es un acuerdo bilateral por el cual una parte, el proveedor, se obliga en forma independiente a mantener en buenas condiciones de funcionamiento, el equipo físico o lógico, indicado por la otra parte, el usuario, que a su vez se obliga a pagar un precio.

En definitiva, serían muchas y muy variadas las definiciones que se podían aportar del contrato de mantenimiento, y considerando la gran variedad de aspectos y matices que pueden tener estas formas negociales, creemos suficiente para conceptuar esta figura, afirmar que el contrato de mantenimiento consiste en el acuerdo de voluntad dirigido a conseguir la optimización de los recursos informáticos, evitando errores, corrigiendo los existentes, realizando las adaptaciones y mejoras impuestas por la evolución técnica y jurídica.

Pero a pesar de lo ya señalado, la forma en que ha evolucionado este contrato nos muestra cómo en un principio, no se consideraba su existencia, por ser algo que iba esencialmente unido a otro contrato, como podía ser el de adquisición de un hardware.

Posteriormente aparecieron las cláusulas de mantenimiento que hoy persisten, haciendo que este contrato no fuera más que una parte de otro principal.

■[98] XAVIER LINANT DE BELLEFONDS y ALAIN HOLLANDE Contratos Informáticos y Telemáticos. El mantenimiento Informático. 2ª Edición J. DELMAS et Cie.

■[99] ALBERTO MARCHILI.- El Contrato de mantenimiento. Agora núm. 6 1983/2.

El paso siguiente supondría la consideración de estos tipos negociales como contratos accesorios o coligados a otros.

En la actualidad, sin embargo, hay una clara tendencia a concertar el mantenimiento como contrato independiente, pues de esta forma los riesgos, responsabilidades, cumplimientos defectuosos o incumplimientos, se diversifican y especifican para cada relación contractual.

NATURALEZA JURIDICA

La cuestión de la naturaleza jurídica de este contrato ha sido ampliamente tratada por la doctrina, al prestarse a las más variadas interpretaciones.

MARCHILI[100] no es partidario de hablar de atipicidad de los contratos de mantenimiento, ya que considera que pueden localizarse bajo diversas fórmulas contractuales típicas, como el arrendamiento de servicios.

FEDERICO TERRADO SANCHEZ[101] entiende que estamos en presencia de una figura contractual perteneciente a la amplia categoría de contratos de arrendamiento de servicios, de los denominados contratos de engineering, en los que se cuidan muy especialmente las condiciones de cada servicio y los aspectos relativos a la responsabilidad de la empresa de servicios por incumplimiento defectuoso de sus prestaciones o no haberlas realizado en los tiempos convenidos.

MARIA DEL CARMEN GETE-ALONSO Y CALERA[102] considera al contrato de mantenimiento como un arrendamiento de obra que comporta una obligación de medios, línea que sigue EMILIO DEL PESO NAVARRO[103].

■[100] MARCHILI.- Obra ya citada.

■[101] FEDERICO TERRADO SANCHEZ.- "La diversidad contractual en la generación y explotación de bases de datos".- Ponencia presentada al II Congreso Internacional de Informática y Derecho. Revista Informática y Derecho Volúmenes 9, 10 y 11, UNED MERIDA 1.996.

■[102] MARIA DEL CARMEN GETE-ALONSO Y CALERA.- "La contratación en materia informática".- LA LEY núm. 3005.- Mayo 1.992

■[103] El art. 1.588 del Código Civil dispone que puede contratarse la ejecución de una obra,

Las opiniones anteriormente expuestas, vienen a identificar la naturaleza de este contrato, o bien con el arrendamiento de servicios o bien con el arrendamiento de obra, lo que supone optar entre contratar una prestación, o un resultado.

Considerado el contrato de mantenimiento como arrendamiento de obra, una de las partes (la empresa de mantenimiento) se obligará a ejecutar un trabajo predeterminado, según las prescripciones contractuales y las reglas de su "arte", en un plazo concreto. Desde este punto de vista, el mantenimiento no supondrá prestar un servicio con independencia del posible resultado, sino que el objeto de este contrato sería precisamente dicho resultado.

Pero el problema de considerarlo como contrato de arrendamiento de obra, es la previa fijación del trabajo a realizar. Realmente un software de mediana entidad nunca está exento de errores y si no se ha determinado previamente el alcance del mantenimiento, el resultado pactado se encontraría con un defecto de indefinición apriorístico que podía dar lugar a una exoneración de responsabilidades.

El problema se agravará si la empresa de mantenimiento es la misma que ha proporcionado el sistema informático, comprometiéndose a hacer los análisis conceptuales y funcionales del software.

De considerarlo un arrendamiento de servicios, como hace CARLOS PEREZ SANZ[104], nos encontramos con el problema de colocar al usuario en una situación de desprotección al contratar exclusivamente la prestación de una actividad que podrá fijarse por horas de trabajo, días de visita..., sin que se le imponga ningún resultado eficiente a la labor del mantenedor.

Podría obtenerse una solución más equitativa y favorable para ambas

conviniendo en que el que la ejecute ponga solamente su trabajo o industria, o también suministre el material.

■[104] CARLOS PEREZ SANZ.- "Cómo gestionar eficazmente los contratos de asistencia y mantenimiento del sistema informático".- Ribas y Rodríguez Abogados Asociados.- 1.992.- INSTITUTE FOR INTERNATIONAL RESEARCH ESPAÑA Madrid 1.994.

posiciones contractuales: orientar el mantenimiento como un contrato que participe de la naturaleza del arrendamiento de servicios y del de obra, en el sentido de no poder exigir un resultado que pudiera tornarse inalcanzable o que fuera difícil de precisar en un principio, pero tampoco dejar al arbitrio de una de las partes, considerar realizadas sus obligaciones por un mero ejercicio infructuoso. Así podemos considerar el contrato de mantenimiento como contrato de servicios, si bien, en su perfeccionamiento, deberán establecerse unos básicos resultados de funcionamiento que muestren, prima facie, el cumplimiento verdadero del mantenimiento.

2) LA RECEPCION DE UN SISTEMA INFORMATICO, LAS GARANTIAS LEGALES Y CONVENCIONALES Y EL MANTENIMIENTO.

La complejidad de los sistemas informáticos y en general de toda la materia informática en su aspecto contractual, hace imposible la simplificación de las posturas en cuanto a la recepción de los bienes informáticos, su buen funcionamiento, su óptimo rendimiento, y por ende, la satisfacción del destinatario del producto.

El proveedor de un bien informático tiene que responder del producto que ofrece y entrega. Las limitaciones de su responsabilidad, no impiden que existan unas garantías legales y que en numerosas ocasiones, se pacten otras convencionales que aseguren un cumplimiento contractual satisfactorio, aún cuando sólo sea eso.

Todo ello, insistimos, no eclipsa la importancia de un contrato de mantenimiento, ni tan siquiera sustituye su utilidad. Los momentos contractuales en que actúan las reparaciones previas a la recepción y las garantías legales o convencionales, deben estar perfectamente diferenciados en el proceso contractual y con ello, en el tiempo.

No podemos entender que la entrega de un sistema informático concebido como una globalidad, sea jurídicamente sinónimo de recepción.

Para que se produzca esta recepción, es imprescindible haber llegado a la aprobación, que requerirá normalmente como fase previa, la entrega del producto informático. La doctrina distingue tres etapas, una vez concluida la obra: a) la verificación de la obra, que supone un examen para determinar si se ha ejecutado

de acuerdo con lo convenido; b) la aprobación que consiste en el juicio resultado de la verificación y que implicará la obligación de aceptar en caso de ser de signo positivo; c) y por último, la recepción, consecuencia de la puesta a disposición del suministrador y la aprobación por el cliente[105].

Cuando la obra sea de una gran complejidad, o si se prefiere, el producto informático suministrado tenga esas complejas características, su examen para verificar si cumple realmente lo solicitado, no puede darse simultáneamente con su entrega, por lo que se llega a una dualidad de recepciones, entre las que mediará el tiempo que prudencialmente se estime para realizar el imprescindible examen de verificación.

La recepción provisional no cubre ninguna clase de defectos, siendo su finalidad únicamente descubrirlos. Una vez transcurrido el plazo entre la recepción provisional y la definitiva, de no haberse denunciado ninguna irregularidad, la recepción, propiamente dicha, se habrá producido.

Si bien nuestro sistema contractual es consensual, esto es, los contratos se entienden perfeccionados por el mero consentimiento, no se entenderá pagada una deuda (art. 1.157 del Cc), en el sentido más amplio que puede darse a esta expresión, sino cuando completamente se hubiera entregado la cosa o hecho la prestación en que la obligación consistía, con lo que, en tanto no se haya cumplido con la obligación asumida en el contrato, el suministrador informático, sea por el título que fuere, seguirá obligado, salvo caso fortuito o fuerza mayor, a entregar aquello a que se comprometió, con todas sus características.

Si el objeto contractual adoleciese de algún error o vicio, tendrá aquel que corregirlo, no por una obligación de saneamiento de vicios ocultos, sino por la obligación de cumplir con la prestación contractual a que se obligó al prestar el consentimiento.

Una vez que la recepción es definitiva, esto es, el cliente ha comprobado

■[105] RICARDO ENRIQUEZ SANCHEZ, CARMELO MADRIGAL GARCIA.- Derecho Civil Obligaciones y Contratos, Vol. V.- Centro de oposiciones Paseo de Juan XXIII, 3, MADRID 1.985.

satisfactoriamente el producto, pueden manifestarse vicios ocultos que no percibió en su examen previo, siendo aquí donde comienza la actuación de la garantía legal.

El art. 1.484 del Código Civil establece que el vendedor está obligado al saneamiento por los defectos ocultos que tuviere la cosa vendida, si la hacen impropia para el uso a que se la destina, o si disminuyen de tal modo este uso que, de haberlos conocido el comprador, no la habría adquirido o habría dado menos precio por ella; pero no será responsable de los defectos manifiestos o que estuvieran a la vista, ni tampoco de los que no lo estén, si el comprador es un perito que, por razón de su oficio o profesión, debía fácilmente conocerlos.

A tenor de esta disposición legal, si el bien, a pesar de haber transcurrido la recepción provisional y la definitiva sin haberse detectado ningún defecto, no sirviese para el uso a que debía ser destinado, el suministrador deberá proceder a su reparación.

Entendemos que no es de aplicación el art. 1.486 de este mismo cuerpo legal que permite al comprador elegir entre desistir del contrato, abonándosele los gastos que pagó, o rebajar una cantidad proporcional del precio a juicio de peritos, dado que un sistema informático sirve para las funciones que se pretenden, o es ineficaz para las mismas, siendo más lógico que rebajar su precio, optar por su reparación, sin perjuicio de, si es imposible esta reparación, resolver el contrato.

La materia informática, como objeto de los contratos, tiene como característica general, la tan repetida complejidad y especialidad técnica que hacen que el que adquiere el sistema, no pueda conocer los defectos de que adolezca el mismo, lo que le hará acudir a un Perito. Pero aún así, consideramos que precisamente las características de estos bienes y servicios hacen inaplicable el último inciso del art. 1.484 del Cc, que exonera de responsabilidad al vendedor.

Nuestro propio Código Civil abre las puertas a unas garantías convencionales e incluso a la desaparición de toda responsabilidad, al establecer en el art. 1.485, inciso 2°, que esta disposición no regirá cuando se haya estipulado lo contrario y el vendedor ignorara los vicios o defectos ocultos de lo vendido.

En un gran número de contratos, señala ISABELLE DE

LAMBERTERIE[106] el proveedor garantiza el buen funcionamiento del sistema durante un tiempo limitado, lo que supone un paso adelante con relación a la simple garantía legal, encontrándose también cláusulas que condicionan, limitan o excluyen la responsabilidad del proveedor.

Por regla general, las garantías convencionales son de naturaleza gratuita, aseguran el buen funcionamiento del sistema en plazos más amplios que las garantías legales y transforman lo que era una sanción, en una obligación, evitando de alguna forma, acudir a los tribunales o a soluciones arbitrales que dilatarían una rápida respuesta; dicha rapidez de respuesta lógicamente se dará si el garante la ha asumido expresamente y no es necesario discutir la procedencia o no de la corrección de un supuesto error, por mandato legal.

Con independencia de estas obligaciones y garantías del suministrador de un sistema informático, en el contrato de suministro se puede estipular una cláusula de mantenimiento o bien celebrar un contrato con la misma finalidad y totalmente independiente.

Este mantenimiento cualquiera que sea su alcance, tiene una naturaleza jurídica y una razón de ser diferente a las garantías reseñadas. Su cobertura va más allá en el concepto y en el tiempo, con las garantías específicas y modalidades que le colocan en un puesto clave dentro de la contratación informática.

3) TIPOS Y GRADOS DE MANTENIMIENTO

Las clasificaciones que la Doctrina hace de los tipos y formas de mantenimiento, son muy numerosas y atienden a una multiplicidad de criterios.

En primer lugar, podemos diferenciar entre lo que podríamos denominar mantenimiento autónomo y no autónomo, desde una perspectiva contractual. Así el cliente puede perfeccionar su contrato de mantenimiento, cualquiera que sea su objeto, con independencia de cualquier otro contrato; o puede también incluir este servicio de mantenimiento como cláusula o anexo de un contrato principal, del que dependerá directamente.

■[106] ISABELLE DE LAMBERTERIE.- "Contratos en Informática. Derecho y Tecnología Informática. Mayo 1.989.

EMILIO DEL PESO NAVARRO[107] distingue entre el mantenimiento del hardware, del software y consultoría.

Este mismo autor, siguiendo a E.B. SWANSON[108] diferencia entre mantenimiento **correctivo,** que tiende a la corrección de errores una vez transcurrido el periodo de garantía; mantenimiento de **adaptación** que supone la modificación del software en función de los cambios legales o de otro tipo que aparezcan; **perfectivo,** que son las mejoras que se realizan debido a las recomendaciones de los usuarios; y **preventivo,** modificaciones que se realizan al objeto, que pueden servir de base a nuevas mejoras.

Otro criterio clasificatorio será el del lugar de realización del servicio de mantenimiento que podrá prestarse: en el domicilio del cliente o en el del proveedor del servicio. En este último caso, si bien resulta en principio menos oneroso para el cliente, supone un mayor tiempo de indisponibilidad del sistema, pudiendo contratarse para software y para hardware, aunque es más habitual en el primero de los casos.

Existen varios métodos de asistencia en el domicilio del proveedor como la telefónica "on line" (a través de un centro de asistencia organizado en los locales del fabricante-proveedor)[109]...

El mantenimiento puede producirse también, como hemos señalado, en el domicilio del cliente, con desplazamiento de personal, que supone menor indisponibilidad del sistema dependiendo de la rapidez con que acude el proveedor, aunque resulta más oneroso.

■[107] EMILIO DEL PESO NAVARRO.- Obra ya citada.

■[108] E.B. SWANSON The dimensions of maintenance proce 2nd Int. Conf Software Engineering IEE Octubre 1.996.

■[109] XAVIER LINANT DE BELLEFONDS y ALAIN HOLLANDE distinguen entre el mantenimiento en el domicilio del proveedor del servicio y el telemantenimiento que según estos autores, se realiza en el domicilio del cliente, sin desplazamiento de personal, pudiendo ser por asistencia telefónica, telemantenimiento automático periódico, por programas de control o telemantenimiento por acceso a un sistema experto.

Por la persona que realiza el servicio de mantenimiento, podemos hablar de mantenimiento directo, entendido como aquel en que el servicio lo presta el fabricante o creador del bien informático que se trata de adaptar, corregir o controlar; mantenimiento por tercero, en el que aparece una tercera persona, diferente a la que une a los contratantes del hardware o del software; o la solución intermedia, en la que una sociedad se interpone entre el usuario y el fabricante, que negociará las tasas de intervención y efectuará sobre un principio idéntico al del seguro, una evaluación de riesgos, que permite reducir el número de intervenciones.

El usuario de esta forma, paga una renta generalmente mensual a la sociedad intermedia, pero acude al fabricante en caso de avería y éste último factura a la antedicha sociedad[110].

4) GRADOS DEL MANTENIMIENTO

Las acciones del mantenimiento tendrán diverso contenido, dependiendo de su referencia al hardware, al software, al personal o incluso al entorno.

La prestación de un servicio, no será lo mismo si estamos ante un simple mantenimiento correctivo o una adaptación completa a las nuevas condiciones surgidas, lo que ha llevado a la Doctrina a establecer cinco grados de mantenimiento, que van desde un servicio sumario a un mantenimiento completo.

Se habla así de[111]:

1.- Primer grado que supone las correcciones más simples o el cambio de elementos consumibles.

2.- Segundo grado que se traduce en el intercambio de ciertos elementos modulares.

■110 XAVIER LINANTE DE BELLEFONDS y ALAIN HOLLANDE.- Obra ya citada.

■111 ISABEL HERNANDO y XAVIER LINANT DE BELLEFONDS y ALAIN HOLLANDE.- Obras ya citadas.

3.- Tercer grado que supone la realización de una serie de pruebas generales para la identificación de los errores acaecidos o de probable aparición.

4.- Cuarto Grado que consiste en un análisis general que puede llevar a la reforma del equipo.

5.- Quinto grado que implica la reestructuración de uno o varios elementos del sistema.

Los tres primeros se realizarán en los locales del cliente, acudiendo a los talleres o al domicilio del fabricante para los dos últimos.

5) ELEMENTOS PERSONALES Y REALES DEL MANTENIMIENTO.

El servicio de mantenimiento puede pactarse dentro de un contrato principal del que forma parte como cláusula más o menos desarrollada, o como anexo; o bien como contrato independiente, lo que no impide que los elementos personales que intervienen en este pacto puedan ser coincidentes en ambos casos.

De una parte, está el usuario o cliente que es quien, poseedor de un bien informático, requiere un servicio de mantenimiento con la amplitud y características específicas que su situación precisa, pudendo pactarse cualquiera de las modalidades de mantenimiento a que hemos hecho referencia en el epígrafe anterior. Por otra parte existe un "mantenedor" que es quien se obliga a realizar las prestaciones que el pacto de mantenimiento contenga.

Si el mantenimiento se pactó como anexo o cláusula del contrato firmado con un proveedor, éste asume las obligaciones que acuerden y que no deben confundirse con las garantías legales o contractuales tratadas en su momento. En este supuesto, el proveedor además se compromete a mantener el bien informático objeto del contrato principal.

De la misma forma el cliente puede pactar el servicio de mantenimiento como contrato independiente con el mismo proveedor y por supuesto con un tercero que cumple las características técnicas que requiere la prestación objeto del mismo.

A su vez es posible que en el servicio de mantenimiento intervenga una empresa intermedia entre el cliente y el fabricante-proveedor. En este supuesto nos encontramos con un doble contrato entre la sociedad intermedia y el fabricante y otro entre la citada sociedad y el cliente, pudiendo también optar por un contrato a tres bandas.

En cualquiera de los casos, como señala CARLOS PEREZ SANZ[112] la empresa que presta el servicio de mantenimiento accede a unos importantísimos datos del cliente, cuya divulgación puede causarle grandes perjuicios, por lo que la confidencialidad se presenta en este negocio jurídico como un elemento imprescindible que hará que en muchos casos el cliente quiera asegurarse que tanto la empresa informática como su personal, guardan el debido secreto, firmándose un pacto de confidencialidad.

El servicio de mantenimiento puede realizarse por el propio personal de la empresa del usuario, lo que quedaría fuera del ámbito contractual y exigiría un potencial económico y técnico importantísimo por parte de éste y una muy cualificada preparación de sus empleados, lo que hace a esta solución inaplicable en la mayoría de los casos.

OBJETO DEL CONTRATO

Es imprescindible establecer de una forma clara en el mantenimiento, las prestaciones que se contratan, siendo el contenido del mismo diferente según la clase de mantenimiento que se precise y el tipo de usuario que lo requieran. El mantenimiento puede recaer sobre el hardware, sobre el software, o sobre ambos. Si bien el mantenimiento del hardware ha sido el más empleado, en la actualidad tiende a imponerse o bien el del software, o bien el conjunto de hardware y software.

Se prefiere por razones económicas, tener unidades de reemplazo y requerir su reparación en un momento determinado, antes que sufrir el coste de contratar un mantenimiento constante.

■[112] CARLOS PEREZ SANZ.- Obra ya citada.

Cuando el contrato de mantenimiento recae sobre el software, debe tenerse en cuenta, que estamos en presencia de un bien inmaterial[113] que caracteriza de forma diferente respecto a aquellos contratos que versan sobre bienes materiales.

Un bien inmaterial es según EDUARDO GALAN[114] fruto o creación de la mente que necesita para que se haga perceptible para el mundo exterior, ser plasmado en un soporte y que puede ser disfrutado simultáneamente por una pluralidad de personas.

De esta forma XAVIER LINANT y ALAIN HOLLANDE[115] afirman que las operaciones de mantenimiento son bastante corrientes cuando se trata del hardware, llegando a considerar como una "ficción terminológica" el mantenimiento del software. Los referidos autores estiman que es posible intervenir en un software para corregir errores (intervenciones que normalmente se realizan en el periodo de puesta a punto y por lo tanto quedan excluidas del mantenimiento) y para adaptarlo a unas nuevas condiciones (tampoco se trata de mantenimiento sino de desarrollo parcial), concibiendo sólo el mantenimiento del software como accesorio del mantenimiento del hardware.

Observamos cómo los contratos que tienen por objeto el software, revisten unas características propias que deben ser tratadas con un cuidado exquisito y que nos obligan a remitirnos a una legislación específica. De esta forma, debemos acudir al Texto Refundido de la Ley de Propiedad Intelectual, Real Decreto Legislativo de 12 de Abril de 1.996, núm. 1/96 que establece una serie de actos sujetos a restricciones y límites a los derechos de explotación, que afectan o pueden afectar al contrato de mantenimiento.

El art. 99 del TR de la LPI dispone el contenido de los derechos de explotación en el mismo sentido que establecía el derogado art. 4 de la Ley 16/93

■113 EMILIO DEL PESO NAVARRO.- Obra ya citada.

■114 EDUARDO GALAN Rapport Espagnol. Les Logiciels. Revista ALI núm. 12 Nov. 1.989, citado por EMILIO DEL PESO en la obra antes señalada.

■115 XAVIER LINANT DE BELLEFONDS y ALAIN HOLLANDE.- Obra ya citada.

sobre Protección Jurídica de Programas de Ordenador[116].

El art. 100 del TR 1/96 establece asimismo los límites a los derechos de explotación, reproduciendo en su punto primero el contenido de los artículos 5 y 6 de la derogada Ley 16/93.

Debemos destacar el punto 7 del art. 100 del TR 1/96 en el que se dice que las disposiciones referentes a la dispensa de autorización del titular para obtener la información necesaria para la interoperatividad de programas, no pueden interpretarse de manera que permitan que su aplicación perjudique de forma injustificada los legítimos intereses del titular de los derechos o sea contraria a una explotación normal del programa informático.

La prestación del servicio por el mantenedor, requerirá que tanto el software como el hardware, estén perfectamente determinados, requisito que lleva como consecuencia que la obligación de mantenimiento desaparezca, cuando el error detectado se deba a una modificación en el programa realizada por el cliente.

GENEVIEVE DEWULF, MARC SCHAUSS y ROLAND LESUISSE[117] aconsejan ante la posibilidad de que adopte la naturaleza de obligación de medios, la redacción de un "libro de a bordo", registrando las demandas de intervención, en que será anotado el número, tiempo, contenido y resultado de las intervenciones del prestatario.

EMILIO DEL PESO NAVARRO[118] ha señalado que las funciones de desarrollo y mantenimiento del software han venido realizándose dentro de los sistemas informáticos, siendo la segunda una actividad complementaria. Entiende gran parte de la doctrina que el contrato de mantenimiento de software es un contrato coligado y accesorio del principal que era el de desarrollo del software,

■[116] Nos remitimos en este punto al epígrafe sobre la Protección Jurídica del Software (X.3)).

■[117] GENEVIEVE DEWULF, MARC SCHAUSS y ROLAND LESUISSE.- Obra ya citada.

■[118] EMILIO DEL PESO NAVARRO.- Obra ya citada.

pero poco a poco estos contratos van adquiriendo entidad propia y en cierto modo independiente.

Los servicios informáticos de las empresas han empezado a contemplar la función de mantenimiento como separada del desarrollo, revalorizando la misma. La contemplación de las dos funciones como entidades distintas, obliga a marcar de forma clara la frontera entre una y otra.

CARLOS PEREZ SANZ[119] ha señalado como módulos más habituales, los siguientes:

a) Hot line

b) Adaptación a cambios legales

c) Corrección de errores

d) Adaptación a cambios sectoriales

e) Nuevas versiones o actualizaciones.

f) Recuperación de Información.

g) Optimización y compresión del disco duro

h) Servicio de Back up[120].

i) Detección y prevención de virus

■[119] CARLOS PEREZ SANZ.- Obra ya citada.

■[120] El back up permite a una empresa continuar con su actividad, a pesar de sufrir cualquier accidente en su sistema. Su objeto es la protección logística y técnica, poniendo a disposición del cliente, por un plazo determinado, un sistema compatible con sus datos y programas que cumpla las funciones esenciales en evitación de un perjuicio grave a la empresa.

■La fórmula más simple de back up es aquella por la que se garantiza, en caso de hardware, otro idéntico para un reemplazamiento provisional o posibilita un acceso a otro hardware.

j) Servicio de escrow o garantía de acceso al código fuente.

k) Gastos de desplazamiento

6) PRINCIPALES CLAUSULAS DEL CONTRATO DE MANTENIMIENTO

Debemos insistir, a pesar de ser reiterativos, que las cláusulas principales de un contrato de mantenimiento estarán en íntima dependencia con el tipo pactado y con los módulos que constituyen su contenido, por lo que al reseñar las siguientes cláusulas, debe tenerse presente siempre este criterio. No obstante algunos de ellos, como la duración o el precio, serán imprescindibles en todos.

Podemos destacar, siguiendo a ISABEL HERNANDO COLLAZOS[121] como cláusulas más habituales, las siguientes:

- alcance del mantenimiento.
- corrección de errores del software.
- tiempos de respuesta.
- actualización de versiones.
- responsabilidad del cliente
- penalizaciones por mantenimiento tardío
- aplicación de las modificaciones realizadas por el cliente
- consecuencias de la extinción del contrato respecto a los programas-fuentes
- renovación o prórroga del contrato.

En esta última línea se manifiesta GENEVIEVE DEWULF, MARC SCHAUSS y ROLAND LESUISSE, añadiendo los métodos de asistencia, la intensidad de la obligación (determinar si es de resultado o de medios) y las posibles cláusulas de exoneración de responsabilidad del mantenedor.

A todos ellos hay que añadir como muy conveniente la cláusula de

[121] ISABEL HERNANDO COLLAZOS.- II Jornadas de la Abogacía Informática.

arbitraje que facilitará y acelerará la solución de los conflictos que entre las partes pudieran surgir. Teniendo en cuenta que la dilación en el tiempo para la resolución de los conflictos puede traer fatales consecuencias para la empresa y el sistema.

Especial atención merecen las cláusulas relativas a la duración, precio y exoneración de responsabilidad contractual.

Por lo que a la duración se refiere, debe establecerse el momento de iniciación del servicio de mantenimiento, que siempre será una vez que hayan cesado las garantías legales o contractuales, de existir éstas.

En el contrato se precisará el periodo de tiempo durante el que se prestará el servicio de mantenimiento, que podrá ser renovado a su finalización, en las condiciones previamente fijadas.

Si no se ha establecido un periodo determinado de duración, el contrato se dilatará en el tiempo hasta que medie un preaviso por la parte que quiera rescindirlo.

Pero la rescisión es en principio muy peligrosa para el cliente, que difícilmente encontrará un mantenedor que, con capacidad suficiente, esté dispuesto a sustituir al primero en las mismas condiciones.

Normalmente, la duración atiende a la vida del hardware que integra el sistema. Si recae sobre el software, los parámetros a tener en cuenta serán: la obsolescencia técnica, la duración de la explotación, los costes de renovación o la amortización de las innovaciones[122].

Pero el tiempo también ha de tenerse en cuenta con relación a estos contratos para determinar no solamente su duración, sino también el cumplimiento o incumplimiento.

Así, si se han fijado unas revisiones periódicas, éstas deberán llevarse a cabo en el momento pactado, pudiendo establecerse sanciones por retraso, para

■ [122] XAVIER LINANT DE BELLEFONDS ALAIN HOLLANDE.- Obra ya citada.

garantizar la eficiencia del servicio. En el caso de mantenimiento preventivo, determinar unas revisiones anuales en uno u otro momento, no supone más que una ventaja de concreción, si bien no modifica sustancialmente la prestación convenida. De esta forma se evita la acumulación al final del periodo de unas revisiones casi simultáneas, para cubrir el cupo de las mismas.

Mayor importancia adquiere la fijación de periodos de intervención en el mantenimiento correctivo, ya que si se ha detectado un error o fallo en el sistema, la mayor celeridad con que se solvente, puede medirse fácilmente en parámetros económicos. Es lógico pensar en la necesidad de establecer unos periodos de servicio y horarios de intervención.

El usuario puede limitar en el tiempo la intervención, bajo la forma de porcentajes de indisponibilidad mensual máxima del software y hardware y de indemnizaciones por retraso[123].

Naturalmente estos periodos dependerán del necesario aviso del cliente, y del lugar en que se proceda a la corrección[124].

En íntima relación con el tiempo, está el precio.

El precio se presenta como uno de los elementos fundamentales en el contrato de mantenimiento, que será objeto de negociación y deberá quedar perfectamente determinado o cuando menos ser determinable en función de una serie de parámetros. Volvemos a insistir en que dependerá del tipo de mantenimiento que se contrate, la forma de fijar este precio.

Puede pactarse un precio a tanto alzado para todo el periodo contractual, solución ésta que nos parece inviable o muy peligrosa, salvo que estemos en presencia de un mantenimiento exclusivamente preventivo, lo que en la práctica es difícil de imaginar. Lógico es, cuando menos, que el mantenimiento sea preventivo y correctivo; y habitualmente tiende a copar, si bien no la totalidad de los módulos posibles, cierto mantenimiento evolutivo. Por supuesto si se fija un

■ [123] GENEVIEVE DEWULF, MARC SCHAUSS, ROLAND LESUISSE.- Obra ya citada.

■ [124] Nos remitimos a lo dicho al tratar los tipos de mantenimiento.

precio a tanto alzado, puede fraccionarse en cuotas, estableciéndose criterios de revisión o actualización.

Parece más correcto establecer un precio base que se incrementará si se supera una facturación determinada. Esta misma idea podrá tener su reflejo en fijar un precio mínimo al que habrá que añadir el coste de cada intervención, según las horas que se empleen, si es dentro del horario comercial, si requiere una rapidez de respuesta mayor que lleve incluso a una reparación nocturna...

Por supuesto, las correcciones pueden tener un nivel de complicación técnica de diferente entidad, que se reflejará a su vez en el precio, como también la distancia del usuario, el lugar donde se realice el servicio de mantenimiento y en general, los módulos que se hayan concertado.

Respecto a la responsabilidad contractual, como en todo contrato, las partes están obligadas a realizar las prestaciones a que se hayan comprometido, si bien en materia informática, la parte económica y técnicamente más fuerte, suele tender a exonerarse de toda responsabilidad. El cliente en el caso del contrato de mantenimiento deberá estudiar la cláusula que tienda a dicha exoneración, dado que no puede ni debe admitirse la exoneración total.

Nada impide, eso sí, que se establezcan una serie de supuestos en los que el mantenedor no sea responsable de las consecuencias de una falla en el sistema.

Las cláusulas exoneratorias nunca pueden eliminar la responsabilidad que por dolo pudiera tener el mantenedor[125].

Asimismo el mantenedor no responderá en caso de fuerza mayor, salvo que expresamente se haya contemplado en el contrato este extremo, o lo imponga

■[125] El art. 1.107 del Cc establece que los daños y perjuicios de que responde el deudor de buena fe son los previstos o que se hubieran podido prever al tiempo de constituirse la obligación y que sean consecuencia necesaria de la falta de cumplimiento.
■En caso de dolo responderá el deudor de todos los que conocidamente se deriven de la falta de cumplimiento de la obligación"
■El art. 1.102 del Cc "La responsabilidad procedente del dolo, es exigible en todas las obligaciones. La renuncia de la acción para hacerla efectiva, es nula."

alguna norma legal[126].

Debe entenderse de aplicación el art. 1124 del Cc que faculta la resolución las obligaciones para el caso de que uno de los obligados, no cumpla lo que le incumbe y la reclamación de daños y perjuicios, o sólo éstos sin resolver el contrato.

La prueba de dicho incumplimiento, y la aplicación de la "exceptio non adimpleti contractus" le corresponde a quien la alega, y requiere control judicial o arbitral que atenderá a la gravedad de las deficiencias.

SALVADOR DARIO VERGEL[127] pone de manifiesto que la suspensión de los servicios de mantenimiento y asistencia técnica sólo puede ser admitida en circunstancias en extremo restringidas, ya que constituye peligro de daño grave irreparable la suspensión de la asistencia técnica a un sistema de elaboración que compromete el funcionamiento de la empresa beneficiaria.

7) CUMPLIMIENTO DEL CONTRATO

Como en todo tipo contractual, las partes estarán obligadas a cumplir con lo que se hubiesen comprometido en el contrato. En el caso del mantenimiento, las prestaciones que engloba esta figura contractual son múltiples, lo que lleva a un muy variado listado de obligaciones por ambas partes.

En términos generales, el proveedor del servicio, tiene como obligación principal, mantener en óptimas condiciones de funcionamiento el equipo determinado por el usuario[128].

La concepción del mantenimiento como una obligación de resultado o de medios, determinará si el usuario debe probar el dolo o culpa del proveedor, en este segundo caso, o si se debe presumir la responsabilidad del mantenedor por el

■ [126] Art. 1.105 Cc.

■ [127] SALVADOR DARIO VERGEL.- Obra ya citada.

■ [128] MARCHILI.- Obra ya citada.

solo hecho de no haber conseguido un resultado, a salvo los supuestos de fuerza mayor.

En caso de un mantenimiento preventivo que supone un control periódico de funcionamiento del sistema informático, no ha de dejarse tampoco el mantenimiento al libre arbitrio del prestador del servicio y deberá especificarse en el contrato, los plazos, parámetros de control, posible recambio de piezas etc...

De no establecerse, tanto en el mantenimiento preventivo, como en el correctivo, plazos de intervención, se estará a la práctica habitual que nos lleva a la conveniencia de que exista una cláusula arbitral en el contrato.

A estas obligaciones habrá que añadir la de confidencialidad ya mencionada y la de consejo y asesoramiento que hemos defendido para todo contrato informático.

En cualquier caso, la conveniencia de una precisión terminológica en este tipo de contratos, se hace más acuciante en el presente, por la laxitud que la obligación de mantenimiento puede conllevar.

Es recomendable hacer referencia a la disponibilidad de personal y el aprovisionamiento de piezas de recambio, garantizando durante un periodo de tiempo viable, la estabilidad del sistema informático.

El cliente indudablemente tendrá que pagar el precio por el servicio de mantenimiento y colaborar con el mantenedor facilitándole el acceso a su local, al hardware y al software, tener a su disposición la información necesaria en ficheros, memorias etc..., e incluso designar a una persona capacitada que actúe de interlocutor con el mantenedor, avisándole sobre la aparición de algún error en el sistema.

Asimismo deberá utilizar el material debidamente y seguir las instrucciones que le pudiera dar el prestador del servicio, consultándole ante cualquier modificación que pudiera repercutir en el mantenimiento.

Una vez firme el contrato de mantenimiento, las partes cumplirán con sus obligaciones pudiendo resolverlo en caso de incumplimiento perfectamente probado por alguna de ellas, con la consiguiente indemnización de daños y perjuicios; indemnización que deberá abarcar tanto el daño producido como el

lucro cesante y que requerirá una prueba exquisita que en muchos casos, y dada la necesidad de mantenimiento, convendrá sólo pedir ésta permaneciendo vigente el contrato.

CONTRATO DE OUTSOURCING

A).- CONCEPTO Y CARACTERES.

Hoy en día las sociedades mercantiles, cualquiera que sea su volumen de facturación, el tipo de negocios que realicen o el ámbito espacial donde se muevan, se encuentran en la necesidad de hacer un uso constante de los medios informáticos para optimizar al máximo sus resultados.

No se puede plantear la existencia de una compañía mínimamente competitiva, sin la decisiva intervención de estos modernos medios, pero lógicamente a todo ello hay que añadir que la progresiva evolución técnica va inexorablemente unida a una mayor complejidad.

Dada la necesidad de utilizar cada vez más información y con mayor celeridad, se impone la búsqueda de una especialización en materia informática: o bien esta especialización se hace desde una perspectiva interna de la empresa, lo que exige una mayor inversión y por ello limita esta opción a las grandes compañías; o bien por el contrario, la gestión informática se exterioriza, encomendándose a un tercero, que de forma especializada se encargará de su funcionamiento, solución más interesante para la gran generalidad de las empresas.

Se nos presenta así una nueva forma de gestionar la actividad negocial sobre la base de la tecnología informática a través de la "externalización" de sus funciones, cómo requisito imprescindible para el mejor desarrollo empresarial.

De esta forma, el empresario centrará toda su atención en el negocio objeto de su empresa, encomendando a otros el manejo de los sistemas informáticos, lo que por regla general llevará a una mejora del servicio y una reducción de costes, junto a otras múltiples ventajas.

RAFAEL ALONSO[129] entiende por outsourcing informático, el servicio independiente que se responsabiliza del óptimo funcionamiento de los sistemas informáticos de la empresa cliente y se preocupa de que dicho sistema sea el idóneo para sus necesidades, teniendo en cuenta tres factores: estructura, recursos humanos y tiempo.

CARACTERES

Se presentan dos causas como principales razones del desarrollo de este tipo negocial. La primera de ellas, referente a la necesidad de reducir costes al liberar a la empresa de los grandes desembolsos que las modernas tecnologías y su vertiginosa evolución precisarían para mantener un nivel apto de competitividad.

La segunda gran base que justifica este contrato, podríamos concretarla con los términos conocimientos técnicos y finalidad empresarial. Entendemos que el encomendar la gestión informática a una empresa especializada en esta materia, indudablemente supondrá un aporte de conocimiento y experiencia que redundarán en beneficio de la empresa, mejorando su eficacia, dado el mejor aprovechamiento de los avances técnicos.

La empresa que subcontrata no solamente tiene acceso a un amplio repertorio de recursos, sino que todas sus miras se dirigirán a su cometido propiamente dicho. Es cierto que como en todo contrato, se originan inconvenientes como la pérdida de independencia, el contraste con la legislación laboral, o los problemas que la titularidad del software y la propiedad intelectual pueden plantear, pero entendemos que las múltiples ventajas que se nos ofrecen, como la flexibilización de recursos, las soluciones a medida, el incremento de capacidad de trabajo, la especialización y la reducción de costes, impondrán su masiva utilización.

■[129] RAFAEL ALONSO "Outsourcing, Presente y Futuro" Artículo publicado en la Revista AMIGOS. Fundación para el desarrollo Directivo, KNOW HOW Business College. Marzo núm. 3 1.996.

B) NATURALEZA JURIDICA

El outsourcing es un contrato atípico, ya que nuestra legislación no lo contempla específicamente. El propio planteamiento de nuestro trabajo y los apartados de este contrato en particular nos permiten observar cómo la mayoría de los contratos informáticos de carácter atípico van adquiriendo una cierta tipicidad práctica o social, al irse repitiendo sus modelos en espera de ser contemplados por nuestro legislador de forma expresa.

La multiplicidad de prestaciones que aparecen en este contrato, le confieren la naturaleza de mixto; mixtura que nos obliga a acudir a las figuras contractuales típicas de nuestro ordenamiento para intentar responder a las cuestiones sobre su naturaleza.

Una primera aproximación al outsourcing nos hace plantear la cuestión desde la intencionalidad de las partes intervinientes en el contrato. Así debemos preguntarnos si lo que se solicita y presta, respectivamente, es un resultado concreto, o bien el objeto del contrato es una simple actividad con independencia del resultado obtenido.

Esta perspectiva nos conduce inexorablemente a los contratos de arrendamiento de obra y arrendamiento de servicios[130].

Si lo que se contrata es la gestión informática, con independencia de cualquier tipo de resultado, indudablemente nos encontramos ante la naturaleza propia del arrendamiento de servicios. Lo único importante es la actividad por la que se fijará un precio determinado. Este precio podrá establecerse atendiendo al tiempo empleado, o bien de una forma alzada. Las dificultades de la previa determinación de las horas a emplear en la gestión, impedirán en cierto modo, esta última solución. Si por el contrario en un previo estudio de las prestaciones

■130 El Proyecto de Ley de 12 de Abril de 1.994 por el que se modifica la regulación del Código Civil sobre contratos de servicios y de obra abandona la denominación "arrendamientos de obras y servicios" para sustituirla por la de "contrato de servicios y contrato de obra". Se sigue con ello una tendencia ya consagrada firmemente en la doctrina, y no sólo en la española, unánime en la idea de que la teoría unitaria del arrendamiento no tiene hoy otra justificación que el respeto a un precedente histórico completamente superado.

solicitadas se pudiera determinar de forma más o menos exacta, el tiempo de servicio, una y otra solución vendrían a coincidir.

Pero la consideración de arrendamiento de servicios y la forma de solicitar el mismo por parte de la empresa que subcontrata la gestión informática, la colocan en una cierta inseguridad, dado que sin haber fijado un objetivo determinado, el tiempo a emplear en esta actividad se puede desarrollar sin un resultado palpable.

La segunda opción se presenta como mucho más segura para ambas partes contratantes, pero también es cierto que la propia esencia del contrato de outsourcing nos muestra cómo el mismo puede alcanzar unos grados de complejidad tales, que impidan la prefijación del resultado a obtener, de forma clara e indubitada.

La solución exigirá un estudio casuístico de los problemas que plantee cada contrato en particular, sus dimensiones, alcance, la intención de las partes...

En cualquier caso, el precio del contrato, dada su naturaleza y aún en el caso de haberse predeterminado de forma exacta, debe admitir unas cláusulas de revisión fundadas en el justo equilibrio de las prestaciones.

C) ELEMENTOS PERSONALES Y REALES

En el contrato de outsourcing aparecen como elementos personales imprescindibles, en primer lugar, la empresa que solicita o se propone contratar toda la gestión de índole informática[131].

Esta parte contractual tiene una actividad diferente a la gestión informática, pero se vale lógicamente de esta última, para conseguir la optimización de sus negocios, al subcontratar toda esa gestión informática con una empresa que por sus características técnicas y de especialización, le solventará los problemas que de esta índole puedan surgirle.

■ [131] Debe tenerse en cuenta en este punto, la diferente amplitud que puede tener el contenido del contrato de outsourcing.

Toda empresa tiene la posibilidad de celebrar un contrato de outsourcing con la intención, entre otras, de rebajar los costes. Si la empresa contratante es de gran entidad, con independencia de que también pueda resultarle favorable la celebración de este contrato, también es cierto que podrá acometer con cierta holgura, todos los gastos tecnológicos, salvando así la pérdida de independencia que lleva implícita este contrato.

Indudablemente, la contratación de outsourcing con esa pequeña pérdida de independencia a la que antes nos referíamos, requiere un importante ejercicio de confianza. Esta confianza ha de presidir todo tipo contractual, pero en mayor medida, en el outsourcing, en que sus consecuencias van más allá del propio contrato que, por otra parte, supone la inclusión de un tercero en lo más íntimo de la empresa.

El segundo de los elementos personales será la empresa que asumirá las labores de la gestión informática de la primera.

Se busca así a un proveedor de experiencia y capacidad tecnológica que abarque en principio todas las facetas de gestión de los sistemas informáticos.

Hasta aquí hemos venido atendiendo a la situación de que la empresa contratante se vincule con un solo proveedor, si bien este no es el único planteamiento posible. BANKIME ha diseñado una estrategia de outsourcing que supone la aparición de tres proveedores diferentes del servicio, coordinados por la vía de un interlocutor único, CAP GEMINI a través del soporte de un sistema CAP Teleservicio[132].

Este tipo de outsourcing supone la subcontratación en tres líneas sobre el mantenimiento del software, infraestructura del hardware y sistema de comunicaciones.

D) NEGOCIACION Y FIRMA DEL CONTRATO

■[132] EZEQUIEL BARRIOS.- ¡Zapatero a tus Zapatos! Banco de Pequeña y Mediana Empresa.- COMPUTING ESPAÑA.- El Especial Outsourcing de 13-3-96.

Todo contrato, cuando menos teóricamente, exige una fase precontractual en que las partes muestran sus intenciones negociales, aclarando sus objetivos, forma de trabajo, necesidades...

En materia informática, esta fase precontractual adquiere una especial importancia, dada la singularidad de la materia sobre la que recae, la complicación técnica, la ausencia en numerosos casos de legislación específica y por ello, la multiplicación de los contratos atípicos, que imponen una fase de negociación más dilatada e intensa. Si esto es cierto en mayor o menor medida, en casi todos los contratos que pueden englobarse bajo el epígrafe genérico de "contratos informáticos", lo es con mayor razón en el contrato de outsourcing. A lo dicho se añade lo novedoso de su contenido y la gran cantidad de matizaciones en cuanto a duración, sectores afectados, amplitud de funciones, precio, forma de pago y de recepción... presentes en esta figura contractual.

Es por todo ello necesario establecer un plan de acción minucioso en el que, previo estudio de las necesidades de la empresa cliente, se fijen de forma precisa y pormenorizada, los servicios que se van a desarrollar, los costes aproximados, el precio, sus parámetros de cálculo, objetivos a alcanzar, expectativas de nuevas necesidades y adaptaciones, así como un esbozo de las responsabilidades, todo ello encuadrado dentro de la estrategia general de la empresa.

Conviene que este plan de acción se plasme por escrito, previamente firmado, y se adjunte al futuro contrato, y así, en caso de posibles discusiones, se podrá acudir a este anexo que servirá como documento aclaratorio.

Una vez finalizada la fase de estudio y negociación, se procederá a la firma del contrato, en el que, de forma precisa, se fijarán todos los parámetros que se estudiaron y discutieron en la fase previa. Se especificarán los objetivos a alcanzar, los plazos de finalización y puesta a disposición de las prestaciones, con posibles cláusulas de penalización, el precio, forma de cálculo y pago, modo de coordinación de las labores a realizar, con el correspondiente seguimiento y control, riesgos y responsabilidades con las consiguientes garantías, el imprescindible pacto de secreto etc...

E) PROPIEDAD DEL HARDWARE Y DERECHOS DEL SOFTWARE

Especial importancia cobra en esta figura contractual, la propiedad del hardware y los derechos del software.

En primer lugar, hay que tener en cuenta que uno de los servicios que pueden ser objeto de este contrato, es la adquisición del hardware, en cuyo caso se tendrá que determinar si la propiedad corresponde a una u otra de las partes contratantes.

Puede ocurrir, no obstante, que no se proceda a esa adquisición, con lo que el problema disminuye de entidad, si bien habrá que precisar en el caso de que la empresa cliente transfiera los equipos a la empresa tecnológica, las condiciones de dicha transmisión.

Mayores problemas plantea la titularidad de los derechos sobre el software.

ISABEL HERNANDO[133] distingue dos supuestos: cuando el cliente es titular de los derechos de explotación sobre el programa y cuando el cliente es titular de una licencia de uso sobre los programas. En el primero de los casos, la empresa cliente es la única autorizada para permitir a la empresa suministradora la utilización de los mismos. En el segundo caso, se requerirá la autorización del licenciatario, y será la empresa tecnológica, la encargada de obtener las licencias necesarias para evitar un uso incorrecto del software.

JOSE MARIA AGUIANO[134] dice que el titular del software debería conceder al usuario una licencia de uso y a la empresa de outsourcing, una licencia de explotación, pero en beneficio del licenciatario de uso y esto se debe a que si se ofrece licencia de uso al proveedor de outsourcing, si hay una ruptura del contrato, el cliente final se queda sin dicha licencia.

En cuanto a la titularidad de las modificaciones realizadas en los programas de la empresa cliente, entendemos con la mayoría de los autores, que

■[133] ISABEL HERNANDO.- Obra ya Citada.

■[134] JOSE MARIA AGUIANO.- Artículo aparecido el 13-3-96.- COMPUTING ESPAÑA. El especial outsourcing. "Riesgos de la subcontratación"

deberá fijarse de forma precisa quien va a ser titular de los derechos de propiedad intelectual resultantes, en caso contrario, creemos indiscutible que pertenecerán a la empresa que los ha desarrollado, dada la presunción de no cesión que dispone la Ley de Propiedad Intelectual, Texto Refundido 1/96 de 12 de Abril de 1.996 (art. 43 en relación con los arts. 21.2 y 23).

Lo más conveniente será pactar una cesión en exclusiva, de estas transformaciones.

F) EJECUCION DEL CONTRATO Y CONCLUSIONES

Una vez perfeccionado el contrato, se procederá al cumplimiento de las obligaciones pactadas, en el que deberá primar una mutua confianza con la consiguiente confidencialidad y colaboración.

El precio pactado se abonará de la forma acordada. Generalmente y dada la entidad económica de estos contratos, se fijarán los momentos, cantidades, y condiciones de este pago habitualmente unidos a las recepciones parciales de las prestaciones que se vayan cumpliendo. Lógicamente, al finalizar el tiempo de duración del contrato, que habitualmente será de cinco o diez años, se extinguirán las obligaciones de ambas partes, si bien es en este momento, cuando entrarán en juego las cuestiones previamente pactadas sobre las titularidades del hardware y del software según los casos.

En el supuesto de incumplimiento se devengarán las consiguientes responsabilidades e indemnizaciones que se hubieran prefijado y entrarán en juego las cláusulas penales que se pudieran haber pactado.

Por todo ello, reiteramos, es más que conveniente establecer una cláusula arbitral que facilite y agilice la solución de las posibles controversias durante el contrato y a su conclusión.

CONTRATO DE ESCROW

A).- CONCEPTO, CARACTERES.- RAZONES DE SU EXISTENCIA.

El contrato de escrow se presenta como un contrato atípico, íntimamente

relacionado con el contrato de depósito, regulado por nuestras leyes civiles y mercantiles (arts. 1.758 a 1.789 del Cc y 303 a 310 del Código de Comercio), pero claramente diferenciable de él, tanto por sus características, peculiaridades de su objeto y razón del mismo.

Este contrato, de origen norteamericano, encuentra su razón de ser en los conflictos surgidos o que pudieran surgir entre el usuario de un programa y sus elaboradores o empresas de software, en relación con la posesión del código fuente.

Para XAVIER RIBAS[135] Código Fuente es el núcleo formal del programa y constituye la primera expresión independiente del proceso de creación, que alcanza una protección directa del derecho de autor.

Partiendo de este concepto, podemos ver claramente que quien posea el código fuente, tiene la posibilidad de alterar de cualquier modo, interconectar y multiplicar el programa. Esta es la razón por la que las empresas de software siempre han sido reticentes a la entrega del código fuente al licenciatario de un programa de ordenador.

Si bien es cierto que la posesión del código fuente no presupone la titularidad, y por lo tanto su utilización estaría protegida por los derechos de propiedad intelectual, es incuestionable, que se crearía una situación de peligro latente.

Si se argumenta que el código fuente es imprescindible para las labores de mantenimiento, se puede argüir que éstas, por regla general, son realizadas por la propia empresa de software, lo que no impide por otra parte, que se den una serie de circunstancias que imposibiliten a la empresa de software, realizar estas labores, colocando al usuario en una difícil situación. Así, el contrato de escrow es el instrumento jurídico para garantizar al usuario en determinadas circunstancias, el acceso al código fuente.

■[135] XAVIER RIBAS.- "Protección jurídica de los Programas de Ordenador".- Institute for International Research España S.A..- Madrid 1.995.

De esta forma, XAVIER RIBAS[136] lo define como aquel por el cual, la empresa de software y el usuario pactan la entrega del código fuente a un tercero (fedatario público, asociación...) que se constituye en depositario del mismo y se obliga a entregarlo al usuario, cuando se cumplan las condiciones determinadas en el contrato.

Podemos considerar este novedoso contrato, no solamente como un contrato atípico, lo que parece incuestionable, sino también como un contrato complejo en cuanto a su naturaleza, dado que participa en cierto modo de la naturaleza del depósito y de la del de mantenimiento, con una intención de garantía de protección y aseguramiento de derechos previamente adquiridos[137].

En puridad, el contrato de escrow se celebra entre la empresa de software, titular de los derechos de propiedad intelectual sobre el programa, y el usuario del mismo, pero a su vez, se exige la concurrencia, por la propia esencia del contrato de un tercero depositario, por lo que este tercero, o bien interviene en el propio contrato, o bien se vincula a él a través de un contrato conexo. Evidentemente el contrato de escrow depende de la existencia del contrato de depósito, incluso hay quien considera que ambos son el mismo.

Nosotros, por el contrario, estimamos que si bien son contratos diferentes, no deben considerarse independientes, dado que no existe el escrow sin el depósito, incluso cuando el depositario es el mismo usuario o el propio titular del software (lo que dificulta su calificación de depósito en sentido estricto).

No queremos terminar sin reconocer la posibilidad de que el contrato de escrow se presente tan sólo como una cláusula de un contrato de mantenimiento o de licencia de uso, que al garantizar el mismo, solventa un hipotético supuesto de incumplimiento por el obligado. Con este tipo negocial se responde a los requerimientos del usuario y a la actitud precavida de las empresas de software,

■[136] XAVIER RIBAS.- Obra ya citada.

■[137] Debemos en este punto tener presente la distinción que hace DIEZ PICAZO, en su libro Fundamentos de Derecho Civil Patrimonial. Madrid 1.993, 4ª Edición, entre contratos mixtos, coligados y complejos.

celosas de garantizar y salvaguardar su propiedad intelectual. No obstante, debemos recordar que la finalidad de este peculiar contrato va más allá de la garantía de acceso al código fuente, dado que supone asimismo una prueba de la titularidad del software en caso de un futuro conflicto, así como el mantenimiento de una copia de seguridad del programa para responder ante un siniestro, que provocará la pérdida de aquel.

B).- TIPOS DE ESCROW

JOSE MARIA AGUIANO JIMENEZ y Asociados[138] utiliza cuatro criterios para clasificar el contrato de escrow: según el tipo de depósito, la finalidad del mismo, la forma de contratación, y el número de usuarios o licenciatarios que tienen acceso al código.

- Por el tipo de depósito: podemos hablar de escrow privado, cuando el depósito del código fuente se hace en una persona física o jurídica de confianza de ambas partes, que no tenga por actividad profesional la de ser depositario; el escrow será institucional cuando el depositario se dedique habitualmente a esta labor, pudiendo a su vez el escrow ser específico o genérico. Es específico cuando el código fuente se deposita en un agente escrow, entendido como la persona jurídica que se dedica a recibir o custodiar depósitos de códigos fuentes, y de su documentación; el escrow no específico o genérico, se da cuando el depositario, si bien se dedica a la custodia de bienes muebles ajenos, no lo hace de forma específica sobre los códigos fuente.

Dentro de este mismo criterio, habla AGUIANO del escrow licenciatario, en el cual, el código fuente, una vez precintado, se deja en manos del licenciatario, con la prohibición expresa de abrirlo, salvo en determinadas circunstancias; y el escrow desarrollador, en el que realmente no se da depósito, sino que se limita a un pacto por el que el desarrollador se compromete a entregar el código fuente al licenciatario en los supuestos previamente fijados.

- Por la finalidad del depósito:

■[138] JOSE MARIA AGUIANO JIMENEZ y Asociados.- "Proteger mejor su inversión en software: un análisis del contrato de depósito de fuentes, de principio a fin".- Institute for International Research España S. A..- Madrid 1.995.

Podemos hablar de escrow titular, cuyo objeto es probar la titularidad del programa depositado; y escrow usuario, cuyo sentido es garantizar el acceso al código fuente.

- Por la forma de contratación:

El escrow puede ser independiente o bien estar integrado, como cláusula de un contrato de licencia o de mantenimiento.

- Por el número de usuarios o licenciatarios con acceso al código.

El escrow será unitario cuando se realiza un depósito por cada licenciatario que suscriba el escrow; y será plural cuando el depósito se realiza para la totalidad de los posibles licenciatarios.

C).- ELEMENTOS PERSONALES

En el contrato de escrow intervienen, en principio, dos partes: en primer lugar está la empresa de software, titular de los derechos de propiedad intelectual sobre el programa, quien para garantizar en determinadas circunstancias el acceso del usuario al código fuente, realiza un depósito en la persona y con las condiciones pactadas en el contrato. De esta forma obtiene, como ya hemos señalado, la prueba de la titularidad del software, consiguiendo mantener una copia de seguridad del programa.

Por otra parte, nos encontramos con el usuario de un programa determinado, que necesita como instrumento imprescindible para el mantenimiento o modificación y para la interoperatividad de los programas de ordenador, disponer del código fuente. Ante la reticencia de la empresa por facilitar esta posesión, se satisfacen ambos intereses mediante la constitución del depósito del mismo, ya sea en un tercero, ya sea en el propio usuario, con la obligación, por parte de estos de entregarlo o desprecintarlo, únicamente cuando se cumplan una serie de supuestos como pueden ser: la quiebra, suspensión de pagos o liquidación de la empresa titular, cuando ésta cambie de actividad o no

cumpla su obligación de mantenimiento, o cuando se produzca incumplimiento respecto de las posibles interoperatividades con otros programas, o el cumplimiento del plazo...[139].

Deberán establecerse en el contrato de escrow, las características o circunstancias de cada uno de los supuestos de retirada, máxime cuando se trata de algo que puede llegar a ser tan discutible como el incumplimiento de las obligaciones de mantenimiento. Supuestos como el de quiebra, suspensión de pagos o liquidación de la empresa, parecen más sencillos de justificar, debiendo tenerse en cuenta que el fijar un límite máximo para el plazo, no impedirá de ninguna forma, que se establezcan otros supuestos de retirada.

Como hemos visto, el contrato de escrow se perfecciona entre la empresa de software, titular de los derechos de propiedad intelectual sobre el programa, y el usuario licenciatario, pero se presenta como imprescindible, la existencia de un contrato de depósito, dado que en último término éste es precisamente el objeto del negocio que estamos tratando.

El depósito al que hacemos referencia, se perfeccionará entre el titular de los derechos del programa y la persona física o jurídica que actúa como depositario.

Nada impide (incluso esta es la forma más habitual de presentación) que el depositario firme el contrato de escrow, asumiendo sus obligaciones como tal en el mismo, sin que formalmente sea necesario un contrato independiente.

Si por el contrario, simplemente se pacta que el desarrollador entregue el código fuente en los supuestos previstos, no se dará en puridad jurídica, ningún depósito, cumpliendo en cierto modo, las mismas funciones.

Respecto a las obligaciones del depositario y a la naturaleza de este contrato, debemos acudir a la reglamentación que sobre el mismo nos ofrece el Código Civil (art. 1.758 y ss.).

Nos remitimos al Título XI del Libro IV del Código Civil en cuanto a la

■ [139] AGUIANO y Asociados.- Obra ya citada.

reglamentación del repetido depósito, si bien debemos destacar que las particularidades del objeto hacen que algunas de estas normas sean de difícil aplicabilidad a este tipo de depósito (art.1.778).

De esta forma, el primer párrafo del art. 1.775, determina que el depósito debe ser restituido al depositante cuando lo reclame, aunque en el contrato se haya fijado un plazo o tiempo determinado para la devolución. Debe tenerse en cuenta que el sentido de este depósito es garantizar la disponibilidad del código fuente al licenciatario, cuando se den determinadas circunstancias, y entendemos que la posibilidad a que hace referencia el art. 1.775, no debe regir en estos supuestos, o en el peor de los casos, deberá precisarse en qué circunstancias y con qué condiciones formales pudiera llegar a darse esta retirada (por ejemplo notificar al licenciatario esta retirada).

Puede darse el caso de un escrow plural, en el que se realiza un solo depósito para un grupo de licenciatarios. En estos casos la rapidez de uno de estos últimos, al concurrir una de las circunstancias de retirada, puede colocar en una muy difícil situación a los demás.

Las soluciones que pueden darse a este problema son varias, así: permitir simplemente que se retire una copia autorizada por el depositario, sin que se de una retirada material; o bien que la retirada sea temporal con obligación de devolución; o que quien retire el código fuente se convierta en nuevo depositario con todas sus obligaciones y responsabilidades.

Podemos observar que todas estas soluciones realmente adolecen de cierto peligro que podría evitarse fácilmente (con un aumento de los gastos) depositando tantas copias del código fuente como licenciatarios tengan la posibilidad de efectuar la retirada, esto es, tantos como hayan firmado el contrato de escrow. En este caso todos ellos tendrían garantizados sus derechos y se evitaría, o bien una cascada de depósitos, un incumplimiento de la obligación de devolución, o una obligación del depositario de autorizar unas copias que excederían a las funciones propias del depositario (conservar y restituir).

D).- EL OBJETO

La función primordial, si bien no la única, del contrato de escrow, es garantizar al licenciatario el acceso al código fuente, cuando concurran determinadas circunstancias.

Por este negocio jurídico se pacta la realización de un depósito del referido código fuente, que puede ser retirado con los límites y condiciones pactados.

Partiendo de esta idea, se plantea la cuestión de concretar el objeto del depósito que origina el contrato de escrow.

El art. 1.761 del Código Civil establece que sólo pueden ser objeto de depósito las cosas muebles. Ciertamente el requisito de esta norma jurídica es cumplido por el negocio jurídico que nos ocupa. Si bien, la especialidad de la materia que tratamos nos exige una mayor precisión. En principio las partes pueden determinar libremente, dentro del límite jurídico establecido, qué se debe depositar (art. 1.255 del Cc), lo que parece imprescindible es que el código fuente esté incluido entre los bienes objeto de depósito.

Por lo que se refiere al código objeto, o documentación necesaria, AGUIANO[140] considera que son optativos, idea que compartimos, si bien, y por lo que se refiere a la documentación, debemos calificarla cuando menos, como de "conveniente" objeto de este depósito.

Respecto al código fuente, como elemento imprescindible del depósito, se deberá determinar evidentemente, la versión a dejar en custodia, así como su correcto funcionamiento, mediante una comprobación previa.

A su vez, debe pactarse un método de actualización del código depositado que podrá hacerse de una forma periódica; cuando se de una mejora o nueva versión en el código objeto; o como es más habitual, llegar a un acuerdo sobre su actualización, previendo ambos supuestos.

CONTRATO LLAVE EN MANO

A) CONCEPTO, NATURALEZA Y CARACTERES.

CONCEPTO

■ [140] AGUIANO y Asociados.- Obra ya citada.

EMILIO DEL PESO NAVARRO[141] al clasificar los contratos, distingue entre los contratos del hardware, del software, de datos, de servicios y complejos. Dentro de estos últimos, que califica como aquellos que contemplan los sistemas informáticos como un todo incorporando al objeto del mismo, tanto el hardware como el software y algunos servicios determinados, trata el contrato llave en mano o "turn key package", definiéndolo como aquel en que un proveedor se compromete a entregar el sistema creado donde el cliente le indique y asume la responsabilidad total de diseño, realización, pruebas, integración y adaptación al entorno informático del cliente, tanto lógico, como físico.

Este contrato realmente supone el ejemplo más extremo de contratación informática y contratación compleja.

Con esta figura contractual una empresa que asume desde el principio su incapacidad para solventar la planificación informática de su negocio y reconoce la existencia de especialistas con conocimientos y medios suficientes para solucionar y proveerle así de un elemento imprescindible en su vida comercial inalcanzable por sus propios medios. La empresa cliente, de esta manera, acude a un único proveedor que atenderá a su demanda y dará la solución global a todos sus pedimentos.

El interesado evidentemente puede optar por multiplicar las figuras contractuales acudiendo a contratos de compraventa, desarrollos, licencias, mantenimiento, instalación, formación..., para satisfacer su demanda. Pero este procedimiento en primer lugar exige un previo conocimiento técnico para poder diferenciar y coordinar a los distintos proveedores y sus aportaciones al resultado final, y por otro lado, supone acoplar innumerables tipos que o bien se presentarían como de difícil ensamblaje, o bien diluirían las responsabilidades y obligaciones, ya que un resultado incorrecto o una necesidad no satisfecha podía ser achacada a uno o a otro. De esta forma, el contrato llave en mano se presenta como una solución ventajosa y factible para solventar las necesidades informáticas de una empresa.

■[141] EMILIO DEL PESO NAVARRO.- Análisis Jurídicos desde una perspectiva informática, la contratación informática.- Actualidad Aranzadi, núm. 14.- Enero 1.995.

El proveedor hará un estudio de la instalación o encargará este estudio, proporcionará el hardware, directamente si es fabricante o lo subcontratará, asimismo suministrará el software o lo hará ejecutar dirigiendo el montaje conjunto y la puesta en marcha de todo el sistema[142], pudiendo asumir obligaciones complementarias como la de asistencia, mantenimiento del software y hardware, formación, conservación, reparación, back up...

CARACTERES

En el contrato llave en mano, las características podrán variar y matizarse según cada caso concreto y las prestaciones solicitadas.

Por regla general y atendiendo a la línea esencial del contrato, estimamos como características más destacadas: en primer lugar la existencia de un único vínculo contractual, ello con independencia de las necesarias subcontratas que para el cumplimiento de las obligaciones que asume, deba celebrar el suministrador. Es posible, si bien se presenta como difícil en la práctica, encontrar una empresa tecnológica de amplitud suficiente para cubrir todas las demandas del cliente. Por ello, como ya hemos dicho, frecuentemente se acude a subcontratar prestaciones concretas que llevarán a difuminar las responsabilidades cuando el cliente no esté unido directamente con el subcontratista.

La empresa tecnológica asume todas las responsabilidades derivadas de su posición contractual, no pudiendo desentenderse de una falla, alegando la impericia de tercero[143] o el defecto de un producto que ella ha adquirido[144].

Una forma de solucionar jurídicamente este problema sería acudir a la figura del mandato representativo, en cuyo caso todos los contratos que realizase la empresa tecnológica con terceras personas, los haría en nombre y

■142 ISABELLE DE LAMBERTERIE.- Contratos en informática.- Derecho y Tecnología Informática Mayo 1.989.

■143 El art. 1.596 del Cc establece que "el contratista es responsable del trabajo ejecutado por las personas que empleare en la obra", de aplicación al supuesto que estamos tratando.

■144 Posición que también adopta la Ley 22/1.994 de 6 de julio sobre Responsabilidad Civil por Daños Causados por Productos Defectuosos.

representación de la empresa cliente, estableciéndose un vínculo directo entre el tercero y esta última (art. 1.725 del Cc), bien entendido que para que el contrato llave en mano no pierda sus características más esenciales y al amparo del citado artículo, deberá acordarse la responsabilidad solidaria del propio mandatario.

Una segunda característica es la globalidad de prestaciones y suministros que hacen posible el funcionamiento de todo el sistema, planificado para dar respuesta a las demandas de la empresa cliente. Todas ellas centralizadas en un solo suministrador, organizador y responsable último del resultado obtenido.

Así se deduce como tercera característica la obligación de resultado que crea este contrato, dado que el cliente espera que el conjunto del sistema sea perfectamente operativo en la fecha prevista.

Por otra parte, la figura del contrato llave en mano hace imprescindible la existencia de dos fases:

1) Fase de estudio, en la que el cliente le muestra todas sus necesidades y características de su empresa, siendo el proveedor quien se encarga (con la posibilidad de subcontratar esta función) de realizar un análisis pormenorizado de las mismas y sus soluciones. Una vez finalizado este estudio, se pasa a la segunda fase.

2) Fase de ejecución, en la que el proveedor se encargará de realizar todos los trabajos necesarios para llevar a buen fin la demanda de un completo sistema perfectamente operativo. También se pueden requerir los servicios de un tercero, técnico en la materia, que controle la ejecución del proyecto, supliendo así el desconocimiento que sobre materia tan complicada, tiene el empresario.

Puede pactarse, eso sí, que sean dos contratos sucesivos y conexos. En el primero se hará simplemente un estudio de las necesidades y la forma de resolverlas con un presupuesto y plazos de cumplimiento, necesitándose la firma de un segundo contrato, si así se decidiese, en el que se pondría en ejecución lo previsto en el primero. En este caso, los precios serían independientes para cada contrato, elevándose el del primero en caso de una negativa a continuar.

NATURALEZA JURIDICA

De nuevo nos encontramos con un contrato atípico, puesto que carece de

regulación específica en nuestro ordenamiento, siendo su atipicidad la de los contratos complejos o mixtos. En él observamos una multiplicidad de prestaciones relacionadas e interdependientes, dado que en último término, el cliente solicita que el conjunto del sistema informático sea plenamente operativo en una fecha determinada. De lo dicho se deduce que estamos ante una obligación de resultado, cuyo núcleo principal está constituido por el hardware y el software de base[145]. Por lo tanto participará de la naturaleza de un arrendamiento de obra en el que una empresa tecnológica se compromete a obtener un resultado cierto.

No obstante, la complejidad a la que nos hemos referido, añade a esta primera naturaleza una serie de prestaciones que diluyen su precisión y que hace que entren en juego normativas de muy diversos contratos (compraventa, arrendamiento de servicios...), lo que no impide que la línea esencial del contrato suponga claramente un arrendamiento de obra asumido por una única empresa que realizará por sí misma todas las prestaciones demandadas o subcontratará la parte de ellas que sobrepasen su capacidad, permaneciendo en todo caso como controlador y coordinador único y responsable de todas ellas.

B).- ELEMENTOS PERSONALES Y REALES

Al definir el contrato llave en mano, ya hemos puesto de manifiesto cómo en el mismo intervienen dos personas jurídicas: por una parte, la sociedad de servicios o empresa tecnológica, que se compromete a proporcionar un sistema completo informático, incluyendo su instalación, que solvente las necesidades de la otra parte; y en segundo lugar, una empresa que sin capacidad tecnológica, solicita, previa manifestación de sus necesidades, una solución informática de las mismas, o si se prefiere, un sistema informático perfectamente operativo y acoplado a esas demandas.

El contrato de esta forma, se perfecciona entre las partes antes reseñadas, con independencia de la subcontratación que de alguna de las prestaciones, haga la empresa tecnológica y todo ello con ajeneidad de la metodología que se emplee en las antedichas subcontrataciones.

■[145] XAVIER LINANT DE BELLEFONDS y ALIN HOLLANDE.- Obra ya citada.

Previa la fase imprescindible de estudio, en la que tras las manifestaciones del cliente, la empresa de servicios informáticos realiza un análisis de las mismas y sus soluciones, se procede al cumplimiento de las múltiples prestaciones que constituyen este contrato y que llevarán al fin perseguido, como es que el conjunto del sistema informático sea perfectamente operativo.

C) REDACCION, EJECUCION Y RESULTADO.

De todo lo estudiado, no podemos por menos que afirmar que las variantes que en la práctica pueden darse del contrato llave en mano, son innumerables, dependiendo de las prestaciones que pueden ser asumidas a través de este tipo contractual. Estas prestaciones en cualquier caso, deben establecerse con un minucioso cuidado, para evitar futuras confrontaciones.

Entre las prestaciones que pueden ser asumidas en este contrato, XAVIER LINANT DE BELLEFONDS y ALAIN HOLLANDE[146] hacen una triple clasificación entre las de estudio, prestaciones de ejecución y las complementarias. Incluyen entre las primeras: estudio previo, análisis crítico de lo existente, definición de funciones y servicios automatizables, elección de objetivos prioritarios del plan de informatización, formalización de una o varias soluciones, elaboración de un cuaderno de responsabilidades, análisis de ofertas y examen de cuentas, asistencia a la elección del material...

Entre las prestaciones de ejecución, a su vez, distinguen entre las que afectan al hardware, al software y a la puesta a punto del sistema. Dentro de las primeras incluyen: planing de instalación, preparación de los locales, acceso a los locales, entrega e instalación, plazo para la compra de la instalación, retrasos imputables al fabricante, retrasos imputables al cliente, casos de fuerza mayor, manual de documentación, periodo de garantía contractual, garantía de vicios ocultos, seguros, suerte de hardware en caso de quiebra... Respecto al software, las prestaciones son: elección eventual de programas standard, adaptación de estos programas, realización de programas-tests, modificaciones, plazo para la compra, retraso en la entrega de los programas-tests, casos de fuerza mayor, criterios de

■ [146] XAVIER LINANT DE BELLEFONDS y ALAIN HOLLANDE.- Obra ya citada.

calidad para los programas, duración del periodo de puesta a punto, subcontratación, propiedad, patentes, derechos de autor y confidencialidad.

Las relativas a la puesta a punto del sistema serían: formación inicial del personal, organización de los diferentes puestos de trabajo, puesta a punto de los programas-tests sobre el hardware-test, creación y depósito de ficheros, procedimiento de recepción provisional, duración de la gestión y recepción definitiva.

Por último estos autores hablan de prestaciones complementarias, entre las que se incluyen: seguimiento de personal y formación, asistencia a la ejecución del sistema y prestaciones de mantenimiento.

Todas ellas aparecerán en el contrato de forma pormenorizada, siendo conveniente que se respete la clasificación de los citados autores, o cuando menos que la diferenciación se muestre claramente entre las prestaciones de estudio y de ejecución. Huelga decir que la empresa tecnológica asume la obligación de realizarlas a tenor de lo pactado para obtener el resultado que le ha sido demandado, siendo responsable de su ejecución, con independencia de las responsabilidades de aquéllos con quienes deban subcontratar.

Un punto fundamental en esta figura negocial, es el tiempo de ejecución. Como sabemos, en todo contrato un cumplimiento tardío equivale a un incumplimiento cuando menos parcial, y las responsabilidades del mismo deberán recaer en ese coordinador general y ejecutor que es la empresa tecnológica. Por supuesto, ello con independencia de la repetición que contra el último responsable pueda accionar aquélla, y junto con los mecanismos jurídicos que puedan emplearse para que también el cliente pueda accionar directamente contra el último responsable, de existir. Pero no debemos olvidar que estamos ante un contrato informático, por lo que la obligación de consejo, por parte de la empresa suministradora y la cooperación necesaria del cliente, adquieren unos tintes muy marcados.

Por otra parte, y precisamente por su carácter de contrato informático, la obligación de resultado a que en tantas ocasiones hemos hecho mención, debe ser matizada por un cierto azar, que posibilitará cláusulas más flexibles en cuanto al precio o el plazo, pero nunca se podrá alegar imposibilidad de cumplimiento por

la inejecución de un tercero, dado que su labor de gestor general conlleva su obligación de solventar estos supuestos, cuya responsabilidad también tendrá su reflejo en el precio[147].

Deberán, por el bien del contrato, prefijarse estos supuestos exoneratorios, teniendo en cuenta el conocimiento especializado que debe observar la empresa tecnológica y que le impedirán liberarse de ciertas responsabilidades, alegando desconocimiento.

OTROS CONTRATOS INFORMATICOS.

Las modalidades contractuales que han sido estudiadas, se han seleccionado como las figuras más características de este nuevo ámbito contractual.

Evidentemente, existen muchísimos otros contratos que por recaer sobre bienes y servicios informáticos, podrían ser tratados en esta ponencia, pero que excederían a nuestras intenciones de determinar las líneas básicas y fundamentales de estos negocios, o supondrían una repetición absolutamente innecesaria de otras ponencias expuestas en estas jornadas.

Y así además de los contratos a que hemos hecho referencia, podemos mencionar los contratos sobre bases de datos, auditoría informática, back up contract, renting, transporte sobre material informático, seguro informático, y un largo etcétera.

CONCLUSIONES

A lo largo de este estudio, hemos intentado hacer un recorrido a través del ámbito contractual en que la Informática se presenta no solamente como el objeto del negocio jurídico, sino también como la peculiaridad y elemento diferenciador del mismo.

■147 El art. 1.105 del Código Civil dispone " fuera de los casos expresamente mencionados en la ley, y de los en que así lo declare la obligación, nadie responderá de aquellos sucesos que no hubieran podido preverse, o que previstos, fueran inevitables".

Desde un primer acercamiento a la contratación informática en general, en el que hemos tratado de poner de manifiesto, las características más peculiares de ésta, hasta el estudio concreto de algunas de las figuras más representativas, se puede observar cómo, si bien estamos inmersos en principio, en una normatividad clásica, de la que debemos partir, no podemos olvidar todas las diferencias y nuevas exigencias que el mundo negocial de nuestros días precisa.

Las notas específicas de la Informática como peculiar objeto contractual, incitan a su estudio pormenorizado, en el que se entremezclan distintas regulaciones (cronológicas y espaciales) y posiciones contrapuestas entre quienes dominan la nueva tecnología y quienes simplemente confían en que una legislación en ocasiones trasnochada, cubra y proteja posiciones jurídicas tan novedosas.

Somos conscientes de que la normativa vigente es la normativa a aplicar y es labor de los juristas, en colaboración con los profesionales de la Informática, encontrar acomodo entre ambas disciplinas. No preconizamos la promulgación de un sinfín de leyes que partiendo de cero, regulen la contratación informática, sino tan sólo una toma de conciencia por nuestro legislador de que la nueva vida negocial demanda mecanismos y protecciones adecuadas que no siempre es fácil encontrar en el ordenamiento vigente.

No obstante debe reconocerse también la progresiva adaptación que en el entorno jurídico se ha ido dando y la cada vez más abundante normativa que se refiere a este tema, tanto en el ámbito nacional, como europeo.

Pero es la Doctrina quien más empeño está haciendo en vislumbrar una salida a la multitud de problemas de acoplamiento que la contratación informática, ha creado en la práctica.

De las figuras contractuales en las que nos hemos detenido, podemos observar cómo las soluciones no siempre son coincidentes, y en muchas ocasiones exigen una labor interpretativa que nos puede conducir a posiciones un tanto inestables.

Por otra parte, ciertos nuevos contratos sí que exigen una regulación concreta y pormenorizada si se quiere asegurar un tráfico jurídico que mueve ingentes cantidades de dinero.

Es pues labor de todos los que de una u otra forma nos relacionamos con el mundo jurídico de manera profesional, estudiar y buscar las soluciones que requieren los nuevos contratos informáticos, solicitando del legislador, como ya se viene haciendo, que acople, modifique o cree, cuando ello fuere necesario, un Derecho que de esta forma cumpla su deber de reglamentar de manera precisa, la convivencia del hombre actual.

Cuestiones eficaces en torno a la Libertad Informática

DIEGO SÁNCHEZ MECA

Profesor Titular UNED

1.- La libertad informática como derecho fundamental

Tal vez se haya debido a las peculiares circunstancias políticas de los últimos años en nuestro país -al fenómeno de la corrupción, el asunto de los GAL, el enquistamiento del terrorismo y la delincuencia urbana, el narcotráfico, etc.-, pero ha sido clara, y casi me atrevería a decir que sigue siendo un clamor abierto, el que pide y plantea una demanda generalizada de ética. Y no sólo en el ámbito de la política, sino también en el de la justicia, en la empresa, en los bancos, en la sanidad, y en los medios de comunicación. Parece como si ahora se hubiera hecho más evidente que la fidelidad a unos principios éticos, un cierto autocontrol de las pasiones y de los impulsos por parte de determinados individuos o grupos, que es en lo que consiste la ética, hubieran evitado

gravísimos males, no sólo a terceros, o sea, a muchos ciudadanos inocentes que se han visto perjudicados y lesionados por los excesos de otros, sino incluso para los mismos individuos que han llevado a cabo esos excesos y que luego, de un modo u de otro, vemos que tienen que pagar altos precios por su inmoralidad y su falta de control.

O sea, lo que se muestra de un modo más evidente a nuestra sociedad, es que la libertad, ese preciadísimo e indiscutido derecho que todo ser humano tiene por el hecho de serlo y que siempre se puede ejercer en mayor o menor medida según las circunstancias de cada cual, es algo peligroso si no va unida a la responsabilidad. Pues se entiende que libertad no es hacer lo que a uno le dé la gana o buscar exclusivamente el propio interés y beneficio, al margen de cualquier norma ética o de cualquier principio general. Eso podría ser así si el individuo viviera sólo y no en relación con otros individuos formando una sociedad. Esta libertad de hacer lo que uno quiere, sin más, como libertad irresponsablemente ejercida, no sólo puede hacer daño a otros y a uno mismo, sino que, en realidad, si carece de criterios y de sentido, nunca será una libertad positiva y constructiva.

Puesto que el hombre es un ser social que necesariamente desarrolla su vida en relación con otros, tenemos que entender la libertad como la autonomía para crear y para darnos a nosotros mismos normas de comportamiento. En este sentido, la libertad va unida a la responsabilidad, que no es otra cosa sino la posibilidad de responder con razones de lo que uno hace ante quien tiene derecho a exigir de nosotros y de nuestras acciones unas lealtades o unos resultados. Por eso esta demanda de ética, de responsabilidad, de mayor vigencia y uso de los principios morales en los comportamientos generales, se puede incluso explicar de un modo utilitarista. O sea, la ética es hasta conveniente y beneficiosa para la sociedad, que somos todos, y va en beneficio del interés que motiva la mayoría de nuestras relaciones en un sistema de mercado.

Por ejemplo, cualquier empresa o industria es, además de otras posibles cosas, un negocio que aspira a ser rentable. Es decir, lo que quiere, ante todo, es vender. Lo mismo que un partido político lo primero que quiere es el poder, ganar las elecciones. Pero en ambos casos, el afán del beneficio económico o político no puede saltar por encima de un cierto respeto a normas de calidad, a una cierta veracidad en la propaganda y en lo que se promete, etc., porque si esa empresa o ese partido engaña a sus clientes y les da gato por liebre, tal vez obtenga una rentabilidad inmediata, pero a costa de destruir la confianza que debe darse en toda relación política y comercial, y a costa de perjudicar su imagen, por

lo que el saldo final le resultará, seguramente, ruinoso. Así que la ética resulta incluso rentable, y eso lo saben muy bien los empresarios, los políticos, los banqueros, y los periodistas.

Pero entonces, ¿por qué no se comportan algo más frecuentemente de un modo ético? La respuesta remite a lo que es la naturaleza humana: o sea, al hecho de que el ser humano no es, sin más, como decía Aristóteles, un ser racional, al que le baste con comprender qué es lo bueno y qué es lo que más le conviene para hacer eso y no otra cosa. En el comportamiento humano inciden multitud de elementos irracionales a los que el individuo cede y por los que se deja llevar, como son la pasión por el poder, el deseo de riqueza, la búsqueda del placer, y tantos otros. Y en este sentido ya poco vale el utilitarismo como argumento contra la falta de ética. Más bien hay que plantear la necesidad de una educación del carácter que haga que el individuo, desde niño, vaya incorporando unos valores, vaya desarrollando una sensibilidad ética y estética que sean las que le guíen, como resortes internos, en las circunstancias concretas en las que tenga que tomar decisiones de índole moral.

No estoy defendiendo, con esto, que es necesario, por ejemplo, volver a esa educación religiosa que era antes la encargada de proporcionar a los individuos esta sensibilidad moral. Yo no creo que los principios éticos tengan que basarse necesariamente en una religión, sino que creo más bien que se basan en la razón, que puede ofrecer criterios y valores capaces de guiar la acción. Por eso, para mí la educación ética es una educación racional y críticamente reflexiva de la sensibilidad y de las pasiones, cuyo fin no es sofocarlas o reprimirlas, sino ennoblecerlas y hacer posible el uso de toda esa energía psíquica que contienen para fines positivos y constructivos.

Ha sido el desarrollo de la razón y de la reflexión crítica a lo largo de los siglos el que ha aportado lo que hoy llamamos los derechos fundamentales, en los que se basan los principios constitucionales democráticos. Cualquier sociedad democrática se basa hoy en tres valores éticos esenciales: la libertad, la igualdad y la solidaridad. Son los valores que inspiraron la revolución francesa y que constituyen el núcleo de la famosa "Declaración de los derechos humanos". Pues los derechos humanos no son, en realidad, otra cosa que los modos concretos de plasmar esos valores generales en nuestras vidas y en nuestras instituciones. Por ejemplo, el valor de la libertad determina e inspira los que se han dado en llamar los derechos de la primera generación, o sea, los derechos civiles y políticos, consustanciales a la idea de ciudadanía: el derecho a la libertad de conciencia, a la

integridad física, a la libertad de expresión, de asociación, de tránsito, de comercio, etc.

Después de las revoluciones burguesas y del predominio de las ideologías liberales durante el siglo XIX, las luchas socialistas y las revoluciones comunistas se oponen a los excesos del liberalismo y terminan por imponer el valor de la igualdad de oportunidades como guía para la formulación de la segunda generación de los derechos fundamentales, los derechos económicos, sociales y culturales: derecho al trabajo, a una vivienda digna, a una justicia imparcial, a la salud, a la inviolabilidad del domicilio, etc. Lo que la ideología socialista defiende es que la libertad del individuo no puede nunca ser absoluta, que no puede ejercerse en detrimento y perjuicio de la libertad de los otros.

Hoy, en el siglo XX, una tercera generación de derechos hace su aparición inspirada por el tercero de los valores que antes enunciaba: la solidaridad. Pues se trata de una clase de derechos que no pueden ejercerse ni disfrutarse sin una cooperación general de carácter internacional. Son el derecho a la paz, a un medio ambiente saludable y limpio, etc. para los que no es suficiente que algunos individuos, o algunas naciones estén decididos a respetarlos e incluso a promocionarlos, pues no se logran las metas a las que apuntan sin un acuerdo y una colaboración de carácter planetario.

Dentro de esta tercera generación de derechos fundamentales hay que situar hoy la libertad informática, entendida como derecho a la autodeterminación informativa.

Puesto que me es imposible abarcar toda la complejidad de problemas y cuestiones que, desde el punto de vista ético, plantea el ejercicio de este derecho fundamental, creo que centrándome en el análisis de sólo dos aspectos de este derecho que a mi juicio resultan suficientemente ilustrativos, será posible comprender el carácter de los juicios éticos básicos en este ámbito y qué alcance debe tener su funcionamiento. Esos dos aspectos de la libertad informática son el que guarda relación con la creación y uso de las bases de datos y el que representa el desarrollo de las redes telemáticas del tipo de Internet.

2.- Problemas éticos que plantean las bases de datos

Hoy, la posibilidad de acumular cantidades ilimitadas de datos relativos a circunstancias personales, de almacenarlos ordenadamente, de recuperarlos de manera inmediata y de transmitirlos sin problemas a distancia genera un tipo de dominio desconocido hasta ahora. (Tal vez uno de los modos por el que mejor nos vamos enterando de esa clase de dominio sea a través de Hacienda). Y es que en nuestras sociedades digitalizadas o informatizadas, el poder ya no radica tanto en el ejercicio de la fuerza física, política o económica, cuanto en el uso de información, con la que se puede influir y controlar el comportamiento de los ciudadanos sin necesidad de tener que echar mano de medios coactivos.

De modo que la libertad personal y las posibilidades de intervenir en los procesos sociales, económicos y políticos, están ahora muy determinadas por el acceso y el control de la información. En este sentido, la libertad informática se entiende como derecho del individuo a tener acceso y a conocer las informaciones que le conciernen archivadas en bancos de datos por gobiernos, bancos, empresas, etc.; a controlar su calidad y a corregir o cancelar, si quiere, los datos que considere inexactos o indebidamente procesados acerca de su persona; y a decidir sobre su difusión, transmisión y uso.

Este derecho es el que se contempla en la norma básica del Consejo de Europa titulada "Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal", y que adapta, al ámbito europeo, la conocida *Privacy Act* norteamericana. Como su título indica, se trata de proteger, no tanto los datos, sino a las personas concernidas por esos datos.

Si la libertad informática es un derecho fundamental, deben cumplirse dos condiciones a su respecto: deben quedar garantizadas para el ciudadano determinadas posibilidades de actuación y de control; y asimismo deben crearse las circunstancias de equilibrio entre poderes para que no se den situaciones de marcada desigualdad en el ejercicio de las libertades. Es obligación de cualquier Estado de Derecho tomar las medidas necesarias para que esa garantía y ese equilibrio de poderes no sea sólo algo formal sino también real.

Fundamentalmente se pueden señalar dos formas principales de abusar de ese derecho y, por tanto, de delinquir. Por un lado, los detendadores de

bancos de datos pueden lesionar los derechos de los individuos mediante la manipulación de la información, bien en fase de entrada o input (o sea, introduciendo en el ordenador datos falsos, alterando los verdaderos, omitiendo unilateralmente los que no interesan o inventándose datos falsos); en la fase de procesamiento (haciendo que el procesamiento de los datos reales conduzca a resultados falsos, o interfiriendo en el programa que contiene las órdenes precisas para el tratamiento de los datos); o, por último, en la fase de salida de los datos o output (es decir, manipulando los resultados, por ejemplo en el momento de pasarlos a la impresora, de grabarlos en un disquete o de transmitirlos a otro ordenador).

Pero también los individuos pueden delinquir actuando indebidamente contra los bancos de datos. Es el caso de lo que se ha dado en llamar la piratería del software o delito a distancia, que se comete con un ordenador conectado a una red por la línea telefónica mediante un módem. Este delito consiste en manipular incontroladamente una información, por ejemplo accediendo delictivamente a los datos de los bancos o a las bases informáticas de los servicios secretos de un Estado, o a las de sus sistemas militares de defensa, etc.

Ciertamente, la protección de datos personales se ha convertido hoy en un importante criterio de legitimación política de los sistemas democráticos en nuestras sociedades informatizadas, constituyendo una de las funciones principales del Estado de derecho asegurar esta garantía básica para cualquier comunidad de ciudadanos libres e iguales. Sin embargo, no es suficiente para ello la simple promulgación de leyes, que dejan siempre un margen amplio de indeterminación. En la protección del honor, de la intimidad personal y del derecho a la propia imagen una ley puede definir la ilicitud de métodos técnicos de entrometerse en la vida íntima de las personas o de divulgar hechos o datos que afectan a la reputación de alguien. Pero no puede delimitar dónde empieza y acaba el ámbito de lo privado y lo íntimo, ni en qué momento la revelación de un dato arruina la reputación de una persona. Incluso la ley determina que, por exigencias del interés general, ciertos datos privados o íntimos pueden llegar a ser revelados.

Está claro que ese margen amplio de indeterminación legal sólo puede ser cubierto por una conciencia ética en la que la sociedad debe estar educada, que le lleve a distinguir con cierta unanimidad lo correcto de lo incorrecto, y que promueva el respeto mutuo entre las personas en lugar del "todo vale". Tener

conciencia ética o moral significa que uno hace lo que hace por convicción y no sólo por convención. Es decir, que uno rechaza lo malo y lo perverso porque lo considera repulsivo y execrable, y no sólo porque tema las sanciones penales que puedan derivarse de la transgresión de una ley.

Esto es lo que hoy se llama comportamiento ético, que no es otra cosa que un comportamiento de acuerdo con la razón, un comportamiento racional. Los principios éticos -como decía antes-ya no se basan en la religión, ni en las costumbres, sino en la razón. El crimen, la tortura, la falsedad, el engaño, la deslealtad, todo eso es rechazado por sí mismo, como algo que no es bueno para el individuo y que hace imposible la convivencia en sociedad. Pero que los individuos sientan esto y se comporten racionalmente ha de ser fruto de una educación ética, que consiste en inculcar valores que lleguen a formar parte de nuestra propia naturaleza, que lleguen a gustarnos y que disfrutemos poniéndolos en práctica.

Más adelante diré algo más acerca de esta educación ética, cuya necesidad se pone aún más de manifiesto cuando atendemos a los problemas éticos que plantea el segundo de los aspectos de la libertad informática que quiero plantear, el que se relaciona con el desarrollo de las redes telemáticas.

3.- Problemas éticos planteados por Internet

Las redes telemáticas alcanzan hoy un nivel técnico que permite la transmisión y la circulación casi instantánea de información en forma de textos, imágenes, sonidos o bases de datos entre los puntos más distantes del planeta. Estas redes inauguran un nuevo modelo de interrelación a distancia del que la red Internet es, sin duda, el ejemplo más importante y espectacular. Porque desde este punto de vista, Internet no es sólo, o no es principalmente, una red de interconexión entre redes de computadores, sino el sistema más amplio, flexible y evolucionado de interrelación que haya existido nunca. Un sistema en el que la acción de millones de individuos, de protocolos, de máquinas y de mensajes dan lugar a un metacomportamiento que se realimenta él mismo y que resulta imposible de controlar tanto desde un punto de vista técnico como político o jurídico. Internet es una estructura interactiva horizontal que se desarrolla hoy a gran velocidad, no sólo en las empresas, en las universidades o en las instituciones gubernamentales, sino también en los hogares de los ciudadanos, provocando

importantes transformaciones en las actitudes y en las conductas de los individuos cuyo verdadero alcance todavía no alcanzamos a prever con claridad.

Mucha gente se pregunta qué evolución tendrá la difusión de Internet, teniendo en cuenta que sus cambios se suceden a una velocidad que apenas nos permite asimilarlos. La pregunta que inevitablemente se nos plantea es: ¿hacia dónde va esta aldea global de millones de individuos unidos por lazos virtuales, tal como nos la prefigura Internet? Al navegar por esta red de redes, nos adentramos en un universo de información sin barreras geográficas ni límites físicos, y comprobamos que, en este mundo, nuestro conocimiento y nuestra inteligencia no son más que un punto borroso y disperso.

Pero también nos damos cuenta de que de la interconexión entre estos puntos surge una especie de cerebro universal en el que las inteligencias de los individuos funcionan como polos activos que crecen y se desarrollan al mismo tiempo que nutren, potencian y desarrollan la mente universal misma. Es la característica que ha llevado a calificar a Internet como *The big mind*, la gran mente.

Pues bien, uno de los rasgos más sorprendentes y más interesantes de esta macro-red de redes telemáticas es que no la dirige nadie. Internet no es una empresa, ni una multinacional, ni la dirigen los gobiernos, ni la CIA, ni la ONU, ni nadie, sino que funciona con un alto nivel de autonomía.

En sus comienzos sólo era un reducido grupo de personas el que formaba Internet y el que tomaba las decisiones, pero hoy son ya millones de usuarios los que intervienen en ella, por lo que nadie tiene capacidad ni poder para imponer aquí su voluntad. Las propias redes locales que componen la macro-red no pueden hacer otra cosa que ofrecer alguna orientación referida a esa red local concreta, pero no existe ningún poder central que abarque y domine todo el complejo planetario que constituye su estructura. Y es que, desde el momento en que Internet no es sino una vía para la interconexión y la comunicación entre personas, grupos, instituciones o empresas de todo tipo, lo que proporciona simplemente es eso, comunicación, dependiendo de todos y cada uno de sus usuarios el contenido y el carácter de lo que se comunique a través de las pantallas de los ordenadores de la red.

Claro que alguien podría decir: para que una red de estas características funcione alguna organización habrá que marque, al menos, las

reglas generales de carácter técnico y homogeinice las posibilidades de acceso y uso de los usuarios. Pues sí, desde luego está, por ejemplo, la *Internet Society*, pero ni es una empresa, ni un consejo de dirección de Internet al que haya que solicitar licencia de acceso, ni un organismo que regule reglamentariamente su funcionamiento. La *Internet Society* la forman un grupo de voluntarios que recomiendan ciertas fórmulas de carácter técnico, que se plantean cuestiones como qué incidencia puede tener el cableado territorial para las emisiones de TV sobre la red telemática, o que llaman la atención sobre los problemas que se pueden presentar cuando la red alcance mil millones de usuarios. Pero nada más.

En Internet no funcionan leyes ni sanciones, como tampoco deciden en ella votaciones por mayoría, ni criterios selectivos propuestos por expertos sobre lo que se debe comunicar o no. Todo esto es lo que ha llevado a definir Internet como "una anarquía que funciona muy bien". Porque es un ejemplo de organización no dirigida por nadie, ni por un gobierno, ni por el peso de la opinión pública, ni por las preferencias de las mayorías, y ello hace que no le pase lo que a la TV, que se ha convertido en un medio para consumidores dirigido por los intereses del mercado, del consumo y de los poderes políticos. Lo que mueve a Internet es el poder de participación: quien más participe más posibilidades tiene de influir sobre los demás. Pero, puesto que las dimensiones de Internet son nada menos que planetarias, lo que motiva la participación no puede ser tanto el afán de protagonismo cuando el deseo de comunicar, de colaborar y de integrarse. Frente a la pasividad que impone la TV, Internet permite expresarse, comunicar ideas y esperar que, entre los millones de cibernautas, alguien recoja nuestra aportación y pueda beneficiarse de ella.

Y si nadie dirige Internet, tampoco nadie controla Internet. Y esta es otra de las característica de la red que más problemas plantea desde el punto de vista ético.

Que sea posible la difusión de información sin restricciones, cruzando las fronteras nacionales y siendo accesible a todo tipo de gentes, sin distinciones de edad, religión, sexo o nivel económico, tiene tanto aspectos positivos como negativos. Pues también los delincuentes, los terroristas, narcotraficantes, pervertidos o locos pueden utilizar la red, y de hecho la utilizan, para darse a conocer y promocionar sus fines delictivos. De nada sirve aquí que un país determinado prohiba en su legislación la pornografía, el integrismo religioso, o la propaganda nazi. Internet llega a todas partes y a toda clase de gente.

Todo el mundo sabe que en Internet se pueden encontrar, desde recetas para elaborar drogas sintéticas, hasta fórmulas para fabricar bombas, por no hablar ya de la propaganda de grupos racistas o terroristas que defienden y animan a practicar los comportamientos más subversivos contra el orden establecido. También hay mucha pornografía en la red, siendo las páginas de sexo o de ligue erótico de las más frecuentadas. Y hay una gran proliferación de sectas y de telepredicadores que, con un discurso más o menos estudiado, pueden inducir hasta suicidios colectivos, como hemos visto que ha sucedido recientemente en Estados Unidos.

Curiosamente, para contrarrestar a estos predicadores cada vez más numerosos, también el Vaticano ha puesto su página Web en Internet, proporcionando información sobre los discursos del papa, las encíclicas, la doctrina de la Iglesia, etc. Y lo propio han hecho también los que protestan contra las opiniones del Vaticano. Por ejemplo, el obispo francés Jacques Gaillot, que fue exiliado por el papa a África por sus opiniones heterodoxas, ha creado una especie de diócesis virtual en Internet que defiende el uso de los preservativos, el matrimonio de los curas, el sacerdocio de las mujeres, la tolerancia con los homosexuales y todo lo que este papa más detesta, llegando sin duda ahora a muchos más fieles que antes en su obispado francés.

Todo esto demuestra que no existe control alguno en Internet, ni funcionan en ella leyes que restrinjan contenidos antisociales o inmorales, permitiendo sólo las actividades legítimas y positivas de la gente normal. Y esto plantea problemas jurídicos muy serios que seguramente ya se habrán discutido, o se discutirán, en el marco de este curso. Por ejemplo, no es posible proteger los derechos de autor, o sea, que cualquiera puede apropiarse de un trabajo o de una información de otra persona y utilizarla indiscriminadamente en su propio beneficio. Tampoco se ve la manera de controlar las licencias de exportación: si se paga una licencia por importar un producto físico, también habría que pagarla para exportar información o servicios de tecnología avanzada. El problema es cómo.

El gobierno de Estados Unidos ha intentado tomar algunas medidas en este sentido, pero sin ningún éxito. Por ejemplo, planteó la posibilidad de restringir mucho más las transacciones codificadas, proponiendo incluso la implantación de un chip de cifrado obligatorio, llamado *Clipper*, cuyas claves estuvieran en manos de la CIA y del FBI. Y ha tipificado como una de las funciones de la CIA averiguar los orígenes de anuncios o webs de narcotraficantes

o grupos terroristas. Sin embargo, parece que técnicamente ninguna de estas medidas es eficaz, y cuentan además con la oposición de las compañías telefónicas e informáticas a las que no les interesa ningún tipo de restricciones en el uso y la expansión de la red.

Con lo que, si en Internet no se pueden aplicar leyes por imposibilidad técnica, por la complejidad misma de su estructura o por la forma tan veloz con que evoluciona técnicamente, de hecho resulta que Internet es un ámbito en el que nada puede considerarse ilegal. Por ello tal vez alguien ponga el grito en el cielo, aunque creo que tampoco habría que exagerar. Se pueden cometer delitos, ciertamente, por medio de Internet, pero son de imagen, de dinero o de difusión indebida de propaganda. Que yo sepa, todavía no es posible matar a nadie por Internet.

Pero dejando los problemas legales a los juristas, a mi modo de ver los problemas éticos que aquí se plantean hay que verlos a la luz de un contexto que contemple las profundas transformaciones culturales, a nivel planetario, que el desarrollo de la red permite prever. En síntesis, Internet es probablemente un boceto, una imagen virtual de una sociedad cosmopolita llegada a su mayoría de edad, una sociedad que se libera hasta cierto punto del dominio de los políticos y las multinacionales y aprende a controlarse y a autorregularse a sí misma, sin esa necesidad tan apremiante que todavía sentimos de un padre, de una autoridad que nos controle, nos amenace y nos castigue. Esta situación "utópica" de mayoría de edad sería, en parte, fruto del desarrollo y de las consecuencias que el progreso técnico pudiera tener en orden a ir favoreciendo ese cosmopolitismo, por un lado, pero, por otro también -y esto de un modo no menos esencial- de una mejor educación ética de los individuos que les lleve a un uso más responsable de su libertad.

Qué duda cabe de que, para personas educadas, ni siquiera sería preciso censurar la propaganda terrorista, la pornografía infantil o a los predicadores dementes: el simple contenido de todo esto les suscita un fuerte rechazo y les pone abiertamente en contra de sus fines despreciables. Hay ejemplos que demuestran que, en cierto modo, también en Internet funcionan ciertos mecanismos de autorregulación. En 1994, un abogado de Phoenix (Arizona) envió propaganda de sus servicios a 9.000 buzones de usuarios de la red. Y la respuesta no se hizo esperar. No sólo recibió más de 30.000 quejas de usuarios indignados por haber enviado publicidad no solicitada, sino que el proveedor que le proporcionaba el acceso clausuró su cuenta y no faltaron

usuarios que se dedicaron a bombardear su buzón telemático con todo tipo de basuras: virus, insultos, sonidos estridentes, etc. Este insignificante incidente constituye una pequeña manifestación del juicio ético fundamental que debe presidir toda sociedad democrática: uno es libre de hacer lo que quiera siempre que no use su libertad para molestar o hacer daño a otro.

Por tanto, y en primer lugar, cualquier planteamiento ético que intente abordar los problemas que genera el desarrollo de la libertad informática debe tener, ante todo, en cuenta esta nueva forma de interacción social que el progreso de la informática está creando a nivel planetario y que nosotros podríamos calificar como un nuevo cosmopolitismo.

4.- **Cosmopolitismo y ética planetaria**

Hoy aún no existe ese cosmopolitismo en sentido estricto. Los individuos seguimos perteneciendo a una patria, a un pueblo, a una nación, siendo esa relación o condición de pertenencia la que nos da nuestro estatuto de ciudadano e incluso, para algunos, sus más profundas señas de identidad. Esa es la fuerza, a veces intensamente irracional, de los nacionalismos.

Pues bien, el talante fundamental del nuevo cosmopolitismo partiría de una crítica a esa relación de pertenencia y de la afirmación de que los individuos no pertenecen ni a su pueblo ni a su nación, sino a ellos mismos. Hasta ahora, a lo largo de la historia, han sido muy pocas las sociedades que han afirmado la individualidad como base de la ciudadanía. Las sociedades se constituían y funcionaban en función de una cierta jerarquía de familias, de clanes, de tribus o de hordas, normalmente capitaneadas o lideradas por los señores de las armas, los propietarios de la tierra o los dominadores de almas. En este sentido no hay un salto demasiado grande entre las sociedades humanas y las manadas animales. Entre los animales no existen los individuos, sino sólo el grupo o la especie. La individualidad es una construcción humana, cultural y social heterogénea al nivel de la mera naturaleza.

Ese nuevo cosmopolitismo anárquico y libertario que se prefigura en el desarrollo de las redes telemáticas sería aquél en el que para ningún individuo lo esencial de sí mismo es pertenecer a una nación, ser hijo natural de un pueblo, sino al revés, cuando la nación o la patria no se muestran sino como lo que son, puras entidades abstractas y formales al servicio de los ciudadanos, en lugar de

estar éstos al servicio de ellas. Una nación o un Estado no debería ser más que una estructura de servicios públicos creada y sostenida por la sociedad civil. De modo que si, en vez de prestar esos servicios con eficacia y honestidad se absolutiza y se erige a sí misma en un fin que utiliza a los ciudadanos como medios, entonces hay que prescindir sin contemplaciones de la primacía formal del Estado y organizar desde la sociedad los servicios públicos que se necesiten.

Ciertamente, todo esto es una utopía que no sabemos si alguna vez llegará a realizarse. En cualquier caso, empieza a divisarse, en el plano del desarrollo de la informática, un rebasamiento de las fronteras territoriales que definen la existencia de los Estados y de las naciones, y se refuerza la imagen del individuo cosmopolita que se asocia libremente con otros formando grupos e instituciones que, a nivel planetario, colaboran y actúan como contrapeso unos de otros. Todo ello prefigura una estructura civil de nuevo cuño en la que el pluralismo, la igualdad y las libertades individuales, elementos básicos de la democracia, se muestran mejor difundidos y realizados.

En el marco de esa nueva sociedad, habrá de tener una presencia también nueva lo que vengo llamando a lo largo de esta charla la educación ética, que debe incidir, de manera especial, en la sensibilidad y en las pasiones irracionales. El ser humano no es sólo inteligencia o espíritu, sino que también tiene una parte de animalidad y hasta de infraanimalidad. No sólo somos capaces de hacer lo malo a sabiendas de que es malo, sino de sentir un intenso placer precisamente en hacer lo malo. Por eso no se puede considerar suficiente una educación ética consistente en el aprendizaje de una serie de normas o principios a nivel teórico, en la medida en que es muy posible conocer esas normas y quebrantarlas movidos por deseos, intereses o pasiones. Más bien habría que combinar ese aprendizaje teórico con otro tipo de educación moral centrada en la paulatina y progresiva asimilación de las virtudes. Mediante el ejercicio de la virtud se va modelando la naturaleza del individuo, se encauzan sus deseos y sus sentimientos. El individuo adquiere así unos resortes internos de su conducta, que ofrecen mucha mayor fiabilidad que el simple recuerdo de unas normas impuestas desde fuera.

En esta línea insistieron mucho, durante el siglo pasado, ciertos filósofos que promovían, como elemento básico de esta educación ética, una educación estética dirigida al refinamiento de los sentimientos y de los gustos a través del contacto y la apreciación de lo bello y de las acciones heroicas y buenas. Lo que se propone, como uno de los elementos fundamentales de la educación

del ser humano, es la familiarización de su espíritu con la belleza, inclinándolo a ella desde la infancia. Suponiendo un íntimo parentesco entre lo bueno y lo bello, se cree que el apego del alma a la belleza se traducirá espontáneamente en conductas moralmente buenas.

Se compartan o no estas ideas, lo que sí parece indiscutible es que no hay verdadera educación ética de los individuos si ésta no les provee de virtudes como dimensiones adquiridas de su carácter y como raíces estables de su comportamiento. Virtudes que no son sólo principios arraigados que inducen a cumplir las normas, sino una especie de nuevos instintos que conllevan cierta capacidad de discriminación y cierta lucidez moral. El individuo ético no es simplemente el que trata de adaptar su conducta a un conjunto de normas morales. Las normas éticas, como las jurídicas, son siempre prescripciones abstractas. Establecen la bondad o la maldad de determinadas acciones, pero al margen de las circunstancias particulares en las que esas acciones pueden presentarse en cada caso.

Sin embargo, el individuo ético con lo que se encuentra siempre es con circunstancias concretas, individuales e irrepetibles en las que tan sólo su sensibilidad moral, su instinto ético le permiten discriminar y decidir lo que debe hacer en cada situación, sopesando los elementos normativos que hay que aplicar. Es ese sexto sentido moral, o lo que, de un modo un poco ridículo, los curas llamaban antes el gusanillo de la conciencia, como facultad, destreza o capacidad que sólo se adquiere tras un lento esfuerzo de educación. Por eso Platón compara el aprendizaje moral con el adiestramiento de un artesano que aprende los secretos de su oficio en un taller y en estrecho contacto con su maestro. Lo que el artesano aprende -por ejemplo, lo que aprendían los artistas del Renacimiento que desde niños se pasaban su vida en los talleres de los grandes maestros pintores o escultores- es como una pericia, una maestría que sólo la dan años de práctica en los que el aprendiz va dominando las técnicas y los secretos podríamos casi decir por contagio vital, más que por comunicación teórica.

Hoy a lo mejor resulta más actual comparar la educación moral con la práctica de un deporte, pues lo mismo que el cuerpo adquiere y se acostumbra a ciertas destrezas y habilidades mediante el ejercicio, así el espíritu ha de ponerse en forma moral mediante el ejercicio de las virtudes. De donde se deduce que, en cierto modo, la educación moral debe organizarse y ponerse en práctica en un contexto de libertad más que de imposición autoritaria, requiriendo una

colaboración de toda la sociedad a cuya sensibilización pueden contribuir, en buena medida, los progresos futuros mismos de las técnicas informáticas.

REFERENCIAS BIBLIOGRÁFICAS.-

BLAZQUEZ, N., *Información responsable*, Madrid, Noticias, 1993

BONET, E. (ed.), *Éticas de la información y deontologías del periodismo*, Madrid, Tecnos, 1995

CARBALLAR, J.A., *Internet: el mundo en sus manos*, Madrid, RA-MA, 1995

CASTELLS, M., *La ciudad informacional*, Madrid, Alianza, 1995

ECHEVARRÍA, J., *Cosmopolitas domésticos*, Barcelona, Anagrama, 1995

ESTRELLA, J.-LÓPEZ, A., *Cibercultura*, Madrid, Anaya, 1996

GATES, B., *Camino al futuro*, Madrid, McGraw-Hill, 1995

HUITEMA, Ch., *Internet, una vía al futuro*, Madrid, Ed. Gestión 2000, 1995

LIBOIS, E., *Ethique de l'information*, Bruxelles, Editions de l'Université de Bruxelles, 1994

LOSANO, M.G. y otros, *Libertad informática y leyes de protección de datos personales*, Madrid, Centro de Estudios Constitucionales, 1989

MACINTYRE, A., *Tras la virtud*, Barcelona, Crítica, 1987

McLUHAN, M., *The Global Village*, New York, Oxford Univ. Press, 1989

NEGROPONTE, N., *El mundo digital*, Barcelona, Ediciones B, 1995

SANCHEZ MECA, D., *Metamorfosis y confines de la individualidad*, Madrid, Tecnos, 1995

TERCEIRO, J.B., *Sociedad digital: Del homo sapiens al homo digitalis*, Madrid, Alianza, 1996

VATTIMO, G., *La sociedad transparente*, Barcelona, Paidós, 1990

La L.O.R.T.A.D. y su fututo. La Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal

MANUEL HEREDERO HIGUERAS

Ex-Jefe del Gabinete Jurídico de la Agencia de Protección de Datos. Consultor de Derecho Informático

I. INTRODUCCION

1. La L.O. 5/1992, de 29 de octubre, culminó un proceso de elaboración doctrinal y normativa que se remonta a 1976 y que tuvo varios hitos, en forma de proposiciones no de ley (1986), proposiciones de ley (1987,1988) y un proyecto del Gobierno (1984). Con esta ley, el Reino de España cumplía, además, el compromiso asumido con la ratificación del Convenio 108 del Consejo de Europa [1] , cuyo artículo 4 obliga a los Estados parte a dotarse de una ley interna de protección de datos dentro del plazo que el propio Convenio (artículo 22) prevé para su entrada en vigor. La ley respondía asimismo a las exigencias del Convenio de 1990, de aplicación de los

[1] Convenio del Consejo de Europa, abierto a la firma el 28 de enero de 1981, para la protección de las personas con respecto al tratamiento automatizado de los datos de carácter personal ("B.O.E." de 15 de noviembre de 1985).

Acuerdos de Schengen de 1985[2], cuyo artículo 117 impone a los Estados parte la obligación de dotarse de una legislación interna de protección de datos de un nivel como mínimo igual al del Convenio 108 y de la Recomendación R (87) 15, de 17 de septiembre, del Comité de Ministros del Consejo de Europa, sobre uso de datos personales con fines policiales. La ausencia de tal legislación impedía a los Estados parte servirse de las transmisiones de datos personales previstas en el Convenio de Aplicación. Adherida España en junio de 1991, la legislación de protección de datos pasaba a constituir una condición perentoria para poder beneficiarse del marco de cooperación judicial y policial definido por el Convenio. Publicada la primera propuesta de Directiva comunitaria de protección de datos en 1990 e iniciada la negociación de dicha propuesta en febrero de 1991, el Gobierno remitió a las Cortes en julio de aquel año un proyecto con el que trató de quemar etapas, a cuyo efecto siguió servilmente la regulación de la primera propuesta de Directiva. La ley fue aprobada en octubre de 1992, cuando ya existía una nueva propuesta de Directiva que había modificado sustancialmente la de 1990. El texto definitivo, aprobado en octubre de 1995 [3], volvió a modificar el texto, separándose aún más de la primera propuesta y, por tanto, del texto de la ley española.

2. La ley no agota el ámbito de la protección de los datos personales. El propio texto deja en vigor disposiciones anteriores que regulaban el uso de los datos personales o incidían en dicho uso. Aun cuando el artículo 2-1 hace extensiva la aplicación al uso posterior, "incluso no automatizado", con el fin de salir al paso de una fácil evasión de la ley, sin embargo, el artículo 2-3 dispone que los ficheros automatizados creados en aplicación de la legislación electoral, de la de la Función Estadística Pública, del Registro civil, del Registro Central de Penados y Rebeldes, de materias clasificadas y del Personal militar, se regirían por sus disposiciones propias,

■[2] Acuerdo de Adhesión del Reino de España al Convenio de Aplicación del Acuerdo de Schengen de 14 de junio de 1985 entre los Gobiernos de los Estados de la Unión Económica Benelux, de la República Federal de Alemania y de la República Francesa, relativo a la supresión gradual de los controles en las fronteras comunes, firmado en Schengen el 19 de junio de 1990, al cual se adhirió la República Italiana por el Acuerdo firmado en París el 27 de noviembre de 1990, hecho el 25 de junio de 1991 ("B.O.E." de 5 de abril de 1994; corrección de errores, "B.O.E." de 9 de abril).

■[3] Directiva 95/46/CE, del Parlamento y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos ("D.O.C.E.", L 281, de 23 de noviembre de 1995).

aun cuando tales disposiciones no existían todavía (Registro civil, materias clasificadas, Registro de Penados y Rebeldes). Por otra parte, dichas disposiciones no contenían, en su caso, una regulación completa de la materia, por lo que, en buena técnica, el legislador debía haber previsto la aplicación subsidiaria de la ley en defecto de disposición específica y en caso de disposición contraria. Asimismo, el artículo 2-2 excluyó de la aplicación de la ley a ficheros poco definidos, como son los de información comercial o tecnológica, e informática jurídica, o ficheros cuya exclusión se justifica por el hecho de que la información que contienen es de dominio público. El legislador estimó, sin duda, que la publicidad de esta información primaba sobre el interés individual de la protección de los datos. La Directiva 95/46/CE no excluye de su ámbito estos ficheros. Ante todo, no contempla ficheros, sino tratamientos, como objeto de regulación. Por otra parte, no excluye los tratamientos que la ley excluye de su ámbito, si bien contiene modulaciones expresas de determinadas disposiciones. La transposición requerirá, por ello, reconsiderar a fondo el cuadro de exclusiones. En general, la transposición exigirá un estudio detenido de la ley, no sólo por haber cambiado esencialmente el modelo que la inspirara, sino porque, además, el transcurso de un primer cuatrienio de aplicación de la ley ofrece una experiencia y una perspectiva que permiten apreciar las imperfecciones e insuficiencias de la ley.

II. EL SISTEMA PROTECTOR DE LA LEY

3. Objeto de la ley es regular el tratamiento automatizado de los datos de carácter personal. Así reza su título. El alcance de la regulación no es tecnológico, sino que, como expresa el artículo 1, lo que se pretende es limitar el uso de la informática y otras técnicas y medios de tratamiento automatizado de la información en aras de la salvaguarda de los derechos de la personalidad, que el precepto, recogiendo la fórmula del artículo 18-4 de la constitución, enumera a título indicativo, como el honor, la intimidad personal y familiar y el pleno ejercicio de los derechos. El uso de la voz "intimidad" se explica por el hecho de que los primeros estudios e informes sobre estos problemas se valían del término angloamericano *privacy*. En realidad, en la bibliografía angloamericana se entiende por *privacy* no la intimidad de las personas, sino una facultad de disposición sobre la información personal, o datos expresivos de circunstancias o cualidades de la persona [4]. Es la misma idea que recogería y reformularía en 1983 el Tribunal Constitucional federal alemán con la expresión "derecho de autodeterminación informativa" , en la sentencia recaída en el recurso

■ [4] Cfr. WESTIN, A., Privacy and Freedom, Nueva York, 1968.

contra la ley del Censo de Población de 1982, que el Tribunal declaró nula en parte[5]. El concepto se perfila claramente en los párrafos cuarto y quinto del apartado 1 de la exposición de motivos de la ley. En ellos se trasluce lo que constituye el núcleo del problema que la ley resuelve: la recogida, acumulación y proceso informático de datos de una persona y la adopción de decisiones que le afectan, a partir de un perfil de su personalidad basado en una inferencia automática. La exposición de motivos menciona expresamente algunas de estas posibles decisiones, como "la obtención de un empleo, la concesión de un préstamo o la admisión en determinados colectivos. La ley prevé a tal efecto un sistema *preventivo* o *cautelar*, tendente a evitar que por efecto del uso incontrolado de los datos se produzcan perjuicios a las personas. La Directiva comunitaria ha mantenido la noción de intimidad como bien jurídico específico, pero ha alterado la concepción que inspirara las leyes de protección de datos, en la medida en que el artículo 1 da preferencia a los intereses del mercado. El fin primordial ya no es la protección de los datos de carácter personal, sino la libre circulación de los datos dentro del mercado interior. La protección de los datos es una limitación a la libre circulación, concebida como una norma protectora de alto nivel y como tal excluye toda limitación de la libre circulación de los datos que invoque la protección de los derechos y libertades.

4. El régimen protector de la ley tiene un carácter preventivo, es decir, tiende a evitar que se produzcan perjuicios como resultado del uso indebido de los datos, en lugar de a reparar tales perjuicios *a posteriori*. La ley regula a tal efecto una relación jurídica entre unos *sujetos*, referida a un *objeto*, con un contenido en *derechos* s y *obligaciones*. Estos conceptos se definen en el artículo 3 de la ley. Los sujetos son el *afectado* ("persona física titular de los datos") y el *responsable del fichero* o persona física, jurídica u órgano administrativo, que decide sobre la finalidad, contenido y uso del tratamiento. En el supuesto del artículo 27 (tratamiento de datos personales por contrato de arrendamiento de servicios) aparece un tercer sujeto, que es el contratista o comisionista. A diferencia de la L.O. 1/1982, de 5 de mayo, de protección civil del derecho al honor, la intimidad personal y familiar y la propia imagen, que en su artículo 4 legitima a los herederos y causahabientes para el ejercicio de las acciones pertinentes, la ley no ha creído necesario incluir una norma específica con respecto a los *nascituri* ni a las personas fallecidas, ni tampoco precisar que los

■[5] Sentencia de 13 de diciembre de 1983; versión española en "Boletín de Jurisprudencia Constitucional", Cortes Generales, IV, Jurisprudencia Constitucional Extranjera, 1984-33, págs. 126 y ss.

afectados deban ser personas vivas. En el caso de las personas fallecidas, carecería de sentido el mecanismo cautelar de defensa de los derechos y libertades que prevé la ley, y no serían viables las garantías de la ley, dado el carácter personalísimo de los derechos que reconoce. Por otra parte, si se trata de defender la memoria o el buen nombre de una persona fallecida, son otros los cauces jurídicos pertinentes - Código penal, protección civil del derecho al honor, etc. La Directiva ha añadido otros sujetos y conceptos, que no hacen sino precisar los antedichos.

5. El objeto de la protección viene determinado por los conceptos de *datos de carácter personal*, *fichero* y *tratamiento*. Por *dato*, se entiende "cualquier información concerniente a personas físicas identificadas o identificables". Por tanto, comprende cualquier modalidad de información, entendida en el sentido de las tecnologías de la información, como conjunto de representaciones codificadas, numéricas, alfabéticas, gráficas, o imágenes, susceptibles de registro, proceso o transmisión. La definición ha sido desarrollada en estos mismos términos por el artículo 1-4 del R.D. 1332/1994. La referencia a una persona identificada o identificable convierte los datos personales (género) en "datos de carácter personal" (especie). Cabe, por tanto, entender por dato no sólo la información numérica o alfabética, sino asimismo imágenes, grafismos, etc. La recogida de imágenes (equipos de control mediante pantallas, filmaciones, etc.) y las modalidades del tratamiento de las imágenes deberán, por tanto, ajustarse a los principios de la ley, siempre que sean susceptibles de un tratamiento informatizado. El concepto de *fichero* debe entenderse asimismo en un sentido amplio y flexible, como conjunto organizado de datos objeto de proceso automatizado, "cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso". En este concepto caben desde el fichero complejo, compuesto de muchas unidades conectadas en una red, de implantación territorial múltiple, hasta el fichero mínimo consistente en una tarjeta de memoria o "tarjeta inteligente", susceptible de acceso o, a su vez, instrumento de acceso a otros ficheros. El artículo 2-2 perfila el concepto de fichero excluyendo de la aplicación de la ley, por una parte (apartado a) a los ficheros estrictamente privados de una persona física (agendas, diarios, etc.), y por otra a los que contienen datos personales que ya han pasado al dominio público por reproducir datos ya publicados (apartados c) y d). La ley no considera ficheros a los llevados por partidos políticos, comunidades religiosas, etc., siempre que registren datos de sus miembros y ex miembros. Sin embargo, dado que estos ficheros pueden contener datos de los que el artículo 7 protege especialmente (ideología, religión, creencias, origen racial, etc.) la ley dispone artículo 2-2 e) que se apliquen la norma del artículo 11, que exige el consentimiento de los interesados para la cesión de sus datos, y las disposiciones del artículo 7, en su caso.

6. Por último, el *tratamiento* comprende el conjunto de las distintas operaciones del proceso de los datos, desde la recogida a la cesión y transmisión de los datos. Estas operaciones pueden ser o no ser automáticas, como sucede con la recogida de datos. La ley se limita a los ficheros automatizados. No se aplica a los ficheros manuales o convencionales. Unicamente se alude a los ficheros convencionales en la disposición final 2ª, que prevé la posible extensión del régimen protector a estos ficheros. También se menciona en el artículo 2-1 el "uso posterior, incluso no automatizado" de datos registrados en soporte físico susceptible de tratamiento automatizado, como objeto del régimen protector de la ley. A este uso posterior se aplica la ley, excepto si se trata de ficheros públicos cuyo objeto sea almacenar datos para su publicidad con carácter general (artículo 2-2 a).

7. En el sistema protector delineado por la Directiva el objeto de la protección no son sólo los ficheros automatizados, sino los tratamientos, no sólo automatizados, sino asimismo no automatizados. El concepto de fichero se reserva a estos últimos. Así resulta del artículo 3, según el cual la Directiva se aplica "al tratamiento total o parcialmente automatizado de datos personales, así como al tratamiento no automatizado de datos personales incluidos o destinados a ser incluidos en un fichero". Para ello, la Directiva ha definido el fichero como "todo conjunto estructurado de datos personales, accesibles con arreglo a criterios determinados" . La Directiva se inspiró en las leyes de Alemania y de los Países Bajos, que no limitan la protección a los ficheros automatizados, sino que definen éstos con una fórmula que abarca los automatizados y los manuales. La Directiva estimó que el concepto de fichero automatizado limitaba innecesariamente el ámbito de aplicación y a la vez constituía un concepto superado por la tecnología. En todo caso, los Estados miembros pueden acogerse a un período de adaptación que prevé el artículo 32 de la Directiva, que puede llegar a doce años en lo que respecta a aplicar a los tratamientos no automatizados la parte esencial de la Directiva (principios de calidad de datos, del artículo 6, y condiciones de licitud, en general y con relación a los datos sensibles, artículo 8).

III. LOS PRINCIPIOS DE PROTECCION DE DATOS

8. El contenido de la relación jurídica comprende unos *derechos* de parte del afectado y unas *obligaciones* por parte del responsable del fichero o tratamiento. Así lo expresa el "considerando" 25º de la Directiva. Los principios se enuncian en los artículos 4, 6 y 9 y se desarrollan o modulan en dichos artículos o, en función del contexto, en los artículos 5, 7, 8, 10 y 11 y en los varios preceptos del Capítulo II del

Título IV. Esencialmente se reducen a dos: *proporcionalidad* (cuantitativa y cualitativa) de los datos con relación a la finalidad del fichero y de los tratamientos de los datos registrados en el fichero, y *transparencia* (conocimiento de la existencia del fichero, de sus fines y del responsable). Estos principios fueron formulados por primera vez en las *Directrices* de la O.C.D.E. [6] y recogidos en el Convenio del Consejo de Europa de 1981. Por último, han sido reformulados en el artículo 6 de la Directiva comunitaria 95/46/CE. Los principios enunciados en el artículo 4 concuerdan sustancialmente con los que se enuncian en el artículo 6 de la Directiva, con algunas matizaciones. Un primer grupo de principios comprende los que se enuncian en el artículo 4, con la denominación genérica de "calidad de datos". A su vez, dentro de estos principios, el artículo 4-1 enuncia tres "subprincipios". Sólo es lícito recoger y procesar datos de carácter personal si los datos son *adecuados, pertinentes y no excesivos* con relación al ámbito y finalidades para las que se hubieran obtenido. Las finalidades deben ser *legítimas*. No se declara así expresamente, pero cabe inferir que la recogida y el proceso de los datos no serán lícitos si la finalidad para la que se recogen es ilegítima. En función de la finalidad, los datos han de ser adecuados, pertinentes y no excesivos. Serán adecuados los datos si la finalidad del fichero es una historia clínica y se registran datos acerca de la confesión religiosa, en la medida en que esta circunstancia puede dar lugar a un régimen alimenticio determinado o impedir que se transfunda sangre al interesado. Serán pertinentes los datos que guarden una relación directa con los tratamientos médicos a que se someta el interesado. Por último, no deberán registrarse datos superfluos. El principio de proporcionalidad se recoge también en el artículo 4-5 de la ley de la Función Estadística Pública; según este precepto, la recogida de datos con fines estadísticos debe ajustarse al criterio de correspondencia entre la cuantía de la información que se solicita y los resultados que del tratamiento se pretende obtener.

9. La ley no recoge de manera expresa el principio, que figura en el Convenio del Consejo de Europa, y en el artículo 6-1 *a*) de la Directiva, de la recogida y tratamiento *lícito y leal*. No basta con que los datos sean pertinentes y proporcionados cualitativa y cuantitativamente, sino que han de ser recogidos, además, por medios que no sean *fraudulentos, desleales o ilícitos*. Este principio de la recogida lícita y leal inspira el artículo 5 y se recoge en el artículo 4-7. El primero de estos dos preceptos da por supuesta la noción de "recogida leal". Tomado de la primera propuesta de Directiva,

[6] Directrices sobre la protección de la vida privada y los flujos transfronterizos de datos de carácter personal, Recomendación aprobada por el Consejo de la O.C.D.E. el 23 de septiembre de 1980, versión española, Madrid, Presidencia del Gobierno, 1983.

define un derecho, en lugar de enunciar un principio. El resultado es el mismo, por cuanto que los principios, a su vez, definen derechos del afectado. El artículo 5, por otra parte, limita el ámbito del principio a la recogida de los datos. Algunas leyes, como las del Reino Unido, Irlanda o los Países Bajos, han preferido mantener la fórmula genérica, de tal manera que la práctica vaya precisando en cada caso lo que deba entenderse por "recogida leal". El texto definitivo de la Directiva comunitaria ha definido en los artículos 10 y 11 una *obligación de informar*, que diversifica en cuanto al momento de cumplirla y el contenido, en función de que la recogida de datos sea directa o indirecta.

10. El principio de *finalidad*, recogido en el artículo 4-2, tiene en la ley una expresión sustancialmente distinta que en el precepto correspondiente de la Directiva, concretamente el artículo 6-1 *b*). Según la ley, los datos no podrán usarse para finalidades *distintas* de aquellas para las que hubieran sido recogidos. La ley sigue en este punto a las *Directrices* de la O.C.D.E. de 1980. La Directiva ha optado por la fórmula del Convenio 108 (artículo 5 *b*), proposición segunda), según el cual los datos recogidos no deben ser tratados posteriormente de manera *incompatible* con los fines de la recogida. La Directiva interpreta el alcance de esta incompatibilidad, precisando que el tratamiento de los datos con fines históricos, estadísticos o científicos, no constituye un uso incompatible. La ley no contiene esta matización. La L.F.E.P. recoge en el artículo 4-4 la misma norma del articulo 4-2 de la ley, proclamando el principio de *especialidad*, según el cual "es exigible a los servicios estadísticos que los datos recogidos para la elaboración de estadísticas se destinen a los fines que justificaron la obtención de los mismos".

11. Los artículos 4-3 y 4-4 enuncian el principio de *veracidad* y concuerdan con el artículo 6-1 *d*) de la Directiva. Los datos han de ser exactos y puestos al día de manera que respondan con veracidad a la situación real del afectado. La Directiva es más laxa en este aspecto, por cuanto que exige solamente que se tomen todas las medidas razonables para que los datos inexactos o incompletos con relación a los fines de la recogida o del tratamiento posterior, sean suprimidos o rectificados. Esta norma de la actualización de oficio es inviable en los casos en que el fichero se nutre de datos publicados y accesibles al público. A menos que otros datos que reflejen la nueva situación del afectado se publiquen en iguales términos, la actualización de tales ficheros no es posible. Sin duda, por esta razón, el artículo 4-4 contiene una proposición que deja a salvo los derechos de rectificación y cancelación del afectado. En los casos en que, por las razones antedichas no sea posible la actualización de oficio, deberá ser el afectado el que promueva la rectificación o cancelación por la vía del artículo 15.

12. El artículo 4-6 añade una regla, según la cual el almacenamiento de los datos debe hacerse de manera que sea posible el ejercicio del derecho de acceso por parte del afectado, es decir, de tal manera que sea efectiva la norma del artículo 14-2 de la ley, que exige que la información sobre los datos no requiera el uso de claves o códigos convencionales que, a su vez, precisen usar dispositivos mecánicos específicos. Se trata de una norma de alcance físico-lógico, que tiene por objeto evitar que la configuración lógica de los ficheros dificulte o haga imposible el acceso.

13. La ley ha incluido entre los principios el *consentimiento* del afectado. Es dudoso que deba considerarse como "principio". La norma del consentimiento procede asimismo de la primera propuesta de Directiva, la cual en este y otros puntos siguió de cerca a la ley alemana de 1990, basada en la citada sentencia del Tribunal Constitucional Federal alemán de 1983 [7]. La ley alemana de 1977 hubo de ser modificada para recibir este concepto y a tal efecto tomó como base la norma según la cual todo tratamiento de datos personales es, en principio, ilícito en la medida en que constituye una limitación (*Eingriff*) de los derechos y libertades. En consecuencia, todo tratamiento debe ser prohibido, a menos que el afectado lo consienta o exista una obligación legal que lo imponga. El consentimiento y la obligación legal son así *condiciones de licitud* de todo tratamiento. La primera propuesta de Directiva recibió esta concepción, que, a su vez, tuvo su reflejo en el artículo 6 de la ley española . La norma del artículo 6-1, *in fine*, deja a salvo preceptos anteriores y posteriores a la ley que obligan a dar datos en relación con determinados tratamientos. Cabe citar a este respecto el artículo 7 de la ley de la Función Estadística Pública, que exige para las estadísticas de cumplimentación obligatoria una ley que determine los organismos que elaboren las estadísticas, los fines, el colectivo de personas y el ámbito territorial de referencia, así como la evaluación del gasto previsible. La ley electoral [8], y la ley 7/1985, de 2 de abril, Reguladora de las Bases del Régimen Local [9] se encuadran en esta excepción del artículo 6-1 de la ley. El texto definitivo de 1995 de la Directiva ha flexibilizado esta concepción y ha sustituido el requisito del consentimiento como

■7 Véase, supra, nota 5.

■8 Ley Orgánica 5/1985, de 19 de junio, del Régimen Electoral General ("B.O.E.", de 20 de enero de 1986), art. 32 y disposiciones de desarrollo.

■9 Artículos 16 y 17, versión modificada por la ley 4/1996, de 10 de enero ("B.O.E." de 12 de enero), sobre renovación permanente del Padrón municipal.

condición de licitud por un conjunto de opciones que enumera el artículo 7 de dicho texto como otras tantas condiciones alternativas de licitud. Entre ellas, la del apartado *f)*, a modo de "cajón de sastre", admite como lícito todo tratamiento que responda a un interés prevalente del responsable. El artículo 5 de la Directiva deja un margen de maniobra a los Estados para precisar las condiciones de licitud a partir de estas opciones del artículo 7.

14. La norma del consentimiento, según se recoge en el artículo 6, está referida genéricamente al tratamiento de los datos, no sólo a la recogida. No obstante, el artículo 11 contiene disposiciones específicas para los tratamientos consistentes en cesiones de datos, concepto que se define en el artículo 1 del R.D. 1332/1994. Asimismo, otros preceptos, como los artículos 28, 29 y 30 matizan esta norma. Hay un paralelismo, en parte, entre los artículos 6 y 11 en lo que respecta a las derogaciones o excepciones a la aplicación de la norma del consentimiento. En uno y otro caso el consentimiento no será necesario si el tratamiento lo exige una ley, si los datos se obtienen de datos accesibles al público o si la creación de un fichero automatizado es consecuencia de la libre aceptación de una relación jurídica cuyo desarrollo requiera el tratamiento. El artículo 6 contiene otra excepción, la de que los datos fueran necesarios para el ejercicio de funciones de control y verificación de las Administraciones públicas. Este precepto es uno de los impugnados por los recursos de inconstitucionalidad presentados contra la ley [10]. La accesibilidad pública de los datos como causa de excepción se recoge asimismo en los artículos 28, 29 y 30. Según estos preceptos, una de las condiciones de licitud de los ficheros de solvencia patrimonial o morosidad, así como de los de direcciones, publicidad directa o prospección comercial, es esta accesibilidad pública de los datos. Eta causa de excepción procede asimismo de la primera propuesta de Directiva, pero no figura en el texto definitivo. Esta especie de "privilegio" de los datos accesibles públicamente ha dado paso a una de las condiciones de licitud específicas que para el tratamiento de los datos sensibles enumera el artículo 8 de la Directiva: la de que el propio interesado haya hecho públicos los datos.

15. En todo caso, el consentimiento es necesario si se trata de unos datos de determinada naturaleza, los que la doctrina denomina *datos sensibles*. En general, la doctrina admite que no existen datos que sean sensibles *per se*, sino que lo son sólo en función del contexto en el que se usan. Sin embargo, las legislaciones (Francia,

■ [10] Recurso de inconstitucionalidad 219/1993, presentado por el Defensor del Pueblo.

Noruega, Reino Unido, Luxemburgo, Dinamarca, Suecia) contienen, en general, unas normas de protección reforzada de unos datos de naturaleza determinada, concretamente los datos que revelan o pueden revelar de algún modo la ideología, las creencias, las opiniones políticas, los antecedentes de salud, la vida sexual, la pertenencia a una raza o etnia. El artículo 7 establece dos niveles al respecto. El primer nivel es el relativo a los datos sobre ideología, religión y creencias. En este caso no son aplicables las excepciones que el artículo 6-2 de la ley prevé para el consentimiento previo y en la exigencia de unas determinadas condiciones para la prestación del consentimiento. No obstante lo dispuesto en el artículo 6-2, que enumera unos supuestos en los que, en contra de la norma general del artículo 6-1, no es preciso el consentimiento (datos recogidos de fuentes accesibles al público, datos recogidos para el ejercicio de las funciones propias de las Administraciones públicas, o bien datos relativos a personas vinculadas por una relación negocial, laboral o administrativa, o por un contrato y que sean necesarios para mantener tal relación o cumplir el contrato), si los datos conciernen a la ideología, la religión o las creencias, no pueden ser tratados automáticamente sin el previo consentimiento expreso y por escrito del interesado (artículo 7-2). Tampoco es aplicable a estos datos la excepción del artículo 6-1 i.f., según la cual no es necesario el consentimiento para tratar datos personales en forma automatizada si la ley dispone otra cosa. En el caso de estos datos, la ley no puede autorizar el tratamiento automatizado sin el previo consentimiento expreso y por escrito del interesado, pues una tal ley sería inconstitucional. El segundo nivel lo constituyen los datos que hacen referencia al origen racial, la salud y la vida sexual. En este caso tampoco es aplicable la excepción del artículo 6-1 i.f., por sí sola. Es decir, estos datos podrán ser tratados automáticamente si una ley lo autoriza, pero esto sólo no basta, sino que además será preciso el consentimiento *expreso* (no necesariamente por escrito) del interesado. En cualquier caso, está prohibido (artículo 7-4) crear ficheros cuya sola finalidad sea almacenar datos de uno u otro nivel. La Directiva (artículo 8) da un trato especial a los datos sensibles, exigiendo que los Estados miembros sometan su tratamiento a la existencia de unas condiciones de licitud específicas, que, en parte concuerdan con las generales del artículo 7.

17. La Directiva y el Convenio dan un trato análogo a los antecedentes penales. La ley prevé unas garantías adicionales para estos datos. El artículo 2-3 c) de la ley remite la regulación de estos datos a sus disposiciones específicas. Como tales sólo cabe entender los artículos 136 y 137 del Código penal, el Real Decreto 2012/1983, de 28 de julio, y el Real Decreto 1882/1996, de 2 de agosto, de Estructura Básica del Ministerio de Justicia (artículo 5-2 a) aun cuando, en rigor, no contemplan los ficheros automatizados correspondientes. El nuevo Código penal ha hecho extensivo el régimen del Registro a las medidas de seguridad (artículo 137)..Estas disposiciones

contienen, en todo caso, un *plus* sobre el sistema ordinario de protección, en la medida en que la inclusión de los datos sobre condenas penales en el Registro Central de Penados y Rebeldes (hoy automatizado) requiere una intervención judicial, los datos inscritos no son públicos, y la cancelación de los datos está revestida de unas garantías especiales. El artículo 7-5 de la ley hace una remisión en blanco a las disposiciones respectivamente aplicables en lo que respecta a los datos relativos a sanciones administrativas - sin duda, se trata de las leyes de Caza, Código de la Circulación, etc., que contienen reglas paralelas a las que regulan los antecedentes penales. En realidad, este artículo 7-5 no considera como datos especialmente protegidos los referentes a las condenas criminales o a las sanciones administrativas. El artículo 7-5 no alude a los datos sobre condenas o sanciones, sino a los relativos a la *comisión* de las infracciones. Habrá que entender que los datos referentes al proceso penal o expediente sancionador correspondiente, que precede a la condena o sanción y que puede terminar con la absolución o el archivo de las actuaciones, sólo pueden registrarse en los ficheros automatizados de las Administraciones públicas competentes. Lo que propiamente prevé este artículo 7-5 es una reserva en cuanto al responsable del fichero. Es una norma afín a la del artículo 30 de la ley francesa, aunque menos contundente que ésta. Hay que entender que estos datos (condena o sanción más actuaciones procesales o sancionadoras previas) no pueden ser registrados por cualquier persona o entidad, sino sólo por las Administraciones públicas competentes. El artículo 8-5 de la Directiva, ante todo, da entrada a las infracciones administrativas y a las medidas de seguridad. En un esfuerzo por dar entrada a prácticas en uso en algunos Estados miembros, ha previsto la posibilidad de que estos tratamientos los lleven a cabo entidades privadas, en virtud de una relación contractual, por ejemplo. La norma es que estos tratamientos sólo puedan efectuarse bajo el control de la autoridad pública, a menos que el Derecho nacional prevea unas garantías apropiadas y específicas". La norma matiza que el "registro completo" de condenas penales sólo puede llevarse bajo el control de los poderes públicos. En cuanto a los registros de sanciones administrativas, deja a criterio de los Estados que el tratamiento se efectúe bajo el control de los poderes públicos (artículo 8-5, párrafo segundo).

18. La ley ha dado un trato confuso a los datos de salud. El artículo 8 parece estar inspirado por el propósito de derogar la prohibición genérica del tratamiento automatizado de estos datos, pero a la vez, prever unas garantías específicas. El precepto es poco afortunado. Las remisiones a la Ley General de Sanidad no son válidas, puesto que el artículo 10 de ésta no regula tratamientos automatizados de datos de salud y ofrece, en cambio, un nivel de protección inferior al de la L.O. 5/1992 y al de la Directiva. Las remisiones a la ley del Medicamento no son pertinentes, puesto que se refieren a tratamientos estadísticos, que ya están regulados

con carácter general en la legislación de Estadística. Por último, las excepciones relativas a la investigación epidemiológica se enmarcan en normas sobre tratamientos de datos en investigaciones científicas y análogas. El artículo 8-3 de la Directiva ofrece un cuadro normativo más amplio y flexible..

19. El artículo 7 del Convenio del Consejo de Europa elevó a principio de protección de datos la obligación del responsable del fichero de adoptar medidas de *seguridad de los datos*. En este caso se trata de medidas de protección física o lógica, o ambas. La norma se recogió asimismo en la primera propuesta de Directiva y pasó, más simplificada, al texto definitivo (artículo 17-1). Las legislaciones concuerdan en imponer esta obligación al responsable del fichero. La ley española ha optado por una vía media entre lo que sería una regulación detallada en el texto de la ley y la mera imposición de una obligación al responsable del fichero. Del texto del artículo 9-1 se deduce que las medidas habrán de ser técnicas y de organización, que eviten la pérdida, alteración y acceso no autorizado. Se trata, pues, de medidas de protección de los datos y medidas de protección del entorno (control del acceso a locales, sistemas, programas). Las medidas se han de basar en varios criterios: naturaleza de los datos, riesgos potenciales y estado de la tecnología. El criterio de la naturaleza de los datos se precisa en el artículo 9-3, que dispone que se adoptarán medidas especiales para la protección - física - de los datos del artículo 7. Sobre esta materia existe ya un amplio cuerpo de doctrina, que ha cristalizado en las *Directrices* que sobre seguridad de sistemas de información aprobó la O.C.D.E. en noviembre de 1992 [11]. Según el artículo 9-2 las condiciones de seguridad se determinarán por vía reglamentaria y el responsable no podrá registrar datos si el fichero no reuniere tales condiciones. El artículo 9-2 de la ley no ha sido todavía objeto de desarrollo reglamentario, lo cual da lugar a una situación peculiar. Según dicho precepto "no se registrarán datos de carácter personal en ficheros automatizados que no reúnan las condiciones que se determinen por vía reglamentaria con respecto a su integridad y seguridad y a las de los centros de tratamiento, locales, equipos, sistemas y programas". Transcurridos cerca de cinco años desde la promulgación de la ley, el Gobierno no ha hecho uso de esta habilitación reglamentaria. Sin embargo, los ficheros han venido registrando datos y la Agencia de Protección de Datos los ha inscrito. Teóricamente ni lo uno ni lo otro debería haber

■[11] O.C.D.E., Lignes Directrices régissant la sécurité des systèmes d'information, París, 1992, OCDE/GD (92) 190

sido posible. La Agencia se pronunció en forma confusa al respecto en la *Memoria* de 1994 [12].

IV. LOS DERECHOS DEL AFECTADO

20. El sistema protector se completa con el reconocimiento de unos derechos, de carácter medial o instrumental a los interesados, "titulares de datos", "afectados", etc. mediante los cuales se hacen valer los principios. De entre los *derechos* o *garantías* que la ley reconoce en el Título III, el principal, que, a la vez, constituye la pieza esencial del sistema protector, es el *derecho de acceso*, en sentido amplio o derecho a conocer la mera existencia de un fichero de datos personales (artículo 13), y en sentido estricto o derecho a conocer los datos (artículo 14). Estos derechos son condición para

■12 "Podemos concluir, por tanto, que la Ley Orgánica proporciona un sistema de objetivos y criterios en materia de seguridad de los 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 dichos criterios en una regulación detallada como la prevista en los apartados 2 y 3 del artículo 9 de la Ley Orgánica", Memoria 1994, Madrid, 1995, pág. 67. No obstante, la Agencia ha acometido este problema con relación al control del acceso a determinados edificios, mediante las Instrucciones 1/1996, y 2/1996, ambas de 1 de marzo ("B.O.E." de 12 de marzo). En todo caso, la ausencia de una regulación general ha dado lugar a disposiciones reglamentarias de alcance departamental, como las siguientes: Resolución de 29 de noviembre de 1996, de la Subsecretaría de Economía y Hacienda, por la que se dictan instrucciones relativas a los accesos a las bases de datos de la Agencia Estatal de Administración Tributaria ("B.O.E." de 20 de diciembre); Orden de 28 de marzo de 1996, de la Consejería de Economía, Industria y Hacienda de la Comunidad Autónoma de Extremadura, por la que se regulan los accesos a las bases de datos de la Agencia Estatal de Administración Tributaria ("D.O.E." de 13 de abril); Decreto Foral 317/1996, de 9 de septiembre, por el que se regula el acceso a los ficheros automatizados de la Dirección General de Hacienda y la utilización de la información contenida en los mismos ("B.O.N." de 25 de septiembre); Circular de la Dirección General de Gestión Tributaria y Fondos Europeos de la Comunidad Autónoma de Madrid, sobre acceso y utilización de la información contenida en la Base de Datos Nacional de la Agencia Estatal de Administración Tributaria ("B.O.C.M." de 12 de septiembre); Orden de 17 de enero de 1996, del Ministerio de Trabajo y Seguridad Social, de regulación de los accesos al sistema informático de la Seguridad Social ("B.O.E." de 25 de enero). Al fin, la Agencia ha redactado un proyecto de Reglamento de Seguridad, basado en textos de Suecia y Países Bajos, que ha sido elevado al Ministerio de Justicia a finales del año 1996, del cual se da cuenta en la Memoria 1996 de la Agencia (Madrid, 1997, págs. 239-244).

poder ejercitar los de rectificación o cancelación de datos (artículo 15), también reconocidos en el artículo 8 c) del Convenio. La versión definitiva de la Directiva no reconoce un derecho separado a conocer la mera existencia del fichero, pero impone a los Estados miembros que adopten las medidas necesarias para garantizar la publicidad de los tratamientos (artículo 21-1), precisando que a tal efecto la autoridad de control deberá llevar un registro de los tratamientos notificados, es decir, de aquellos que, de acuerdo con lo dispuesto en los artículos 18-2 y 20-1 deban serlo por afectar a los derechos y libertades. El artículo 21-3 dispone que deberán adoptarse medidas para que las personas que lo soliciten sean informadas por los responsables o por un organismo determinado, acerca de los tratamientos que no debieren ser notificados.

21. Sólo mediante esta publicidad, registral o individualizada, es posible ejercitar el derecho que el artículo 13 reconoce y, en un segundo estadio, los derechos reconocidos en los artículos 13, 14 y 15. La ley prevé a tal efecto en los artículos 24 y 38 la inscripción de los ficheros en el Registro General de Protección de Datos, que, a su vez, constituye un órgano integrado en la Agencia de Protección de Datos (artículo 38-1). Según el artículo 38, todos los ficheros, cualquiera que sea su titular, deben ser inscritos en dicho Registro. Esta obligación "universal" de notificar procede de la primera propuesta de Directiva comunitaria. Los artículos 5 a 10 del R.D. 1332/1994 han regulado el procedimiento de notificación e inscripción, en uso de la habilitación reglamentaria del artículo 38-3 de la ley. La ley no tipifica expresamente como infracción administrativa la omisión de la inscripción. Puede incluirse este supuesto en el del apartado d) del artículo 43-3 (infracciones leves): infracciones que afecten a "cuestiones meramente formales o documentales" y que no constituyan infracción grave o muy grave. La inscripción requiere la previa notificación del fichero. Aun cuando los artículos 8 y 24 contemplan lo referente a la creación de los ficheros, el primero los de titularidad pública y el segundo los de titularidad privada, sólo este último menciona expresamente la notificación y ulterior inscripción. Cabría pensar que los ficheros de titularidad pública no tienen que ser notificados ni inscritos, y que bastaría con que fueran creados por el cauce de una disposición de carácter general. En rigor, la publicación de la disposición general en un diario o boletín oficial es una publicidad mayor, y además la disposición es recurrible en vía contencioso-administrativa. Sin embargo, el artículo 38-2 es terminante. El artículo 38-3 se remite a las disposiciones reglamentarias que regulen el procedimiento de inscripción, y se refiere expresamente a los de titularidad pública y a los de titularidad privada. Por ello, no hay duda de que unos y otros deben ser inscritos. La ley no precisa, sin embargo, si para inscribir los ficheros públicos es precisa una formalidad de notificación expresa. Existe un "hueco" entre la publicación de la disposición general de creación en el "Boletín Oficial del Estado" o diario oficial (artículo 18-1), y la inscripción. En el caso

de los ficheros de titularidad privada, la notificación y la creación se confunden, puesto que para crear el fichero, es preciso notificarlo, dando al Registro la información que prevé el artículo 24. En cambio, en los ficheros de titularidad pública, el artículo 18 sólo regula la creación del fichero. En las disposiciones reglamentarias dictadas en ejercicio de la habilitación del artículo 38-3, a saber, el R.D. 1332/1994, ha sido aclarado este punto. Los artículos 5, 7-1, 7-3 y 8-1 de dicho Real Decreto regulan separadamente la notificación y la inscripción de los ficheros de titularidad pública. La finalidad de la inscripción se deduce claramente de los artículos 13 y 38-2 e). Este último dispone que la inscripción debe contener los datos necesarios para el ejercicio de los derechos de información (artículo 13), acceso (artículo 14), y rectificación y cancelación (artículo 15). El R.D. 1332/1994 y la Resolución de 22 de junio de 1994, de la Agencia de Protección de Datos, han alterado la orientación de la ley en lo referente a la notificación y la inscripción, en la medida en que exigen como trámite previo la aportación de una información pormenorizada sobre la adecuación de los ficheros a las disposiciones de la ley por medio de la cumplimentación del formulario anejo a la Resolución. Lo que la ley parecía concebir como un acto certificante de la existencia, fines y responsables de los ficheros, se convierte así, de hecho, para los ficheros de titularidad privada en una verdadera autorización administrativa [13] .

22. Si, en un principio, la notificación tuvo esta finalidad de hacer posible el ejercicio de los derechos del afectado, la Directiva comunitaria ha dado una orientación distinta a la notificación. El artículo 18 del texto definitivo recoge la notificación como norma, pero, a diferencia de la primera propuesta, admite la posibilidad de eximir de la notificación o prever una notificación simplificada en el caso de los tratamientos que no pudieren afectar a los derechos y libertades. Para ello, es preciso que el Estado miembro identifique tales tratamientos (artículo 18-2 en relación con el 20-1).. Otra opción consiste en la designación de un comisario de protección de datos. El precepto no precisa si este comisario, "encargado de protección de los datos personales" sólo procede si el responsable del tratamiento es una persona privada o si, por el contrario, también los organismos públicos pueden designar a un encargado. El encargado asume dentro de la organización respectiva funciones propias de la autoridad de control, tales como hacer cumplir las disposiciones de transposición de la Directiva, y llevar un registro de los tratamientos. La Directiva exige que el encargado sea eficaz, es decir, no basta con el nombramiento,

■[13] La Memoria 1994 de la Agencia de Protección de Datos lo entiende así, ya que en las páginas 38-40 enumera unos ficheros "archivados" por no cumplir los requisitos de la ley.

sino que es preciso que garantice que el tratamiento de los datos no pueda ocasionar una merma de los derechos y libertades de los interesados. También cabe eximir de la notificación otros tratamientos, como son los que tienen por finalidad llevar un registro destinado a informar al público y abierto a su consulta por el público en general o por cualquiera que acredite un interés legítimo (artículo 18-3). Por último, cabe la exención de la notificación cuando el tratamiento se lleve a cabo por una fundación, asociación u otro organismo sin fin de lucro cuya finalidad sea política, filosófica, religiosa o sindical, siempre que se refiera solamente a sus miembros y ex miembros o personas relacionadas con la entidad y siempre que no se cedan los datos a terceros sin consentimiento de los interesados (artículo 18-4 en relación con el 8-2 d). La notificación es previa a la realización del tratamiento. De este modo la autoridad de control o el encargado del tratamiento pueden comprobar si el tratamiento afecta o no a los derechos y libertades. La comprobación puede llevarse a cabo si el tratamiento ha sido regulado por ley o disposición reglamentaria o sobre la base de la misma (artículo 20-3).

23. El derecho de acceso fue definido desde un primer momento, antes de que se promulgaran las primeras leyes de protección de datos, siendo bautizado con la expresión *habeas data*, por estimar que constituía una modalidad de acción exhibitoria análoga a la de *habeas corpus*. Con el nombre de *habeas data* fue recogido en la Constitución de 1988 del Brasil. La ley ha utilizado la expresión más extendida, aun cuando no es la más afortunada, ya que el "acceso" a los datos es propiamente una operación técnica o mecánica. Por ello, el artículo 14-2 de la ley muestra que no se trata del mero uso de un terminal o un equipo autónomo en el que figuren los datos, sino que de lo que se trata es de conocer el contenido o significado de los datos. Cabe, por ello, la mera consulta mediante visualización en pantalla o su comunicación "en forma legible e inteligible", sin utilizar claves o códigos convencionales que requieran el uso de dispositivos mecánicos específicos". El artículo 14 sólo permite el acceso a los datos registrados, pero no precisa si también pueden ser objeto del acceso otras informaciones, tales como la procedencia de los datos (fuentes accesibles al público, recogida indirecta, etc.), o los datos generados por los procesos del tratamiento. El artículo 29, en cambio, permite expresamente que el afectado sea informado del origen de los datos que sobre él figuran en ficheros de publicidad directa y análogos. Asimismo, el artículo 28-2 permite que las personas cuyos datos figuren en ficheros de morosos o de solvencia accedan no sólo a sus datos, sino igualmente a las "evaluaciones y apreciaciones" que sobre el afectado hayan sido comunicadas al responsable del fichero en el curso de los seis últimos meses. También puede conocer el afectado, por medio del derecho de acceso, el nombre y dirección del cesionario de tales evaluaciones y apreciaciones. El R.D. 1332/1994 (artículo 13-2) ha generalizado

el acceso a los datos resultantes de los procesos, a su origen y a los cesionarios de los datos.

24. El artículo 17 añade a estos derechos lo que puede denominarse "derecho de recurso judicial". Este derecho figura asimismo en el artículo 22 de la Directiva y se recogió igualmente en el artículo 8 d) del Convenio 108 para los supuestos de denegación del acceso o de la rectificación de los datos. La ley ha añadido, además, un derecho a obtener indemnización en caso de daño o lesión en los bienes o derechos, causados por el incumplimiento de la ley por parte del responsable del fichero. La indemnización puede exigirse por vía civil en los casos de ficheros de titularidad privada (artículo 17-5), o por los cauces previstos en la legislación reguladora del régimen de responsabilidad de las Administraciones Públicas (artículo 17-4)[14].

25. Tanto el Convenio 108 del Consejo de Europa como la Directiva comunitaria prevén la posibilidad de excepciones a las normas reguladoras de los derechos del afectado. El artículo 9 del Convenio se inspira en los apartados 2 de los artículos 6, 8, 10 y 11 del Convenio Europeo de los Derechos del Hombre de 1950, que, con relación a cada uno de los derechos que reconoce, prevén la posibilidad de establecer excepciones. Para ello es preciso que la excepción constituya una medida que en una sociedad democrática sea necesaria para defender determinados bienes jurídicos. El precepto marco del Convenio 108 es el artículo 9-2, que recoge dicho concepto y condiciona las excepciones a que se trate de medidas necesarias para proteger la seguridad del Estado, la seguridad pública, los intereses monetarios del Estado o la represión de los delitos, o para proteger al propio interesado o los derechos y libertades de otros. La Directiva recoge en el artículo 13 la norma del artículo 9 del Convenio, haciendo extensiva a todos los derechos del interesado la posibilidad de excepciones o limitaciones, pero, en todo caso, a condición de que constituyan medidas necesarias a igual efecto. La ley ha procurado lograr un equilibrio de los diversos bienes jurídicos e intereses involucrados, haciendo uso de esta facultad en diversos preceptos. Las excepciones que prevé la ley hacen referencia, de una parte, a los principios (Título II) y, de otra, a los derechos o garantías de los principios (Título III). La norma general viene expresada en el artículo 22, que establece unas causas de

■[14] La regulación vigente al respecto está constituida por el real Decreto 429/1993, de 26 de marzo, por el que se aprueba el Reglamento de Procedimientos de las Administraciones Públicas en materia de responsabilidad patrimonial ("B.O.E." de 4 de mayo).

excepción a la obligación de informar prevista en el artículo 5 de la ley, cuando la información pudiere crear riesgos para el ejercicio de las funciones de control y verificación de las Administraciones Públicas [15]. Asimismo, la recogida y tratamiento automatizado de datos con fines policiales está exceptuada de la aplicación de la norma del consentimiento (artículo 20-2), aun tratándose de datos sensibles (artículo 20-3). Los datos recogidos o elaborados por las Administraciones Públicas no tienen que ajustarse a lo dispuesto en el artículo 11 en cuanto a las cesiones de datos (artículo 19-1 y 19-2). El artículo 21-1 contiene una excepción de la aplicación de los derechos del afectado cuando se trata de ficheros de las Fuerzas y Cuerpos de Seguridad: en este caso, cabe la denegación pura y simple si se dan ciertos supuestos de riesgo para la defensa, la seguridad, o las investigaciones policiales en curso.

26. Otra excepción, prevista asimismo en el artículo 21-2, hace referencia a los ficheros tributarios. Esta excepción se funda igualmente en el artículo 9-2 del Convenio, que enumera entre las posibles causas de excepción a las disposiciones del Convenio, las medidas que fueren necesarias para proteger los "intereses monetarios del Estado". Los responsables de estos ficheros pueden denegar el acceso a los datos "cuando el mismo obstaculice las actuaciones administrativas tendentes a asegurar el cumplimiento de las obligaciones tributarias y, en todo caso, cuando el afectado esté siendo objeto de actuaciones inspectoras". Este precepto invalida la práctica de la Administración tributaria de denegar sistemáticamente el acceso a los ficheros fiscales, en aras del respeto a la intimidad del propio interesado [16]. También en este caso cabe la reclamación ante la Agencia de Protección de Datos si el afectado estima que no se

■ [15] Véase, supra, nota 10.

■ [16] Cfr. la sentencia de 13 de noviembre de 1991, del Tribunal Superior de Justicia de Madrid, Sala de lo Contencioso-Administrativo, Sección Novena, R.C.A. nº 639/91. La recurrente, invocando el Convenio 108 del Consejo de Europa, había solicitado del Centro de Proceso de Datos del Ministerio de Economía que le notificara los datos de carácter personal que sobre su persona se encontraran en dicho Centro de Proceso de Datos, así como las finalidades principales para las que fueran utilizados dichos datos. La Dirección General de Informática Tributaria denegó la notificación, aduciendo que " ... la información disponible en las bases de datos tributarios debe considerarse confidencial, ... y únicamente el personal autorizado al efecto debe tener acceso a la misma, estando obligado a guardar el más estricto secreto a propósito de su contenido". Interpuesto recurso contencioso-administrativo por la vía de la ley 62/1978, el T.S.J.M. no lo estimó, declarando que la recurrente conocía los datos por haberlos dado y que la obligación de todo ciudadano de contribuir a las cargas públicas constituye una limitación al derecho a la intimidad personal.

dan los supuestos del artículo 21-2. Al margen de estas excepciones expresas, el artículo 22-2 prevé la posibilidad de denegar el acceso a ficheros de titularidad pública cuando así lo aconseje una ponderación de los intereses en presencia -el interés del afectado, de una parte, y el interés público o los intereses prevalentes de terceros, de otra. La denegación ha de ser motivada y notificada al afectado, con expresión de los derechos que le asisten en cuanto a formular reclamación ante la Agencia de Protección de Datos. Por lo que respecta a los ficheros de titularidad privada, la ley no admite excepción alguna al derecho de acceso. Las excepciones al derecho de acceso se aplican por analogía a los derechos de rectificación y cancelación, según se deduce del artículo 22-1 i.f. [17]. El artículo 16 del R.D. 1332/1994 ha añadido una opción para el caso de que no sea posible la cancelación física de los datos o cuando se pretenda cancelar datos que hubieran sido recogidos o registrados por medios fraudulentos, desleales o ilícitos: en tales casos procederá el bloqueo de los datos, modalidad de tratamiento que se define en el artículo 1-1 de dicho R.D. como "*la identificación y reserva de datos con el fin de impedir su tratamiento*".

V. LA AGENCIA DE PROTECCION DE DATOS.

27. En los varios anteproyectos y proposiciones de ley se incluía un órgano específico que debía asumir el control de la aplicación del sistema protector determinado por la ley. Es a noción se conceptualiza por primera vez en la Resolución del Parlamento Europeo de 1979 [18] y, sobre todo, en la primera propuesta de Directiva comunitaria, cuyo artículo 26 imponía a los Estados miembros de la Unión Europea la obligación de crear una autoridad encargada de vigilar la aplicación en su territorio de las disposiciones de transposición de la Directiva. La ley prescindió de los propuestas de los citados anteproyectos y proposiciones de ley y sólo tuvo en cuenta la primera propuesta de Directiva comunitaria. La exigencia de una autoridad "independiente" tenía su base en la preocupación, que se refleja en el § 10, apartado 2, de la primera ley de Hesse (1970) y en la ley francesa de 1978, de que la concentración de grandes volúmenes de información en manos del Ejecutivo pudiera trastocar el orden

■[17] Hay una errata en la remisión que el artículo 22-1 hace al 15-1: debe ser al 15-2.

■[18] Resolución de 8 de mayo de 1979, del Parlamento Europeo, sobre la protección de los derechos de la persona ante el desarrollo de los progresos técnicos en el ámbito de la informática ("D.O.C.E.", nº C 140, de 5 de junio de 1979.

constitucional. El § 10, apartado 2, de la citada ley de Hesse atribuyó, por ello al Comisario de Protección de Datos del *land* la función de observar las repercusiones que el tratamiento mecánico de los datos tuviere sobre los métodos de trabajo y las competencias decisorias de las Autoridades "*... determinando si tales repercusiones conducen a un desajuste en la división de los poderes entre los órganos constitucionales del Estado, o entre los órganos de la Administración autónoma estatal y municipal*". El Comisario podría en tal supuesto promover las medidas que estimare idóneas en orden a impedir tales repercusiones. Esta misma preocupación tuvo asimismo su reflejo en la composición inter-poderes de la CNIL francesa. Todo ello tenía su explicación en el hecho de que a la sazón los grandes sistemas de información de carácter personal fueran los del sector público. Esto explica igualmente que la primera medida adoptada en Francia cuando se inició la tramitación de la que sería ley de Informática y Libertades de 1978 fuera la prohibición de toda interconexión de ficheros de datos personales del sector público y la consiguiente frustración del proyecto S.A.F.A.R.I. de creación de un gran fichero informatizado de los ciudadanos franceses basado en un identificador universal. Es significativo, sin embargo, que ninguna de las demás leyes de primera generación, la mayoría coetáneas de la ley francesa - alguna incluso anterior, como la primera ley federal alemana, de 1977 - no previeran la creación de una administración independiente ni le atribuyeran la función mencionada de restaurar el equilibrio constitucional. Ninguna de las autoridades de control que dichas leyes crearon era externa a la Administración, sino que incluso estaban bajo la dependencia de un Ministro. La nueva ley de Hesse de 1986 no contiene ya una disposición análoga. La ley creó (artículo 34) un Ente público independiente, con la denominación de Agencia de Protección de Datos. En cumplimiento de lo dispuesto en el apartado 2 de dicho artículo y en la disposición final 1ª, la Agencia fue dotada de un Estatuto que fue aprobado por el Real Decreto 428/1993, de 26 de marzo. Al frente de la Agencia hay un Director (artículo 35), y en ella se integra un Registro General de Protección de Datos (artículo 38). La Agencia es, pues, una persona jurídica distinta del Estado que, como tal, no está inserta en la estructura jerarquizada de la Administración.

28. El legislador estimó que la única posibilidad de ajustarse al modelo definido en la propuesta de Directiva era la de configurar a la Agencia como una de las llamadas "Administraciones independientes", concepto que comienza a perfilarse en la doctrina [19]. La Agencia se alinea así con una treintena de Entes públicos, tales

[19] Cfr. GALLEGO ANABITARTE, A., DE MARCOS FERNANDEZ, A., Derecho administrativo I. Materiales, Madrid, 1989, págs. 125 y ss.; PARADA, J.R., Derecho administrativo, III. Organización y empleo público, 7ª edición, Madrid, Marcial Pons, 1993, capítulo VIII;

como la Comisión Nacional del Mercado de Valores, Puertos del Estado, Aeropuertos, etc., regidos por el artículo 6-5 de la ley General Presupuestaria y, en la actualidad, por los artículos 53 a 65 y la disposición transitoria tercera, de la ley 6/1997, de 14 de abril, de Organización y Funcionamiento de la Administración General del Estado. El artículo 34-1 de la ley define a la Agencia de Protección de Datos como un Ente de Derecho público "que actúa con plena independencia de las Administraciones Públicas en el desempeño de sus funciones". La misma norma se recoge en el artículo 1-2 del Estatuto. Asimismo, el artículo 35-2 dispone que el Director de la Agencia "no estará sujeto a instrucción alguna en el desempeño" de sus funciones. Por último, el artículo 16 del Estatuto desarrolla esta doble noción, disponiendo que el Director desempeña su cargo "con plena independencia y objetividad" y que "no estará sujeto a mandato imperativo, ni recibirá instrucciones de autoridad alguna". Esto implica la ausencia de toda relación jerárquica o de tutela. El artículo 1-2 i.f. del Estatuto se limita, por ello, a establecer un cauce de relación de la Agencia con el Gobierno, que es el Ministro de Justicia. En concreto, el Ministro de Justicia propone al Gobierno el candidato a Director y los candidatos a vocales del Consejo Consultivo, propondrá al Gobierno las disposiciones de desarrollo reglamentario (artículo 5 del Estatuto), y elevará a los órganos competentes [20] la propuesta de relación de puestos de trabajo (artículo 37-1 del Estatuto), y elevará a las Cortes Generales la Memoria Anual (artículo 8-2 del Estatuto). Otros cauces de relación son la Intervención General de la Administración del Estado, en lo que respecta a la rendición de cuentas al Tribunal de Cuentas (artículo 33-1 del Estatuto); y el Ministro de Economía y Hacienda para la elevación al Gobierno del proyecto de Presupuesto (artículo 34-1 del Estatuto). Siguiendo el patrón utilizado para otros entes públicos, el Estatuto ha exceptuado a la Agencia del régimen general del control de la Intervención General de la Administración del Estado, disponiendo en el artículo 33-3 que el control de las actividades económicas y

GARCIA LLOVET, E., Autoridades administrativas independientes y Estado de Derecho, "Revista de Administración Pública", nº 131 (mayo-agosto 1993). Sobre los problemas de la Agencia de Protección de Datos como autoridad independiente, véase el dictamen 97/93, de 18 de febrero de 1993, del Consejo de Estado, relativo al proyecto de Estatuto de la Agencia, págs. 15-16.

■[20] Los órganos competentes a que se refiere este precepto son los que se determinan en la ley 37/1988, de 28 de diciembre, artículo 37, y en el Real Decreto 469/1987, de 3 de abril ("B.O.E." de 9 de abril): Ministerios de Economía y Hacienda y para las Administraciones Públicas, y Comisión Interministerial de Retribuciones.

financieras de la Agencia se ajustará al procedimiento de control financiero de carácter permanente [21].

29. La Agencia se rige por las disposiciones de los artículos 34 a 39 de la ley y por las del Estatuto. El Estatuto ha añadido algunas funciones a la Agencia, en uso de la habilitación contenida en el artículo 36 n) de la ley. Son las que definen los artículos 4-1, 5 *b*), 5 *d*), 6, 8-2, 9, y 10. El artículo 3-1 del Estatuto se remite al artículo 36 de la ley. Este precepto hace una enumeración de las funciones de la Agencia, sin un criterio sistemático. Cabe esbozar una sistematización de estas funciones y agruparlas como sigue: a) funciones de *policía administrativa*: emitir autorizaciones (artículo 36 b); ordenar la cesación de los tratamientos de datos y la cancelación de los datos cuando el tratamiento no se ajuste a la ley (artículo 36 f); ejercer la potestad sancionadora (artículo 36 g); ejercer el control del movimiento internacional de datos (artículo 36 l); velar por el cumplimiento de la legislación estadística del Estado, en lo referente a la recogida de datos y al secreto estadístico y dictar instrucciones sobre la seguridad de los ficheros estadísticos (artículo 36 m); b) funciones de *prestación*: dictar instrucciones para adecuar los tratamientos automatizados a los principios de la ley (artículo 36 c); informar a las personas de sus derechos en materia de tratamiento automatizado de datos personales (artículo 36 e); velar por la publicidad de los ficheros y a tal efecto llevar el Registro General de Protección de Datos (artículo 38) y publicar periódicamente una relación de los ficheros (artículo 36 j). Cabría añadir otras funciones, como la *consultiva* en materia de desarrollo reglamentario de la ley (artículo 36 h), y la de *cooperación internacional* (artículo 36 l), segundo inciso), que comprende entre otras cosas, la cooperación interinstitucional prevista en el artículo 13-3 del Convenio 108, en el artículo 115 del Convenio de Schengen de 1990 (artículo 10 del Estatuto) y en el artículo 29 de la Directiva comunitaria. . La Agencia no tiene atribuida una potestad reglamentaria, pero coopera al desarrollo reglamentario (artículo 36 h), disposición final segunda). También tiene atribuida la Agencia una función de orientación en cuanto a la elaboración de los códigos tipo o normas deontológicas previstos en el artículo 31, mediante los cuales se podrán completar a escala sectorial y de empresa las disposiciones reglamentarias de desarrollo de la ley. El Estatuto de la

■ [21] El control financiero permanente se rige por el Real Decreto 1124/1978, de 12 de mayo, por el que, con el carácter de Instrucción Provisional, se desarrollan las normas de los artículos 17 y 18 de la ley General Presupuestaria. En el caso de la Agencia de Protección de Datos, este R.D. ha sido desarrollado por la Circular 2/1994, de 28 de julio, de la Intervención General de la Administración del Estado, por la que se dan instrucciones para el ejercicio del control financiero permanente en la Agencia de Protección de Datos ("B.O.M.E.H." de 6 de octubre de 1994).

Agencia ha resuelto ciertas ambigüedades que en cuanto a las relaciones orgánicas y al proceso de adopción de decisiones ofrecía la ley. La ley atribuye la decisión unas veces a la Agencia (artículos 17-1, 17-2, 24-5, 36, 47, 48) y otras al Director (artículos 21-3, 22-2, 31-2, 32, 35, 40-3, 41-1, 41-2, 43-2 b), 43-4 d), 43-4 e), 45-1, 45-2, 45-3, D.F. 2ª). El Estatuto ha concentrado todas las funciones de decisión en el Director, como centro de imputación de todas las decisiones de la Agencia que tengan trascendencia externa. El Estatuto diferencia entre estas funciones del Director como titular de la Agencia y centro de imputación de las decisiones ad extra, de una parte, y las de *manager* de la Agencia, de otra. La distinción se recoge con toda claridad en los artículos 12 y 13 del Estatuto, que regulan por separado las funciones de dirección y las de gestión, respectivamente. Sólo las funciones de gestión, excepto el control económico-financiero de la Agencia, la aprobación de la Memoria Anual y la convocatoria del Consejo Consultivo, pueden ser delegadas en el Secretario General. Las funciones de dirección, en cambio, no son delegables. El artículo 3-3 del Estatuto imputa al Director todas las decisiones institucionales de la Agencia, entendiendo por tales las que tienen trascendencia externa. Así se refleja asimismo en los artículos 12-2 y 13 y en el artículo 3-4. Este último precisa que las resoluciones del Director agotan la vía administrativa y abren la vía al recurso contencioso-administrativo. El administrado (afectado o responsable del fichero) puede, por ello, instar la revisión jurisdiccional de los actos de la Agencia, interponiendo el recurso contencioso-administrativo contra las resoluciones del Director. A este efecto, puede acogerse, bien al régimen ordinario de la ley de la Jurisdicción Contencioso-Administrativa, bien al régimen especial de la ley 62/1978, de Protección Jurisdiccional de los Derechos de la Persona, en función del derecho respectivamente lesionado.

30. Abundando en este criterio, de identificar la Agencia con el Director en el plano operativo, el artículo 16-1 del Estatuto define la independencia, no de la Agencia, sino del Director, en cuanto persona que "ostenta la representación de la Agencia": el Director desempeña su cargo "con plena independencia y total objetividad", no está sujeto a mandato imperativo "ni recibe instrucciones de autoridad alguna" (artículo 16-2). Además de resolver la aludida ambigüedad, el Estatuto ha simplificado el proceso decisorio, evitando niveles intermedios de decisión, como pudieran ser el Registro General de Protección de Datos o la Inspección de Datos. En caso contrario, el acceso al recurso contencioso-administrativo contra las resoluciones del Registro o de la Inspección habría requerido un recurso de alzada interno ante el Director. Por ello, los artículos 26 y 29 atribuyen al Registro y a la Inspección una función meramente instructora, correspondiendo la resolución exclusivamente al Director. La Agencia es, por ello, mero dispositivo de apoyo del Director. El artículo 37 completa el dispositivo de apoyo del Director con un órgano de asesoramiento, el

Consejo Consultivo, formado por representantes de los sectores sociales y económicos más directamente interesados. La ley no detalla, sin embargo, los supuestos en los que el Director debe requerir el parecer del Consejo Consultivo. El Estatuto (artículo 18-2) se ha limitado a prever que el Consejo emita dictamen siempre que el Director lo recabe, sin perjuicio de que el Consejo eleve propuestas al Director sobre la materia propia de la ley.

31. El dispositivo orgánico no se agota en los órganos que crean los artículos 34 a 39. El artículo 40 abre la vía a unos órganos paralelos de las Comunidades Autónomas. Excepto las funciones consistentes en el control del movimiento internacional de los datos y en el ejercicio de la potestad sancionadora y de inmovilización de ficheros (artículos 36 f), g) y l), 45 y 48), las funciones de la Agencia podrán ser asumidas por órganos autonómicos específicos. A pesar de que el artículo 40-1 atribuye solamente a la Agencia el ejercicio de la función de publicidad de los ficheros, prevista en el artículo 36 j), por medio del Registro General de Protección de Datos, el artículo 40-2 habilita, sin embargo, a las Comunidades Autónomas a que creen sus propios registros para la publicidad de sus ficheros públicos [22]. A la vista de esta habilitación, cada Comunidad Autónoma podrá crear un órgano de competencia general, atribuir estas funciones a un órgano existente, o crear una pluralidad de órganos de control de tipos concretos de ficheros [23].

32. ¿Hasta qué punto ha hecho la Agencia de Protección de Datos un uso racional de sus competencias? ¿Ha contribuido con ello a los fines que la ley le asigna?

■[22] Sobre la competencia autonómica en materia de ficheros privados, cfr. Dictamen del Consell Consultiu sobre la Llei Orgànica 5/1992, del 29 d'octubre, de regulació del tractament automatitzat de les dades de caràcter personal, "Butlletí Oficial del Parlament de Catalunya", nº 69, 13 de enero de 1993 (en especial apartados 4 a 9 y conclusión). Cfr. asimismo, el texto del recurso de inconstitucionalidad presentado por el Gobierno de Cataluña contra la L.O. 5/1992, en el volumen "La protección de los datos personales. Regulación nacional e internacional de la seguridad informática", Barcelona, Centre d'Investigació de la Comunicació y Universitat Pompeu Fabra, 1993.

■[23] Por el momento, la Comunidad Autónoma de Madrid, mediante la ley 13/1995, de 21 de abril ("B.O.C.M." de 4 de mayo), ha creado ya un dispositivo orgánico específico, la Agencia de Protección de Datos de la Comunidad de Madrid, integrada por el Director y un Consejo de Protección de Datos como órgano consultivo (artículo 27). La ley 4/1992, de 17 de julio, de Policía del País Vasco ("B.O.P.V.-E.H.A.A." de 11 de agosto de 1992), artículos 12 a 15, atribuye a una Comisión del Parlamento Vasco el control del uso de los datos registrados en el centro de tratamiento de datos de la policía vasca.

Hay que admitir en términos generales que el uso de la competencia de la Agencia no ha sido equilibrado. La Agencia ha hecho escaso uso de algunas funciones y un uso excesivo e innecesario de otras. En buena parte, el escaso uso de algunas funciones obedece a dificultades derivadas de la concepción de la Agencia como administración independiente. Esta presunta "independencia" lleva consigo una situación de aislamiento que impide un adecuado flujo de información y un poder efectivo en algunos aspectos. La labor de la Agencia parece haber estado centrada en el afán de controlar o vigilar a los responsables de los ficheros, en conseguir una notificación total de los ficheros y en el ejercicio de la potestad sancionadora, y no tanto en orientar al afectado, en mediar entre el afectado y el responsable del fichero y promover un "estilo" de tratamiento de los datos de carácter personal en consonancia con los fines de la ley. Esta función es la que definen los artículos 36 e) de la ley y 4 del Estatuto. Este último menciona el recurso a las campañas de difusión mediante los medios de comunicación, pero sólo a título indicativo. El precepto comprende asimismo la información directa de los afectados. Por otra parte, los folletos y trípticos [24] editados por la Agencia, así como los fugaces *spots* televisivos no parecen haber causado un impacto satisfactorio.

33. La función de cooperación en la elaboración normativa, prevista en el artículo 36 h) de la ley y en el artículo 5, párrafo único, apartados a) y b), constituye una de las funciones primordiales que la ley encomienda a la Agencia. Por esta vía debía haberse ido extendiendo el sistema protector a todo el ámbito del ordenamiento jurídico, con las modulaciones que el contexto respectivo requiriera. La elaboración de las disposiciones legales y reglamentarias ofrece una ocasión de excepción para plantear la problemática de la protección de datos en el ámbito de la disposición respectiva. Sin embargo, no consta que esta función se haya ejercido en la medida deseable. Pese a que en las *Memorias* anuales de la Agencia se incluye una relación de informes sobre disposiciones (que no exceden de una treintena, por término medio, cada año), en el preámbulo de las aprobadas y publicadas no figura la mención del informe de la Agencia - si se exceptúa un escaso número, menor de cinco, que comprende solamente las promovidas desde el Ministerio de Justicia. Esta omisión indica que las disposiciones pertinentes no han sido informadas por la Agencia o que - menos probable - lo hayan sido y se haya olvidado mencionar el trámite de la consulta

■[24] Evita que la informática invada tu intimidad. La Agencia de Protección de Datos protege tus derechos contra los posibles abusos de la informática, Madrid, 1995.

en el preámbulo [25]. El estatuto jurídico de administración independiente y la consiguiente "soledad" del Ente y la ausencia de unos cauces regulares de información al respecto puede ser la causa de esta situación.

34. El ejercicio de las funciones definidas en el artículo 36 c) de la ley en el artículo 5, párrafo único, apartados c) y d), del Estatuto de la Agencia ha creado una cierta confusión, en la medida en que bajo la voz "Instrucción" se han cobijado meras resoluciones aplicativas, pero que en parte contienen normas reglamentarias. Estas "Instrucciones" [26] no pueden tener valor normativo de disposición reglamentaria, ya que la intención del legislador fue precisamente la contraria [27]. La confusión a que podría dar lugar el uso de la voz "instrucción" fue denunciada por el Grupo catalán del Congreso (enmienda 387), que propuso sustituir "instrucciones" por "recomendaciones". La enmienda no prosperó y el resultado fue incluir ambos términos, aumentando el riesgo de confusión. Si la Agencia no tiene potestad reglamentaria, lo que los preceptos citados definen ha de ser algo distinto. La única posibilidad de interpretar adecuadamente estos preceptos es la de que atribuyan a la Agencia una función de orientar a los responsables de los ficheros en cuanto a las medidas físicas y lógicas a adoptar para que los tratamientos se ajusten a la ley. La propia ley recoge esta idea en el artículo 4-6, según el cual los datos deben ser

■[25] Curiosamente, ha habido cierta resistencia por parte del Ministerio de Justicia a requerir el informe de la Agencia en estos casos. Cfr. Informe del Servicio Jurídico del Estado de 10 de febrero de 1995 (AG Varios, 30/94).

■[26] Instrucción 1/1995, de 1 de marzo, relativa a prestación de servicios de información sobre solvencia patrimonial y crédito ("B.O.E." de 4 de marzo); Instrucción 2/1995, de 4 de mayo, sobre medidas que garantizan la intimidad de los datos personales recabados como consecuencia de la contratación de un seguro de vida de forma conjunta con la contratación de un préstamo hipotecario o personal ("B.O.E." de 9 de marzo); Instrucción 1/1996, de 1 de marzo, sobre ficheros automatizados establecidos con la finalidad de controlar el acceso a los edificios ("B.O.E." de 12 de marzo); Instrucción 2/1996, de 1 de marzo, sobre ficheros automatizados establecidos con la finalidad de controlar el acceso a los casinos y salas de bingo ("B.O.E." de 12 de marzo).

■[27] En el curso de la tramitación del proyecto en el Congreso de los Diputados, varios Grupos parlamentarios presentaron sendas enmiendas que proponían la atribución de potestad reglamentaria a la Agencia: enmiendas 47, 85 y 127 (Grupos Mixto EE y EA e IU-IC); en el Senado, el Grupo Mixto (CDS e IU-IC) insistieron al respecto, con las enmiendas 22 y 76; todas estas enmiendas fueron rechazadas. En el Congreso, el partido mayoritario justificó la no aceptación por entender que era contradictorio que la Agencia fuera externa al Estado y a la vez tuviera potestad reglamentaria. A modo de transacción, se optó por la función consultiva del artículo 36 h).

almacenados de modo que permitan el ejercicio del derecho de acceso por los afectados. Los datos pueden ser almacenados físicamente y recuperados con arreglo a una lógica determinada, pero cabe que el almacenamiento y la recuperación se hagan *técnicamente* en formas diversas, algunas de las cuales podrían dificultar o impedir el acceso. Lo mismo cabría decir del resto de la ley. La Instrucción 1/1995 recomienda asimismo que la recogida de los datos relativos a la concesión de créditos hipotecarios o personales se haga mediante modelos separados para cada contrato a celebrar; esta medida "física" tiende, sin duda, a impedir la mezcla o cruce de datos de ficheros distintos. Las "Instrucciones" de la Agencia no se limitan, sin embargo, a estas orientaciones de índole informática, sino que van más allá y algunos preceptos contienen elementos normativos nuevos, como nuevos trámites, plazos, informes preceptivos, etc. En la medida en que añaden nuevos elementos normativos, estas Instrucciones (propiamente "resoluciones") son parcialmente nulas.

35. La cooperación internacional, que el artículo 36 l), proposición segunda, de la ley atribuye a la Agencia a título exclusivo, ha sido escasa. Se ha limitado a la participación en las tareas de la Conferencia de Autoridades Europeas de Protección de Datos (Bruselas, 1994; Madrid, 1994; Bruselas, 1995; Lisboa, 1995; Estocolmo, 1996, Madrid 1997) y a la asistencia a la Conferencia Mundial de Autoridades de Protección de Datos (La Haya, 1994; Copenhague, 1995; Ottawa, 1996). La Agencia ha estado ausente de la negociación de la Directiva 95/46/CE, así como de la propuesta de Directiva COD 288, sobre protección de datos en servicios de telecomunicación. Tampoco ha estado presente en los trabajos del Comité de Expertos de Protección de Datos del Consejo de Europa. La Agencia no ha participado en la negociación de los Convenios Europol, y del Sistema de Información Aduanero, ni en la del Sistema de Información Europeo. No se prevé, al parecer, cooperación alguna en la Comisión de Control Interno de los Ficheros de la O.I.P.C. (Interpol), prevista en el Acuerdo de Sede de 1982, pese a la activa participación que siempre han tenido otras autoridades de control en dicha Comisión, a través del presidente o del vicepresidente [28].

■[28] En 1993, el presidente de la Comisión era R. Biever, que lo había sido de la Comisión de Protección de Datos de Luxemburgo; el vicepresidente, P.J. Hustinx, presidente actual de la Registratiekamer de los Países Bajos; y entre los vocales Jacques Fauvet, presidente actual de la CNIL de Francia.

36. La función de publicidad registral de los ficheros, piedra angular del sistema protector, se complementa en la ley (artículo 36 j) y en el Estatuto (artículo 7), con una función de difusión pública de los ficheros inscritos, que la Agencia ha ejercido de forma singular. En 1995 se publicó el catálogo anual previsto en el citado artículo 7 del Estatuto[29]. En dicho catálogo sólo figuraban los nombres y direcciones de los responsables de los ficheros, pero no la identificación y fines de cada fichero. La publicación carecía de utilidad. En realidad, habría bastado, con respecto a los ficheros del sector público, con reproducir las disposiciones creadoras de ficheros publicadas en el B.O.E. y en los diarios oficiales de las Comunidades Autónomas[30] . En 1996 la Agencia difundió un disco *CD-rom* con la información prevista en los preceptos citados. Es dudoso que esta forma de publicidad, limitada al colectivo de las personas que dispongan de recursos informáticos suficientes, satisfaga las exigencias de la ley en cuanto a difusión de los ficheros inscritos.

37. El texto definitivo de la Directiva 95/46/CE ha modificado sustancialmente la concepción de la autoridad de control de la propuesta de 1990, en la cual se inspiró la L.O. 5/1992, de 29 de octubre. Ya no es preciso que la autoridad de control sea *independiente,* es decir, un órgano, organismo o ente separado, creado *ex professo* y externo a la estructura de la Administración, ni dotado de presupuesto propio, distinto del Estado. La memoria periódica de la autoridad de control no tiene que ser elevada al Parlamento, sino que solamente debe ser publicada. El artículo 28-1, párrafo segundo, dispone que las autoridades de control "*ejercerán las funciones que les son atribuidas con total independencia*".

38. Por otra parte, como se puso de manifiesto en el curso de la negociación de la Directiva, la opción de la administración independiente llevaba consigo el riesgo de la irresponsabilidad de la autoridad de control ante el Parlamento. Así lo denunció la delegación alemana, cuyas propuestas dieron lugar al texto definitivo del artículo 28-1, párrafo segundo. Este problema lo señaló asimismo el Consejo de Estado de España en el dictamen referente al proyecto de Estatuto de la Agencia de Protección de Datos [31]. Por otra parte, la independencia, entendida como "externalización" y

■[29] Ficheros automatizados de datos de carácter personal, Titularidad pública 1994-1995, Titularidad privada, 1994-1995, vols. I y II, Madrid, Boletín Oficial del Estado, 1995.

■[30] Así lo han hecho A.ORTI y sus colaboradores en la publicación Legislación de datos de carácter personal, Madrid, Tecnos, 1996, págs. 97 a 299

autonomía presupuestaria, es en realidad un inconveniente. Dejando aparte la necesidad de duplicar servicios logísticos que, de otro modo, quedarían absorbidos por los del departamento de adscripción o dependencia, con el consiguiente ahorro, la externalización da lugar a un aislamiento y a una "soledad" del órgano, que dificulta su gestión y lo priva de un poder efectivo. Ya hemos aludido a la ausencia de cauces formales de acceso a los proyectos de leyes y reglamentos y a su incidencia en el incumplimiento de la función de cooperación en la actividad normativa.

39. En el Derecho español no existe inconveniente para crear una autoridad de control que cumpla con las exigencias de la Directiva, sin necesidad del recurso a la opción de la administración independiente. A este respecto, no hay que olvidar que, según la constitución (artículo 103-1), la Administración "sirve con objetividad" los intereses generales y actúa "con sometimiento pleno a la ley y al Derecho" - no a la orientación política del momento. Por ello, es plenamente viable una autoridad administrativa que ejerza sus funciones con total independencia, como prescribe la Directiva. La reciente historia administrativa española ofrece un caso arquetípico de órgano de control del ejercicio de un derecho fundamental, inserto en la estructura del Ejecutivo, como es la Comisión Asesora de Libertad Religiosa, creada por el artículo 8 de la L.O. 7/1980 bajo la dependencia del Ministro de Justicia. El derecho a la libertad religiosa ha sido tradicionalmente fuente de graves conflictos y, sin embargo, el encuadramiento de dicha Comisión no parece haber creado dificultades especiales. El reciente Real Decreto 2458/1996, de 2 de diciembre, por el que se crea el Consejo para la Defensa del Contribuyente en la Secretaría de Estado de Hacienda, ofrece un modelo válido que cumple con las exigencias de la Directiva. El artículo 5-3 dispone lo siguiente: "*El Presidente del Consejo para la Defensa del Contribuyente actuará con independencia respecto de cualquier otro órgano administrativo y con total autonomía en cuanto a los criterios y directrices a aplicar en el ejercicio de sus funciones*". Esto significa que es posible un órgano de la Administración del Estado que ejerza su función con total independencia, sin sujeción a instrucciones.

40. La aplicación de la Directiva dará lugar a una disminución considerable del volumen de la gestión de la Agencia. En primer lugar, gran parte de los tratamientos no tendrán que ser notificados, ya que, en primer lugar, sólo deberán ser notificados los tratamientos "*que puedan afectar a los derechos y libertades de los interesados, habida cuenta de los datos a que se refiere el tratamiento*", a tenor de lo dispuesto en el artículo 18-2, primer guión, de la Directiva. Sólo los tratamientos que deban ser notificados

■[31] Dictamen 97/93, de 18 de febrero de 1993, págs. 15 y 16.

serán objeto de un examen previo por parte de la autoridad de control. En segundo lugar, a tenor de lo previsto en el artículo 20-3, incluso tales tratamientos podrán no ser notificados, siempre que por vía de disposición legal o reglamentaria, se compruebe que no afectan a los derechos y libertades de los interesados. Este sucedáneo de notificación se aplicará, tanto a los tratamientos del sector público, como a los del sector privado. Cabe que disposiciones legales o reglamentarias que regulen un sector determinado susceptible de aplicación de los tratamientos automatizados o manuales de datos personales, contengan una regulación circunstanciada del tratamiento. Por último, la notificación no será precisa si el responsable del tratamiento designa un Comisario de protección de datos, que asumirá el control del tratamiento y llevará un registro de los tratamientos. En caso de existir este Comisario, será esta institución y no la autoridad de control, quien juzgue si los tratamientos ofrecen riesgo para los derechos y libertades. A favor de la opción del Comisario existen ya precedentes en el Derecho español: por ejemplo, el mencionado Consejo de Defensa del Contribuyente, el Defensor del Asegurado[32], y otras figuras análogas, aun oficiosas, como los defensores de los clientes de los grandes Bancos.

VI. EL FLUJO INTERNACIONAL DE DATOS DE CARACTER PERSONAL

41. Los artículos 32 y 33 de la ley se ocupan de los problemas del tráfico internacional de los datos personales. Estos problemas tienen su raíz en la diversidad de soluciones que las distintas leyes nacionales ofrecen en cuanto a la protección de clases determinadas de datos (datos de salud, etc.) o a los datos usados en determinadas actividades (policía, publicidad, etc.). No todas las leyes protegen los mismos datos ni regulan las mismas modalidades de su uso, ni prevén un mismo nivel en punto a garantías del afectado (publicidad de los ficheros, excepciones al derecho de acceso, etc.). El Convenio 108 no creó una uniformidad a escala internacional, excepto en lo que respecta al "núcleo irreductible". Por el contrario, ofrece opciones diversas en cuanto a la aplicación del sistema protector a los ficheros manuales, a la inclusión de las personas jurídicas entre los sujetos beneficiarios de la protección, etc. El artículo 11 (recogiendo, a su vez, la norma del artículo 60 del Convenio Europeo de los

■32 Véase la ley 30/1995, de 8 de noviembre, de Ordenación y Supervisión de los Seguros Privados ("B.O.E." de 9 de noviembre), artículo 63. La generalidad de la dicción del texto de este artículo permite incluir entre las reclamaciones de los asegurados las referentes al tratamiento de sus datos de carácter personal.

Derechos Humanos de 1950) declara que sus disposiciones no deben interpretarse en el sentido de impedir a los Estados parte reconocer a sus súbditos una protección mayor que la que establece el Convenio. Esta diversidad puede dar lugar a un desequilibrio en la protección de los afectados en sus relaciones con personas de otros Estados. Un control riguroso de las cesiones o transferencias internacionales de datos constituiría un obstáculo a la libertad de información, derecho reconocido asimismo por el artículo 10 del citado Convenio Europeo de los Derechos Humanos de 1950. Por ello, el artículo 12 del Convenio 108 trató de llegar a un compromiso. Tras proclamar la libertad de circulación de los datos, prohibiendo a los Estados someter a autorización las cesiones internacionales, permite, sin embargo, a los Estados miembros someter la cesión a una autorización previa si, en general, o en relación con una clase determinada de datos, el Estado de destino no tiene una legislación protectora del mismo nivel que la del Estado de origen. El artículo 32 de la ley recoge esta norma del artículo 12 del Convenio 108 y prevé la posibilidad de una autorización del Director de la Agencia de Protección de Datos como condición de la cesión, salvo que se trate de datos transferidos en los supuestos del artículo 33: auxilio judicial, intercambio de datos de salud con fines de atención médica o estudios epidemiológicos, o transferencias dinerarias, según la legislación aplicable, y, en general, cuando la cesión resulte de la aplicación de convenios o tratados en los que España sea parte. Los artículos 3 y 4 del R.D. 1332/1994 han regulado el procedimiento. El artículo 1-6 de dicho Real Decreto ha incluido una definición específica, que acomoda la regulación al Convenio 108, en cuanto que incluye en la noción legal el transporte de datos por cualquier medio de transmisión, incluyendo el correo u otro medio convencional.

42. Con la Directiva comunitaria, este problema de la difusión transnacional de los datos ha adquirido una fisonomía distinta. Dentro del espacio comunitario la transferencia de datos de un Estado a otro no deberá ofrecer problema alguno, en la medida en que existirá una legislación uniforme o armonizada. La problemática de estas transferencias sólo se dará entre Estados de la Unión y Estados terceros cuya legislación pudiere ofrecer un "desnivel" en la protección de los datos. Sin embargo, la realidad es que, por el juego del artículo 5 de la Directiva, seguirán existiendo diferencias entre los Estados, en la medida en que unas legislaciones serán más rigurosas y otras más flexibles. Por otra parte, el régimen de la Directiva se basa en la noción de "tratamiento", en lugar de la de fichero. Gran parte de los tratamientos automatizados se desarrollarán en todo o en parte en más de un Estado. Habrá que determinar qué Derecho nacional deberá aplicarse a un tratamiento dado. La ley española, a diferencia de las de Bélgica, Reino Unido o Países Bajos, ignora totalmente el problema territorial. La ley de transposición deberá, por tanto, transponer el artículo

4 de la Directiva, que se ocupa de estos problemas. El artículo es confuso, como lo prueba el hecho de que el legislador comunitario haya creído necesario interpretarlo mediante un conjunto de varios "considerandos". La solución de la Directiva consiste, por una parte, en obviar la sumisión fraudulenta a un ordenamiento más favorable, y en procurar que haya un solo ordenamiento aplicable. Sin embargo, la Directiva admite la posibilidad de varios ordenamientos, si el responsable del tratamiento está establecido en varios Estados. En tal caso el responsable del tratamiento debe garantizar el cumplimiento de los distintos ordenamientos. El artículo 28-6 de la Directiva confiere a las autoridades de control una competencia "transterritorial" en la medida en que permite que las de otros Estados miembros "insten" a la respectiva autoridad a que ejerza su competencia dentro del territorio del Estado de ésta.

VII. EL SISTEMA SANCIONADOR

43. A diferencia de las demás leyes de protección de datos, la ley no ha tipificado unos delitos. La ley ha seguido la orientación que ha venido inspirando a este respecto las leyes administrativas promulgadas desde mediados de la década de los ochenta, fundada en el principio de "mínima intervención". En consecuencia, el dispositivo coercitivo de la ley no contiene unos tipos de delito, sino sólo de infracciones administrativas, en el artículo 43. Las infracciones se ajustan a un sistema paralelo a las normas de los artículos 4 a 7, 9, 11, y a las de los preceptos de los Títulos III y IV (en especial los artículos 18, y 24. El artículo 43 ofrece una cierta gradación, desde las infracciones que afecten a cuestiones meramente formales o documentales (infracciones leves, según la fórmula genérica del artículo 43-2 d), hasta las consistentes en tratar de forma automatizada los datos "con menosprecio de los principios y garantías que les sean de aplicación, cuando con ello se impida o se atente contra el ejercicio de los derechos fundamentales". El artículo 43 no ha recogido como infracción administrativa el supuesto que la ley francesa había definido como "desviación de finalidad" (*détournement de finalité*) en su artículo 44, delito penado con pena de privación de libertad y que fue integrado en el nuevo Código penal francés de 1992. Unicamente, en el artículo 43-3 b) se define un supuesto de infracción consistente en iniciar la recogida de datos de carácter personal para incluir en ficheros automatizados con finalidades distintas de las que constituyen el objeto legítimo de la empresa o entidad. No se menciona como parte del supuesto de hecho el uso ulterior de los datos recogidos.

44. Las sanciones del artículo 43 y las correspondientes previstas en el artículo 44 no agotan el dispositivo coercitivo de la ley. Los artículos 45 y 48 prevén un sistema

de medidas tendentes a la cesación de los tratamientos ilícitos de datos y a la inmovilización de los ficheros. La ley distingue dos sistemas coercitivos, según se trata de ficheros de titularidad pública o de titularidad privada. El sistema de sanciones de los artículos 43 y 44 sólo afecta a los titulares de ficheros privados. No tendría carácter disuasorio alguno imponer sanciones pecuniarias a un órgano de una Administración Pública, pues la sanción se resolvería en una adscripción o transferencia a favor del Tesoro, de parte de un crédito del presupuesto del órgano que incumpliera la ley. Por ello, el artículo 45 prevé un sistema más directo, consistente en ordenar la cesación de un tratamiento de datos que incumpla la ley y, en su caso, instar actuaciones disciplinarias contra el personal correspondiente. En cambio, la potestad de inmovilización de ficheros, que el artículo 48 atribuye al Director de la Agencia, afecta a cualesquiera ficheros. Hay que añadir las facultades que el artículo 41 atribuye al Director en los casos de infracciones cometidas por los órganos de las Comunidades Autónomas.

La Directiva no prescribe un tipo determinado de sanciones, penales o administrativas. Tampoco dispone que las sanciones previstas en el artículo 24 deban ser impuestas por la autoridad de control. El precepto deja a los Estados miembros en libertad en cuanto a la adopción de las "medidas adecuadas" para garantizar la plena aplicación de las disposiciones de la Directiva, y, en concreto, para determinar las sanciones a aplicar en caso de incumplimiento. Tales "medidas adecuadas" serán función del ordenamiento jurídico del Estado miembro. Por ello, podrán consistir en infracciones penales, infracciones administrativas, o incluso medidas cautelares en vía civil. El procedimiento sancionador es sólo una de las opciones posibles. En primer lugar, el Código penal de 1995 tipifica unos delitos específicos en el artículo 197. Estos delitos no cubren todos los supuestos de incumplimiento de las disposiciones de la Directiva. Por otra parte, el sistema sancionador de la ley no contempla a los infractores, sino sólo a los responsables. En la práctica, esto ofrece la incongruencia de que el sistema sólo es aplicable a los responsables de ficheros privados. Los responsables de ficheros públicos son "irresponsables", ya que la ley sólo prevé la responsabilidad disciplinaria. De acuerdo con la definición de "responsable del fichero" incluida en el artículo 3, sólo pueden serlo los titulares de órganos de designación política, que, como tales, no están incluidos en el régimen disciplinario. La responsabilidad se traslada así a los funcionarios, que como tales no deciden, sino que proponen y ejecutan. El "considerando" 55 de la Directiva 95/46/CE precisa a este respecto: "*... que deben imponerse sanciones a toda persona, tanto de derecho privado como de derecho público, que no respete las disposiciones nacionales adoptadas en aplicación de la presente Directiva*". El sistema sancionador deberá ser revisado a fondo con motivo de la transposición.

Una interesante opción al respecto es la que ha sido propuesta recientemente por el profesor FAIREN GUILLEN [33], consistente en instaurar un procedimiento judicial de naturaleza interdictal, basado en precedentes del Derecho histórico aragonés. Cabría regular este procedimiento en la nueva ley de transposición. El procedimiento interdictal tendría por objeto paralizar el tratamiento de los datos en determinados supuestos que habrían de definirse. La iniciativa podría ser del afectado o de la Agencia de Protección de Datos, ya que, según la Directiva (artículo 28-3, segundo guión) deberá disponer, imperativamente, de *potestad de intervención*, la cual se define *ad exemplum* en dicho precepto. Esta potestad podrá concretarse en "ordenar el bloqueo, la supresión o la destrucción de datos, o incluso prohibir, provisional o definitivamente, un tratamiento, o dirigir una advertencia o amonestación al responsable del tratamiento", o "someter la cuestión a los parlamentos o a otras instituciones públicas nacionales". Se trata de opciones definidas *ad exemplum*, por lo cual no es necesario utilizarlas todas. El procedimiento interdictal no sería otra cosa que una adaptación del de inmovilización de ficheros, previsto en el actual artículo 48, pero sería un procedimiento autónomo, no complementario del procedimiento sancionador, que como tal desaparecería. Tendría la ventaja de que también el afectado sería oído [34]. La iniciativa de la Agencia se ejercería al amparo de lo previsto en el artículo 28-3, cuyo tercer guión dispone que la autoridad de control deberá tener capacidad procesal. El ejercicio de esta iniciativa en el procedimiento interdictal se ajustaría plenamente a la función primordial de la autoridad de control, de auxiliar al afectado. La instauración de este procedimiento constituiría una "judicialización" del sistema coactivo y la exclusión de la Agencia de Protección de Datos del marco de la legislación de procedimiento administrativo, al menos en lo relativo al procedimiento sancionador.

El Código penal de 23 de noviembre de 1995 ha tipificado como delito de descubrimiento y revelación de secretos el hecho de "apoderarse, utilizar o modificar, en perjuicio de tercero datos reservados de carácter personal o familiar de otro que se hallen registrados en ficheros o soportes informáticos" (artículo 197-2). Asimismo, se

■ 33 FAIREN GUILLEN, V., El habeas data y su protección actual sugerida en la Ley Española de Informática de 29 de octubre de 1992 (interdictos, habeas corpus), "Revista Española de Derecho Procesal", Primera parte, 1996, págs. 523-557, Segunda parte, 1997, págs. 85-108.

■ 34 El profesor FAIREN GUILLEN (op. cit., Segunda parte, pág. 107) subraya la falta de participación del afectado en el procedimiento sancionador, en el que no tiene carácter de parte.

tipifican como sendas agravantes cualificadas la realización de tal hecho por los responsables de los ficheros (artículo 197-4), o el hecho de que los datos objeto del apoderamiento, uso o modificación ilícitos sean datos que "revelen la ideología, religión, creencias, salud, origen racial o vida sexual" (artículo 197-5).

El Documento Electrónico

JOSÉ MARÍA ALVAREZ-CIENFUEGOS SUÁREZ

Magistrado-Jefe del Gabinete Técnico del Presidente del Tribunal Supremo

IMPLICACIONES JURIDICAS DEL DOCUMENTO ELECTRÓNICO

El Presidente de la República francesa, al dirigirse a todos los ciudadanos el 20 de enero de 1997 para describir la situación de la Administración de Justicia, puso especial énfasis en la importancia de los medios informáticos para hacerla más rápida, más clara y más cercana a las necesidades de los ciudadanos. En concreto, consideraba imprescindible la introducción de nuevas tecnologías que permitan agilizar y simplificar los procedimientos judiciales.

Por su parte, la nueva Ministra de Justicia, Elisabeth Guigou, al tomar posesión de su cargo y fijar los objetivos prioritarios de su ministerio, señalaba entre sus prioridades la mejora del servicio público de la justicia, para lo cual insistía en la mejora y modernización de sus medios.

El anterior Ministro de Justicia francés Jacques Toubon, en el discurso pronunciado el 22 de marzo de 1997, en la Escuela Nacional de la Magistratura, sobre el futuro de la Cyberjusticia, ponía de relieve las dificultades que ofrece al mundo del derecho la regulación de un espacio desmaterializado, que no tiene ni centro ni periferia.

Fenómenos como Internet ofrecen, por lo que a la documentación jurídica se refiere, la posibilidad de acceder a numerosas bases de datos y enviar mensajes, por vía electrónica, a cualquier parte del mundo.

Se ha puesto fin a un concepto tradicional del Estado, el «Estado sedentario y territorial». El estado ha perdido la capacidad de controlar y poner fronteras a las relaciones entre los ciudadanos. Asistimos al nacimiento del denominado «territorio virtual».

El cyber-espacio surge como un mundo virtual y de cambio no localizable, como realidad material, responde a las palabras de Heráclito para quieto todo cambia.

El tiempo y el espacio, como realidades objetivas, han dejado de condicionar el fenómeno jurídico. El desafío de nuestros días, para evitar el Estado del caos que algunos anuncian con la llegada de Internet, hace necesaria la cooperación de todos los países para construir el «estado del cosmos».

La ordenación de las telecomunicaciones exige, como ha puesto de relieve la 0. C.D.E. una mayor cooperación técnica, jurídica, policial y judicial de los Estados. El cyber-espacio no es sólo una fuente de interrogaciones para la aplicación del derecho, es un entorno nuevo, técnico, cultural y social, afecta a la producción del derecho mismo.

El Ministro de Justicia francés recuerda como estas modernas herramientas pueden ayudar eficazmente a los Magistrados y funcionarios judiciales. En Francia el servidor instalado por el Ministerio de Justicia para informar a los ciudadanos ha ofrecido 23.000 conexiones en sólo dos semanas.

La teletransmisión de datos, lo que podríamos denominar el envío electrónico de documentos se ha convertido en una de las tareas prioritarias del Ministerio de Justicia francés, quien está comprometido con la construcción de toda una arquitectura de comunicaciones que sirva de base al sistema de información de la Justicia.

Se plantea, con carácter general, la desmaterialización de los escritos en el ámbito de la Administración de Justicia., estudiándose la creación del EDI judicial. El desarrollo de una informática judicial que permita a los tribunales comunicarse con todos los profesionales del derecho será una fuente de progreso y de ahorro de tiempo para los magistrados y funcionarios.

Entre estas necesidades que son predicables de la realidad española. Entiendo, se encuentran los medios informáticos al servicio de la Administración y el uso progresivo y generalizado de los sistemas de comunicaciones que permitan la implantación del documento electrónico.

La aparición y difusión de las nuevas tecnologías en la convivencia diaria de los ciudadanos hace que, en muchas ocasiones, los conceptos jurídicos tradicionales resulten poco idóneos para interpretar las nuevas realidades. Así, resulta que el jurista tradicional, formado en esquemas conceptuales no informáticos, encuentra verdaderas dificultades para adaptar la Ley y la jurisprudencia a los cambios tecnológicos.

Donde estos problemas son más intensos es en el campo de la prueba, deberemos acostumbrarnos, como ocurrió en su día en el derecho mercantil, a los nuevos usos informáticos.

Los medios informáticos se nos presentan como instrumentos idóneos para la generación de actos y negocios jurídicos en masa; facilitando el intercambio de documentos mediante sistemas de comunicación electrónica, sin embargo, nos ofrecen grandes dificultades para acreditar la validez y autenticidad de un documento elaborado electrónicamente.

En este sentido, pocas épocas de nuestra historia han soportado una disociación más radical entre los avances tecnológicos y su consecuente proyección sobre la convivencia social por una parte, y por otra, los conceptos jurídicos destinados a regularlos. Los Códigos Civiles y las leyes procesales, por lo que respecta a la prueba, siguen concibiendo sus preceptos pensando en el soporte tradicional, en el papel, la prueba documental, la prueba de peritos, por ejemplo, están pensadas para la escritura y la calificación tradicional.

Pongamos algunos ejemplos; mientras que en la vida diaria de nuestras ciudades un alto porcentaje -cada día mayor- de las transacciones económicas y comerciales se realizan por medios electrónicos, nuestros códigos civiles y nuestras leyes procesales desconocen la figura del negocio jurídico celebrado por medios informáticos y sus consecuencias jurídicas, fundamentalmente en el ámbito de la prueba.

Mientras que la dogmática tradicional ha elaborado durante siglos, el concepto de acto jurídico y las consecuencias que de él se derivan para la persona,

los juristas modernos encuentran serias dificultades para delimitar los efectos de una voluntad consecuente y libre proyectada sobre un programa informático.

La misma idea de documento, tradicionalmente unida a un soporte físico, como el papel o el cartón, encuentra dificultades para ser aplicada a los discos magnéticos y ópticos en los que, cada día con mayor intensidad, se almacenan los actos y negocios jurídicos.

Toda estas nuevas realidades nos ofrecen un panorama que, con acierto, la doctrina italiana ha calificado de nueva cultura informática.

Los juristas en general, y los jueces, los abogados y los profesores universitarios en particular, tienen que hacer un gran esfuerzo para adaptarse a estas nuevas realidades.

La informática asociada a la persona y a sus derechos, tanto personales como patrimoniales, se nos manifiesta como un fenómeno social de primera magnitud.

Ante el nacimiento de un mercado telemático europeo, acorde con el mercado único, el derecho y particularmente los juristas tendrán que conciliar, en los que a la circulación de datos se refiere, aspectos tan diversos como el respeto a la vida privada, el acceso a los sistemas de información, los intereses generales de los Estados, los derechos de autor, su fiscalidad, todo lo que, en síntesis, podríamos denominar estatuto jurídico europeo de los datos informatizados, su libre circulación y transmisión.

Surge así una nueva forma de entender ..la circulación jurídica», en el marco del espacio judicial europeo que supera las fronteras nacionales, y que cada da demanda una mayor uniformidad de la documentación judicial, paso imprescindible para hacer efectivo el espacio judicial europeo.

Esta situación viene favorecida por el desarrollo de los programas EDI (Electronic Data Interchange), mediante los cuales se permite la transferencia de ordenador en ordenador de mensajes «estructurados». El EDI ofrece una mayor seguridad, rapidez y eficacia en el intercambio de mensajes, mediante la oportuna codificación de los documentos. Así se ha acreditado en el sistema bancario (Sistema Swift); en la industria automovilística (Proyecto Odette); electrónica (proyecto Edifice); química (proyecto Cefic); del seguro (proyecto Rinet) y

transportes (proyecto Cost 306), entre otras. No es suficiente, con ser mucho, que existan redes, autopistas de la información, en el espacio jurídico europeo, es necesario y esto me parece fundamental desde el punto de vista de las Administraciones Públicas, estructurar y codificar los mensajes para que el intercambio de información sea efectivo, establecer unas normas generales para estandarizar la información jurídica y ofrecer controles que permitan otorgar fiabilidad a los mensajes.

En otro orden de cosas, la Comunidad Económica Europea, a través del programa TEDIS (Trade Electronic Data Interchange System), pretende armonizar las legislaciones de los Estados Miembros para facilitar el intercambio electrónico de documentos comerciales, siendo consecuente, por otra parte, de la necesidad de cambiar unos sistemas jurídicos que fundan sus medios de prueba, muy especialmente, sobre la escritura. Por lo que respecta a nuestro país, la reciente Reunión Plenaria de Actividades EDI en España, patrocinada por la CEOE, ha puesto de relieve la necesidad de intensificar la estandarización de los mensajes y la creación de un organismo de Certificación Nacional Electrónica.

Hoy día, puede decirse que ante la carencia de una regulación normativa adecuada, los empresarios europeos han asumido voluntariamente el valor probatorio de las transferencias y los negocios jurídicos concertados por medio del EDI. En nuestros días la ..factura electrónica» es una realidad obtenida a nivel comunitario. Es deseable, por tanto, una regulación comunitaria en la materia. Sin embargo, mientras llega esta normativa opino que, las instituciones nacionales con responsabilidades en materia de justicia, deben comenzar a celebrar convenios que les permitan utilizar entre sí, con plena eficacia jurídica, este tipo de medios de comunicación electrónica. No está lejano el día en que los Juzgados y Tribunales europeos estén unidos por redes telemáticas e informáticas para intercambiar documentos e información.

ALGUNOS EJEMPLOS:

Llama la atención el tremendo contraste entre la masiva aplicación de los sistemas electrónicos en la contratación empresarial y la carencia de normas para regular la prueba de estas operaciones.

Ya anticipo mi opinión, el Derecho y el trabajo de los juristas es, con frecuencia, una vuelta a los principios, en este caso, debemos recordar como se

generalizó la validez y eficacia de instrumentos de pago como la letra de cambio, los pagarés y los cheques.

Donde la innovación tecnológica, representada por los sistemas informáticos, ha encontrado una rápida y eficaz aplicación dentro del sector público ha sido en los mercados modernos de compraventa de títulos valores que hoy día están implantados en todo el mundo.

En España, el Real Decreto 505/1.987, de 3 de abril, creador del sistema de anotaciones en cuenta para la deuda del Estado, puso de relieve como el título valor, tal y como ha venido siendo concebido, supone un obstáculo para el tráfico mercantil, condicionado por la rapidez y la masificación de las operaciones.

Así, la propia exposición de motivos reconoce como la rapidez en el tratamiento de la información, la posibilidad de incorporar mecanismos que eviten o subsanen los errores cometidos, así como las facilidades de interconexión permiten el intercambio, a distancia, de cientos de miles de datos. Hoy día, el tratamiento informático permite la sustitución del viejo soporte documental del titulo valor tradicional, por simples referencias procesables en los ordenadores.

Por su parte, el nuevo Texto Refundido de la Ley General Presupuestaria, de 23 de Septiembre de 1. 988, establece, ya con carácter general y con el adecuado rango normativo, que: ..La Deuda Pública podrá estar representada en anotaciones en cuenta, títulos-valores o cualquier otro documento que formalmente la reconozca».

Surge así la Central de Anotaciones en el Banco de España en la que se toma constancia, mediante la oportuna anotación en cuenta, de las transacciones efectuadas con la deuda del Estado. La Central de Anotaciones, auténtico servicio público del Estado, junto con las Entidades Gestoras, titulares de cuentas, se convierten en protagonistas de un nuevo sistema que ha revolucionado el mercado de la deuda pública, al modificar sustancialmente el concepto de titulo valor en su dimensión material.

Dicho resguardo, importante cuestión (reflejo de la incidencia tecnológica en el derecho), debe codificarse de manera que se garantice la correspondencia con los registros de la Entidad y con la información comunicada a la Central de Anotaciones.

La Ley reguladora del Mercado de Valores, Ley de 28 de julio de 1. 988, crea un mercado único e integrado mediante una interconexión informática que permita la inmediata compensación y liquidación de valores.

Su artículo 5, permite que los valores negociables puedan representarse por medio de anotaciones en cuenta o por medio de títulos tradicionales. Se potencia así la rapidez, la fiabilidad y el control de la información, la cual se convierte en un bien jurídico de primer orden en nuestra sociedad.

Los negocios jurídicos sobre valores representados por medio de anotaciones en cuenta tendrán lugar mediante transferencias contables, produciendo la inscripción de la transmisión a favor del adquirente (art. 9), los mismos efectos que la tradición de los títulos, siendo oponible a terceros.

Para la gestión de todo este nuevo mercado la ley prevé la constitución de una red informática, columna vertebral de un sistema de interconexión bursátil de ámbito estatal. Dicho sistema aparece administrado por una sociedad denominada Servicio de Compensación y Liquidación de Valores.

El Real Decreto 291/1.992, de 27deMarzo (R. 1.992, 784), sobre emisiones y ofertas públicas de venta de valores, ha asignado a la Comisión Nacional del Mercado de Valores, por su disposición adicional quinta 1, el desempeño de las funciones en materia de codificación de valores negociables, configurándola como única entidad competente en esta materia.

En concreto, mediante la Circular 8 de Octubre de 1.992 se establece que la asignación por la Comisión Nacional del Mercado de Valores de los códigos correspondientes se contrae exclusivamente a los fines identificadores y de normalización operativa que inspiran la función de codificación, sin que la asignación de esos atributos alfanuméricos por la Comisión Nacional del Mercado de Valores suponga pronunciamiento alguno sobre la regularidad del instrumento codificado, en lo que toca a su naturaleza, mecanismo de circulación, o legalidad de su emisión, en aquellos otros planos de verificación y registro que dicho Organismo tiene encomendados por la Ley 24/1 . 988, de 28 de Julio del Mercado de Valores.

La transformación de los métodos operativos en el sector público y privado es ya irreversible. La reciente circular 13/1992, de 26 de junio, publicada en el B.O.E. de 11 de Julio de 1.992, da un paso, a nuestro juicio definitivo, en la

consolidación del Sistema Nacional de Compensación Electrónica: la circular 1/1.990, de 2 de Febrero, establecía como sistema de comunicación para la liquidación del sistema general de cheques y pagarés de cuenta corriente el telefax y el fax.

Una forma eficaz de facilitar la futura prueba requiere, a mi juicio, intensificar los controles y requisitos en el acceso a la circulación electrónica, ofrecer garantías, dar seguridad inicial a los sistemas. Como ejemplo, estos últimos días la prensa de Madrid anunciaba que la Bolsa, en una sola sesión, había realizado más transacciones que en todo el año 1983. Yo diría que la futura prueba se facilita con la credibilidad de los sistemas.

Pues bien, a partir de esta nueva Circular las comunicaciones entre las Entidades asociadas y el servicio de liquidación del Banco de España, se efectuará, como sistema ordinario, a través de un proceso automatizado que permitirá el diálogo directo entre el Centro de Procesos del Banco de España y los Centros de las Entidades participantes en el Sistema Nacional de Liquidación.

De esta forma, la constatación de las liquidaciones interbancarias se incorpora totalmente a sistemas informatizados. La prueba misma del incumplimiento de una obligación derivada de una relación jurídica mercantil, concertada por los medios tradicionales, se condiciona a la existencia de un diálogo electrónico entre una Entidad Bancaria asociada y el Centro de Procesos del Banco de España, en donde, con plena eficacia solutoria, quedan anotadas informáticamente miles de operaciones cada día.

La creación de centros oficiales y privados que controlen la circulación electrónica, el nacimiento de notarias electrónicas, facilitará la credibilidad de las condiciones en que se desarrolla el envió de los mensajes. Ante la falta de la percepción material del mensaje mismo, debe reforzarse el control sobre los sistemas de transmisión y recepción.

Este fenómeno que, sin duda, constituye un paso decisivo en la consolidación de los medios electrónicos de prueba, culmina con una declaración impensable hace solo unos pocos años: A partir de ahora, el fax y los terminales telex, último reducto en el que aparecía el papel como soporte físico de la liquidación de una obligación, solo podrán ser utilizados, con carácter extraordinario, cuando el Centro de Procesos de Datos del Banco de España o de

alguna de las Entidades asociadas no puedan utilizar el sistema ordinario que es, ya, desde hoy, la comunicación electrónica.

Como fruto de esta progresión conceptual en el reconocimiento y circulación de los documentos elaborados por medios electrónicos, la circular de 8 de Octubre de 1.992 de la Comisión Nacional de Valores, establece un sistema de Codificación de los valores negociables (acciones de Sociedades Anónimas, obligaciones, participación en fondos de inversión, pagarés, etc.), con objeto de normalizar su operatividad en un mercado dominado por las transacciones electrónicas.

Advirtiéndose, sin embargo, por la circular que la asignación de esos atributos alfanuméricos, no supone pronunciamiento alguno sobre la regularidad del instrumento codificado, en lo que toca a su naturaleza, mecanismo de circulación o legalidad de su emisión. En este sentido, la aprobación de nuevas Directivas comunitarias, encaminadas a liberalizar y hacer más flexibles los mercados financieros europeos, va a obligar a nuevas reformas legislativas encaminadas a permitir la intervención en los mercados españoles de agentes financieros de otros países comunitarios. Todo ello conllevará, como no puede ser menos, un nuevo esfuerzo de codificación e identificación electrónica en un mercado de valores cada vez más dependiente de la tecnología.

A mi juicio, un mayor control de los mecanismos de creación e introducción de los mensajes en el sistema electrónico, permitirá una mayor flexibilidad y agilidad de las operaciones. En mi opinión, se puede garantizar, ante todo, el sistema, en si, más que la transmisión individual, en su pura singularidad.

La documentación y posterior circulación de los actos jurídicos por sistemas informáticos ha penetrado con fuerza en núcleos esenciales del ordenamiento jurídico privado. En concreto, el derecho notarial y los registros de la Propiedad se ven favorecidos por los sistemas informáticos. Así, la Reforma del Reglamento Notarial, operada por el Real Decreto 1368/1992, de 13 de Noviembre de 1.992, ha previsto (véase el articulo 4 del Anexo al citado Reglamento), que el Registro General de Actos de Ultima Voluntad se lleve por procedimientos informáticos.

En consecuencia, la información que los Colegios Notariales deben remitir periódicamente al Registro General se enviará en soportes informáticos,

para, en su momento, dar paso al sistema de comunicación telemática (Orden del Ministerio de Justicia de 4 de Diciembre de 1.992).

En desarrollo de esta normativa, la Dirección General de Registros y Notariado, por resolución -Circular de 31 de Marzo de 1. 993, ha aprobado las instrucciones necesarias para el envío de los partes testamentarios y los partes de iniciación de las actas notariales de declaración de herederos ab-intestato.

Con ello, al utilizarse el soporte informático, se sustituye el tradicional envío de la información mediante tarjetas escritas.

Se establecen reglas de elaboración de la información para facilitar su tratamiento informático: se configura el número de identificación del Notario o Fedatario autorizante como el elemento básico para el sistema informático y, a la vez, se fijan las características de los soportes magnéticos y del sistema operativo, dándose instrucciones precisas respecto a la forma en que han de estructurarse los datos. Todo ello en garantía de la perfecta compatibilidad y comunicación de los sistemas informáticos.

Siguiendo la línea de informatización progresiva de los registros y las Notarías, asistimos a una nueva reforma de los Reglamentos Notarial e Hipotecario, originada por el Real Decreto 2.537/1994, de 29 de Diciembre.

El nuevo articulo 175 del Reglamento Notarial impone al notario que antes de autorizar una escritura de adquisición de bienes inmuebles o de constitución de un derecho real sobre ellos, deberá solicitar al Registro de la Propiedad correspondiente la información adecuada, pudiendo utilizarse para ello el telefax. Se impone, ya con plena vigencia la interconexión electrónica entre los Notarios y el registro de la Propiedad.

Asimismo, el nuevo artículo 249 del citado Reglamento autoriza al Notario para remitir por telefax al registro de la Propiedad la comunicación relativa a la autorización de escritura susceptible de ser inscrita, que dará lugar al correspondiente asiento de presentación.

Por su parte, el nuevo artículo 354 del Reglamento Hipotecario permite al registrador remitir su información respecto a la titularidad, cargas, gravámenes y limitaciones de fincas registrales, cuando sean solicitadas por las Notarías, por medio de telefax.

La Disposición Adicional Unica del Real Decreto de 29 de diciembre de 1994 impone, a nuestro juicio una obligación de excepcional transcendencia: en el plazo de un año, la obligación de informatizar el Diario de todos los Registros de la Propiedad de España.

La reciente Instrucción de 29 de octubre de 1996, de la Dirección General de los Registros y del Notariado prevé la intercomunicación entre todos los Registros de la Propiedad, permitiendo que la publicidad registral se desarrolle a través de sistemas informáticos, como parece reconocer el art. 12 del nuevo Reglamento del registro Mercantil, aprobado el 19 de julio de 1996. En el art. 23 del citado Reglamento se establece que los libros del Registro de la Propiedad puedan elaborarse por medios informáticos. La Instrucción de 1.996 requiere que el 3I de diciembre de 1.988 estén incorporados a los índices informatizados de los registradores todos los datos necesarios de las fincas con asientos posteriores a 1. 950.

El art. 10 reconoce, igualmente, que los registros de la Propiedad puedan comunicarse directamente por vía telemática, utilizando el correo electrónico para recibir información de las fincas registradas.

Por último y por lo que se refiere a los órganos judiciales, éstos podrán enviar por telefax al registro de la Propiedad competente, las resoluciones judiciales que puedan causar asiento registral, el da de su firma o en el siguiente hábil.

Recientemente, como ya hemos visto, se han producido en nuestro ordenamiento jurídico privado reformas de especial significación; nos estamos refiriendo a la modificación operada en la configuración material y organización de los Registros de la Propiedad: el Real Decreto de 30 de Marzo de 1.990 modifica el Reglamento Hipotecario de cara a una informatización integral de los registros de la Propiedad.

En este sentido, la reforma prevé la creación de un Indice General Informatizado de las fincas y derechos inscritos, para lo cual, el Colegio Nacional de Registradores de la Propiedad remitirá periódicamente al Centro de Gestión Catastral y Cooperación Tributaria, en soportes magnéticos, la información relativa a las transmisiones inscritas (art. 398.c).

Por su parte, el ya citado art. 418.b permite utilizar la telescopia o procedimiento similar para remitir al registro competente los datos necesarios para efectuar el oportuno asiento de presentación.

Esta decidida apuesta por la informatización de los Registros Públicos, en la que se consuma un cambio radical en la concepción del documento público, en lo que a su dimensión material y formal se refiere, ha continuado en los últimos días. Así, la Orden Ministerial de 10 de junio de 1997, por la que se desarrolla el ya citado Reglamento del registro Mercantil, respecto de la inscripción de las entidades, de cualquier naturaleza jurídica, que se dediquen al comercio mayorista o minorista o presten servicios de intermediación, cuando sus operaciones excedan de cien millones de pesetas. Precisa, entre otros extremos, en su Disposición final primera que la Dirección General de los Registros facilitará la intercomunicación con la Administración del Estado y de las Comunidades Autónomas, para facilitar el intercambio de información.

Los Registradores de la Propiedad, en la recepción de solicitudes y en la expedición de información registral por medios telemáticos o en soporte magnético deberán asegurar, en todo caso, la integridad, la conservación y no manipulación de sus bases de datos y archivos, debiendo utilizar el correo electrónico o el soporte magnético, con cumplimiento de las normas de protección de datos de carácter personal evitando la publicidad en masa y la creación de registros paralelos.

Se reconoce, pues, el acceso al Registro de información referida a entidades que se dediquen al comercio mayorista o minorista, utilizando medios telemáticos, luego la realidad documental que subyace en dichos medios de transmisión aparece unida a un medio de comunicación: el correo electrónico o el soporte magnético.

El respeto a la protección de los datos lleva consigo el reconocimiento de la realidad documental que subyace en los archivos de una manera implícita.

Las garantías que ofrece la realidad registral, cualquiera que sea la forma en que se conserve la información, incluidos los soportes informáticos, deberá asegurar la integridad, conservación y no manipulación del contenido de sus archivos y bases de datos.

Es frecuente en la terminología registral, lo que a mi juicio es tremendamente revelador de los cambios operados en los conceptos jurídicos, que se asocie en la manifestación del concepto, las expresiones «archivos» y «bases de datos".

Esta nueva forma de entender el funcionamiento de los registros públicos justifique el que, con acierto, se trate de evitar, tratándose de registros magnéticos, la publicidad en masa y la creación de registros paralelos.

Por último, la Disposición final 3a de la Orden de 10 de Junio de 1.997, en su apartado 2 °, precisa que los Registradores Mercantiles Provinciales estarán intercomunicados a efectos de la expedición de la publicidad formal por nota simple informativa, debiendo hacer constar en ella el valor jurídico de la información y la referencia a sus archivos, una vez examinado el contenido de los asientos registrales que, como hemos dicho, podrán estar constituidos por soportes informáticos.

Estos principios, a mi juicio de gran alcance, van a permitir que cualquier interesado pueda solicitar información del Registro Mercantil que libremente elija, y éste, con referencia expresa a aquél que expide la nota simple informativa, la entregará al solicitante sellada con el sello oficial.

Esta intercomunicación y ese fácil acceso a la información nos puede hacer pensar, por analogía con otras situaciones ya experimentadas, en el «Registro virtual» en el que, como es fácil deducir, el territorio, el espacio físico, como delimitación rigurosa del ámbito competencial, cobra una dimensión muy diferente a la hasta ahora conocida.

En este orden de cosas, la Instrucción de 29 de octubre de 1996, de la Dirección General de los registros y del Notariado, fija criterios para generalizar la publicidad registral por medio de sistemas informáticos.

Como expresión de esta decidida apuesta, no imitada, de momento, con el mismo entusiasmo por la Administración de Justicia pese a contar con una normativa ciertamente ambiciosa en la materia, el preámbulo de la Instrucción pone el énfasis en los progresos en la tecnología de las comunicaciones, asociándolos con la importancia misma de la publicidad registral, lo cual impone la obligación de utilizar todos los avances técnicos en orden a la información que

pueden prestar tanto el Servicio de Indices como los Registradores de la Propiedad y Mercantiles.

Se reconoce plenamente la posibilidad de la dación de fe pública por vía informatizada, de acuerdo con los datos básicos del Archivo contenidos en los índices. Se trata, en consecuencia, de facilitar el ejercicio de la función pública que tienen encomendada los Registradores, mediante el uso de las nuevas vías de actuación que permiten los avances tecnológicos, todo ello en beneficio jurídico y económico de los ciudadanos.

Se impone como obligación, antes del 31 de diciembre de 1998, la incorporación a los Indices informatizados de los registros todos los datos necesarios de las fincas con asientos posteriores a 1950, recogiendo, entre otros datos, los siguientes: Identificación de los datos registrales, identificación de la finca, identificación planiomética, referencia catastral, identidad del titular y carácter de su titularidad, naturaleza del derecho, cargas y limitaciones.

Para facilitar esta significativa tarea se prevé, con enorme acierto, la homologación de los programas por el respectivo Colegio.

Se fija, también, como fecha limite para la centralización por vía informática de la situación de incapacitación de los titulares de fincas, el 31 de diciembre de 1997.

Este encomiable proyecto de informatización de los Índices de los registros de la Propiedad se completa con el deseo de ofrecer esta información a las Administraciones Públicas, lo cual se realizará a través de los Servicios Centrales o de las terminales que puedan establecerse en las Presidencias Territoriales del Colegio de registradores.

Para garantía de todo este nuevo sistema que constituye, sin duda, una modificación sustancial en el modo de concebir y administrar la información registral, se permite, en el art. 10, a los registradores de la Propiedad y Mercantiles, comunicarse con el Registro de índices directamente, por vía telemática, para la obtención de la información del contenido de la base de datos de dicho Servicio, dejando constancia de la identidad del solicitante y del motivo de la solicitud.

El establecimiento de una red de comunicaciones entre todos los registradores permitirá, la remisión de notas simples a través del correo electrónico. De esta manera, los registradores podrán apreciar el interés en la solicitud de información con archivo de la identidad del solicitante, remitiéndola al Registrador que deba proporcionarla, una vez apreciada su competencia territorial y una vez calificados los asientos del registro, enviando la información al remitente, en el plazo más breve posible, para lo cual podrá utilizar los medios telemáticos descritos.

Como última garantía, se prohibe, a efectos de publicidad e información, el acceso directo, por cualquier medio, físico o telemático, a los Archivos de los Registradores de la Propiedad y Mercantiles, quienes vendrán obligados a responder de su custodia, integridad y conservación.

Se completa con ello, tanto en su dimensión formal como material, una nueva forma de entender la comunicación y circulación de la información jurídica, reconociéndose, con claro beneficio para los ciudadanos, la plena validez documental de estos nuevos soportes asociados a las posibilidades que ofrece, hoy día, la nueva tecnología.

En el campo del derecho público, la Ley de régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, Ley 30/92, de 26 de noviembre, ha reconocido plenamente respecto de los actos de la Administración, su posibilidad de manifestarse y documentarse por medios informáticos, teniendo, a todos los efectos, valor probatorio.

El nuevo artículo 230 de la Ley Orgánica del Poder Judicial, además de reconocer la validez de los documentos emitidos por medios electrónicos, informáticos y telemáticos, siempre que se garantice su autenticidad e integridad, permite en su apartado n° 4 que las personas que demanden la tutela judicial de sus derechos e intereses puedan relacionarse con la Administración de Justicia a través de dichos medios técnicos, siempre que éstos sean compatibles con los equipos de que dispongan los Juzgados y Tribunales.

Recientemente el Ministerio de Justicia ha aprobado una Orden Ministerial (30 de noviembre de 199S, B.O.E. de 2I de diciembre) por la que dispone la informatización del Registro Civil de Murcia.

Y, más recientemente, la Orden de 22 de Marzo de 1.996, por la que se desarrolla el artículo 88 de la Ley 37/1.992, del Impuesto sobre el Valor Añadido y el artículo 9 bis del Decreto 2. 402/1. 985, de 18 de Diciembre, desarrollan el sistema de facturación telemática en el Impuesto del Valor Añadido. A partir de ahora, las facturas en soporte papel son sustituidos por facturas electrónicas que deberán conservarse en soportes magnéticos u ópticos.

Así se define la factura electrónica: Se entenderá por factura electrónica ..un conjunto de registros lógicos, almacenados en soportes susceptibles de ser leídos por equipos electrónicos de procesamiento de datos, que documentan las operaciones empresariales o profesionales, con los requisitos exigidos en el Real Decreto 2. 402/1. 985, de 18 de Diciembre. En las líneas de las facturas electrónicas, que en todo caso deberán respetar los mencionados requisitos, podrán sustituirse las descripciones de los bienes o servicios que constituyan el objeto de las operaciones facturadas por sus correspondientes códigos estables.

Se entiende por códigos estables aquellos códigos alfanuméricos que identifican de forma única e inequívoca, entre otros, los bienes, servicios, lugares, personas, etcétera, cuya información se transmite a través de un sistema de intercambio de facturación por medios telemáticos y que tienen un carácter de permanencia en su aplicación, y con idéntico significado para cualquier usuario del sistema. Las listas de códigos estables y la descripción de los mismos deberán constar en tablas históricas que puedan ser utilizadas automáticamente por los programas de los usuarios para el tratamiento de los ficheros producidos».

Surge así una nueva metodología en el tratamiento de los fenómenos jurídicos, la transmisión electrónica de declaraciones de voluntad que generan derechos y obligaciones para los participes en el «diálogo informático" está provocando un cambio terminológico, a mi juicio inevitable, en los conceptos jurídicos tradicionales. ¿ Cómo interpretar, hoy día, nuestro Código Civil cuando impone al vendedor la obligación de «entregar la cosa al comprador».

Por último la Disposición Adicional de la citada Orden establece que: ..Los empresarios, profesionales o sus agrupaciones que lleven por medios informáticos sus libros, facturación o registros fiscalmente exigibles, deberán conservar en soporte magnético u óptico, durante el período de prescripción, además, los ficheros y documentos siguientes:

a) Ficheros de datos, tanto históricos, como maestros generados por sus aplicaciones informáticas y de los que se deriven los libros a diligenciar.

b) Ficheros de los programas fuentes, con los cuales se procesan los ficheros de datos anteriores.

c) Todos aquellos ficheros, programas y documentación necesarios que permitan la reconstrucción total del camino de auditoría informática del sistema de información del contribuyente u obligado tributario».

Es de resaltar, por lo que afecta a la realidad jurídica de nuestro país, la voluntad decidida de las Instituciones Comunitarias de superar los obstáculos que suponen las lagunas existentes en la normalización de los mensajes, la interoperatividad de las redes telemáticas, la validez jurídica y la seguridad informática de la información transmitida por medios electrónicos.

Estamos asistiendo, quiérase o no, al ocaso de la civilización del papel, de la firma manuscrita y del monopolio de la escritura sobre la realidad documental. Aparece, cada día con más fuerza, una nueva forma de concertar y garantizar la identidad de la voluntad generadora de los negocios jurídicos, reveladora de una nueva concepción del documento jurídico, asistimos, en muchos casos sin prestarle la necesaria atención, al nacimiento de nuevas formas de documentar los actos y negocios jurídicos.

El análisis de la realidad que acabamos de describir nos permite afirmar que el proceso informático, por el que se crean modifican y extinguen relaciones jurídicas, es un proceso «creíble y probable». El jurista no puede desconocer la realidad social, en palabras del profesor Hernández Gil, el derecho, como el lenguaje, es un producto de la cultura y un sistema de comunicación entre los seres humanos.

La Comunidad, con exquisita sensibilidad hacia los avances tecnológicos, ha insistido en las últimas reuniones del Consejo Europeo (reunión de 1.989 en Estrasburgo y de 1. 990 en Dublín) en la necesidad de abordar la creación de redes transeuropeas de datos comerciales e industriales.

En concreto, durante los años 1.988 y 1.989 se han desarrollado programas de Intercambio Electrónico de Datos en sectores tan importantes

como: la fabricación de automóviles, la industria química, la industria electrónica e informática, los reaseguros y los transportes, de los que, sin duda, habrán tenido ustedes abundante información durante estos días.

No se nos ocultan los problemas jurídicos que entraña este diálogo «sin papel»; es necesario, por tanto, superar los obstáculos legales que exigen la presentación del soporte escrito para dar por válida una obligación. La desaparición física de documentos básicos para el derecho mercantil, tales como los conocimientos de embarque, las cartas de crédito y el nacimiento de «notarías electrónicas» plantean problemas jurídicos de gran alcance que no se pueden ignorar.

La seguridad e integridad de los mensajes cursados por medios electrónicos ofrecen, no puede ocultarse, dificultades operativas en lo que respecta a la recepción y confidencialidad del mensaje.

Sin embargo, todo este panorama no es sólo un ..futurible» deseado, se trata más bien de una realidad inminente que se nos aproxima impulsada por la voluntad decidida de las autoridades comunitarias. La lectura de los documentos y trabajos de las Comisiones comunitarias vaticinan la llegada de un día, no muy lejano, en que, como presupuesto necesario para operar comercialmente en el marco de la comunidad, se nos impongan cambios normativos en nuestro ordenamiento que, hoy por hoy, nos parecen impensables.

Como pone de relieve la doctrina mayoritaria la Comunidad Económica Europea ha potenciado el desarrollo de la transmisión electrónica de datos (programas EDI), facilitando la celebración de contratos tipo entre pequeñas y medianas empresas con el consiguiente logro de una normalización y homogeneización de los documentos a transmitir.

Los usuarios del EDI, a través de acuerdos y convenios particulares, llegan a aceptar el valor probatorio de los mensajes enviados por sistemas electrónicos, dándose al mensaje electrónico normalizado el mismo valor que al documento escrito y firmado.

Nos encontramos, por tanto, ante un auténtico sistema internacional de circulación electrónica de valores que ha sabido salvaguardar las características más esenciales que la legislación mercantil asigna a los títulos valores.

Esta nueva expresión simbólica que permite la circulación electrónica de los valores mercantiles, a la vez que provoca el abandono de la «materialidad» de los títulos valores, paradójicamente, les vuelve a dotar de una nueva forma de significación: la informática. El ordenador y los ficheros que en él se almacenan constituyen hoy día una nueva forma de entender la materialidad de los valores. Para el lenguaje electrónico la «dimensión formal de los valores» es tan evidente, bajo su lectura codificada, como hace cien años para un banquero tradicional lo era el depósito de las acciones.

I.- REFORMAS LEGISLATIVAS QUE FACILITAN LA UTILIZACIÓN DEL SISTEMA EDI EN LA ADMINISTRACIÓN.

Recientemente, se ha aprobado en España una Ley que pone de manifiesto la preocupación de la Administración Pública por modernizar sus métodos operativos, incorporando al texto soluciones avaladas por los cambios tecnológicos que, hace pocos años, resultarían impensables.

Nos estamos refiriendo a la Ley de régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común. Esta importante norma destinada inicialmente a regular la actividad de todas las Administraciones Públicas, en virtud de lo dispuesto en el art. 149. 1, 18° de la Constitución, se dirige a la Administración General del Estado, a las Comunidades Autónomas, a las Entidades que integran la Administración Local y a las entidades que componen o forman parte de la Administración Institucional.

El punto S de la Exposición de Motivos de la Ley, al hablar de la mecanización y automatización de los procedimientos administrativos, califica, con cierta audacia legislativa a la informatización como el soporte y tejido nervioso de las relaciones sociales y económicas de nuestra época. Y, a ello añade que 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.

La nueva realidad de los métodos operativos de las Administraciones Públicas, tal y como venimos exponiendo, se reflejan en diversos artículos de la Ley, de los que, a título de ejemplo, sólo citaremos uno:

El artículo 45, Entre otros, incorpora dos novedades dignas de mención; por una parte, permite que los procedimientos administrativos se tramiten y terminen en soporte informático; por otra, se da validez a los documentos emitidos por medios electrónicos, informáticos o telemáticos, siempre que quede garantizada su autenticidad, integridad y conservación y, en su caso, la recepción por el interesado.

Por lo que respecta a las formas tradicionales de relacionarse con las Administraciones Públicas españolas, la Ley comentada introduce una novedad de gran transcendencia práctica: el artículo 45.3 permite a los ciudadanos relacionarse con las Administraciones Públicas utilizando técnicas y medios electrónicos, informativos o telemáticos, lo cual implícitamente, viene a reconocer la validez y adaptación del EDI en la práctica administrativa española. Recientemente, el Real Decreto 263/1.996, de 16 de Febrero, regula la utilización de técnicas electrónicas, informáticas y telemáticas por la Administración General del Estado, ampliando el marco establecido por la Ley 30/1. 992, de 26 de Noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.

Estas posibilidades ya son una realidad práctica y operativa en determinados sectores de la Administración Pública, especialmente en el campo de la Administración Tributaria y en el campo de la gestión de la Seguridad Social en la que se permite la comunicación entre empresarios y las entidades gestoras a través de sistemas electrónicos.

En desarrollo de las posibilidades que ofrece el art. 45 de la Ley 30/92, la Ley de 10 de enero de 1996, por la que se modifica la Ley de Bases del régimen Local de 2 de abril de 1985, instaura un nuevo sistema de gestión informática de los Padrones Municipales, de carácter activo y permanente, obligando a los Ayuntamientos, a las Diputaciones provinciales, a los Cabildos y Consejos insulares a asumir la gestión informatizada de los Padrones Municipales.

Esta intercomunicación, mediante el envío periódico de las variaciones que se hayan producido en las inscripciones padronales de todos los Ayuntamientos, sólo se puede conseguir, como muy bien expresa la Orden

Ministerial de 11 de julio de 1997, por la que se aprueban las instrucciones técnicas sobre comunicaciones electrónicas entre Administraciones Públicas, si los sistemas informáticos emisor y receptor se entienden de una manera automática, para lo cual es esencial que se definan unos formatos de cada campo de la información y se diseñen unos registros de los ficheros de intercambio que se respeten por todas las partes en el momento de llevar a cabo la comunicación.

Como puede apreciarse, se resume aquí la filosofía esencial del fenómeno EDI: el intercambio electrónico de documentos sobre la base de mensajes previamente definidos y estandarizados, susceptibles de ser «entendidos» por todos los sistemas informáticos integrados en el proyecto.

Resulta por tanto imprescindible, como pone de relieve la Instrucción, definir técnicamente las características de los ficheros informáticos de intercambio de los datos que se contienen en los ficheros municipales. Unico camino para que el «diálogo electrónico» sea fiable y operativo.

Otra novedad, esta de excepcional importancia para toda la Administración de Justicia en España, viene contenida, como ya hemos anticipado, en el nuevo artículo 230 de la Ley Orgánica del Poder Judicial. Dicho precepto, desarrollado por el Reglamento del Consejo General del Poder judicial 5/1995, autoriza la utilización de medios electrónicos e informáticos en los Juzgados y Tribunales, reconoce también la validez, a todos los efectos, de los documentos judiciales emitidos electrónicamente y, lo que es más importante para los ciudadanos, les permite relacionarse con los Juzgados y Tribunales utilizando medios electrónicos, informáticos y telemáticos, para recibir y presentar escritos y documentos.

Sin embargo, esta importantísima declaración, reconocida a nivel de Ley Orgánica -el mayor rango normativo posible-, carece, hoy da, al cabo de tres años, de realizaciones concretas que permitan pensar con optimismo en las reiteradas e incumplidas promesas de los Poderes Públicos de ocuparse de una reforma, en profundidad, de la Administración de Justicia.

El sistema judicial español no cuenta, al día de hoy, con un sistema integrado de comunicaciones electrónicas, indispensable en una administración que se precie de moderna, que le permita tramitar y gestionar el cada vez mayor número de procedimientos que saturan las oficinas de Juzgados y Tribunales.

Esta carencia, incomprensible por la gravedad de sus consecuencias, hace que resulte muy difícil satisfacer derechos básicos de los ciudadanos, entre los que se encuentra el elemental derecho a ser informado de la situación de un determinado procedimiento.

Partiendo de esta triste realidad, resulta fácil comprender que otros proyectos más ambiciosos como la existencia de una información estadística fiable o la realización de estudios sobre rendimientos y cargas de trabajo resulten prácticamente una utopía.

Si bien puede decirse que hay día ya no hay obstáculo legal alguno que impida a los Abogados y Procuradores enviar sus escritos a los Juzgados por vía electrónica e, igualmente, la Ley también autoriza a los Jueces para que envíen sus notificaciones a los Abogados por medios telemáticos. En la práctica, la falta de desarrollos técnicos y de inversiones precisas, a diferencia de lo que ha ocurrido en otros sectores del ordenamiento que hemos examinado, hace que estas soluciones, por el momento, no sean viables. Con diferente sensibilidad a la manifestada por las autoridades españolas, otros países de la Unión Europea, próximos a nosotros, como Francia e Italia, viene desarrollando importantes proyectos de modernización de sus oficinas judiciales, en ellos, con una clara visión de futuro, ocupa un lugar destacado la aplicación de las nuevas tecnologías. Así, Francia viene desarrollando, desde hace ya tiempo, un ambicioso proyecto denominado EDIJUSTICE, encaminado a introducir la tecnología EDI en los Juzgados, todo ello con el patrocinio y apoyo económico de la Unión Europea.

Mientras en Francia las reflexiones sobre la «cyberjustice» son objeto de atención permanente por parte de la Escuela Nacional de la Magistratura y el Ministerio de Justicia francés ha procedido a convocar para los días 18 y 19 de septiembre de 1997 una importante reunión para examinar la seguridad informática de los sistemas utilizados por sus tribunales y valorar también las posibles ventajas de usar la red Internet en sus comunicaciones, estos objetivos, cuya prioridad no requiere mayores explicaciones, parecen estar muy lejos de las preocupaciones cotidianas de nuestros gobernantes.

Por su parte, el Gobierno italiano, mediante la aprobación de la Ley de 7 de junio de 1993, sobre la utilización de los medios de telecomunicación para la transmisión de actos relativos a los procedimientos jurisdiccionales, y la Ley de 21 de enero de 1994, que habilita a abogados y procuradores para notificar actos

civiles, administrativos, ha contribuido a solucionar uno de los puntos negros de la justicia; el de las notificaciones.

II.- TRANSFERENCIAS ELECTRÓNICAS Y MEDIOS DE PRUEPA

La incorporación de todas estas realidades al mundo del derecho plantea problemas de especial transcendencia. En este orden de cosas, uno de los puntos críticos pasa por el valor jurídico atribuido a los actos y negocios jurídicos incorporados a soportes informáticos (discos magnéticos y ópticos).

A.- LA PRUEBA ELECTRÓNICA: GACIA UN NUEVO CONCEPTO DE DOCUMENTO.

Los medios de prueba tradicionales reconocidos en el derecho español (arts. 1.215 del Código Civil, 47 del Código de Comercio y 578 de la Ley de Enjuiciamiento Civil), y en especial la prueba de documentos -tradicionalmente unida al soporte papel y a la escritura incorporada-, se revelan insuficientes para explicar las nuevas operaciones y negocios celebrados con la colaboración de soportes informáticos.

Vemos como, hoy día, la informática invade el mundo del derecho, transformando sus pautas de conducta y sus modos operativos.

La llegada del lenguaje electrónico, obtenido por intermediación de una máquina, nos hace arribar a un nuevo concepto del documento; el documento electrónico, el cual se encuentra cada día más cerca del calificativo de documento jurídico.

De ello ya existen múltiples ejemplos en nuestro ordenamiento (véanse los arts. 49 de la Ley del Patrimonio Histórico Artístico de 1985, el art. 1.429 n° 7 de la Ley de Enjuiciamiento Civil y el art. 26 del nuevo Código Penal).

En todo instrumento probatorio hay que distinguir entre la materialidad del soporte (al que se incorpora una manifestación de voluntad o la expresión de un simple hecho) y el contenido del mismo. Por ello, podemos afirmar que el concepto de documento -tanto público como privado- que hoy recogen nuestras leyes se identifica más que con el documento en si, con las manifestaciones

históricas del mismo. En concreto, con el papel y la autografía como única manifestación de la expresión simbólica.

Claro ejemplo de este condicionamiento histórico del concepto de documento son las expresiones utilizadas por el derecho romano clásico: epístola, codex, scriptura y en sentido más genérico tabula e instrumentum.

Nuestro derecho tradicional, por influencia del romano, desconoce, hasta fechas muy recientes, la voz documento. Así, las Partidas utilizan exclusivamente la voz ..escritura», definiéndola como toda carta que es hecha por mano de escribano público de Consejo, o sellada con sello del Rey (Partida 3a, Título XVIII, Ley 1). En el mismo texto, al examinar los diversos tipos de escritura los equipara con el término cartas.

Nuestro diccionario de Autoridades, publicado en 1.739, desconoce la acepción jurídica de la palabra documento. Por influencia del derecho clásico, recoge la voz «instrumento a que, en una de sus acepciones, se identifica con la escritura u otro papel que sirva para justificar alguna cosa o certificarla.

Para Carnelutti, el medio de la representación documental puede ser, en el estado actual de la técnica, verbal o figurativo; una especie, pero no la única del documento verbal es la escritura, al lado de la cual se coloca hoy el documento fonográfico; una especie, pero no la única del documento figurativo es la fotografía, junto a la cual está el documento figurativo indirecto (el dibujo, la pintura, etc.).

En el informe Nora-Minc, elaborado bajo la iniciativa del Presidente Francés en 1.978, ya se indicaba que la telemática supone un cambio profundo en la dimensión y naturaleza de los archivos tradicionales. Para el informe francés, la constitución de bancos de datos informatizados va a originar una rápida reestructuración de los conocimientos humanos, con arreglo a esquemas hoy difíciles de establecer.

Francisco de Santis, recordando la opinión de Carnelutti, según la cual la teoría del documento está dominada por la idea de paternidad del texto escrito, defiende la posible existencia de documentos públicos o privados -según las circunstancias- confeccionados a impulsos de una computadora, siempre que contenga el texto integro y éste aparezca autenticado por una firma o contraseña electrónica.

Para Francesco Parisi, en el contrato celebrado mediante un ordenador la firma electrónica vendría a sustituir a la autógrafa con la única diferencia del soporte electrónico en lugar del papel.

Ettore Giannantonio, al pronunciarse sobre el valor jurídico del documento electrónico, advierte que no es difícil prever como en un breve período de tiempo, toda la actividad de documentación será desarrollada, salvo casos excepcionales, de forma automatizada, con la consecuencia de que el «documento manual», el documento redactado por formas tradicionales, será sustituido casi completamente por el «documento electrónico".

Este mismo autor, en su trabajo sobre los delitos informáticos (publicado en el número de Mayo-Agosto de 1. 992, de la Revista n Diritto dell 'informazione e dell 'informática), a la hora de estudiar la falsificación del documento electrónico, advierte como ante la dificultad de aplicar las normas comunes en materia de falsificación del documentos a la falsificación de documentos informáticos, muchos países han comenzado a dietar normas especiales: así la ley inglesa de 21 de Octubre de 1.981 y el parágrafo 267 del Código Penal alemán.

Citando ejemplos del derecho anglosajón, Giannantonio recuerda la existencia en el derecho inglés de la Civil Evidence Act, cuyo artículo 5 prevé expresamente la posibilidad de presentar en juicio un documento electrónico; otra norma como la Banking act de 1.979 y la Stock Exchange Act de 1. 976, ofrecen la posibilidad de hacer valer en juicio documentos informáticos en el ámbito bancario y en materia de escrituras de contabilidad.

La fiabilidad del contenido de los documentos generados y enviados por sistemas electrónicos esta condicionada, como en todo caso de discrepancia o controversia jurídica, a lograr el convencimiento psicológico del Juez que ha de valorar las pruebas presentadas bajo las reglas de la sana crítica y de la lógica.

Volviendo a los principios, entiendo que es de excepcional importancia para dotar de «credibilidad ante los Tribunales» a este tipo de mensajes electrónicos recordar las reglas generales del derecho que han sido el motor de todo el desarrollo normativo en el mundo de las empresas. Principios como el de «contabilidad ordenada», la «buena fe en la contratación», la conducta de un «comerciante leal», unidos a las garantías y controles sobre el funcionamiento y

acceso a los sistemas electrónicos de elaboración y transmisión de información, pueden, en un momento concreto, llevar al convencimiento del Juez de la validez y eficacia de una operación comercial celebrada por sistemas electrónicos.

Enzo Meriggiola, haciendo una síntesis del valor probatorio de los documentos electrónicos en los distintos países de la C.E.E., recuerda como ya el Consejo de Europa en 1.981 había elaborado una recomendación en la que invitaba a los Estados miembros a revisar el valor privilegiado que se otorgaba a la prueba escrita, en sentido convencional, en detrimento de la prueba no escrita, estableciéndose reglas comunes respecto de los registros informáticos.

Refiriéndose a la doctrina francesa, en la que se admiten los contratos concertados por medios telemáticos, pone de relieve la desconfianza que suscita la admisión de los documentos elaborados mediante datos obtenidos de la memoria de un ordenador, ante el riesgo de manipulación del documento electrónico.

Por lo que se refiere al derecho alemán, Meriggiola advierte que la presentación en juicio de microfilm, fax, telex y bandas magnéticas, así como discos ópticos, puede ser admitida por el juez en controversias referidas a la actividad comercial.

Asimismo, la jurisprudencia viene aceptando su admisión en los asuntos sobre negocios, dejando a salvo la facultad del juez de valorar, según su prudente arbitrio la prueba, valiéndose, incluso de la inspección de las fuentes de la información y de la ayuda de un experto.

Es Luxemburgo, según el artículo 1.348 de su Código Civil, donde, de una manera expresa, la ley reconoce a los datos registrados el mismo valor que a la escritura firmada, de no haber prueba en contrario.

El Doctor Daniel Ricardo Altmark, a quien la Secretaria de Justicia de Argentina encargó la elaboración de un proyecto de reforma del Código Civil, en lo referente al valor probatorio del documento electrónico (Comisión formada en 1986 por diversos expertos, bajo la presidencia del Doctor Enrique Paixao), entiende que la utilización masiva y la relevancia económica de las transacciones efectuadas con el concurso del ordenador, han contribuido a intensificar la investigación en este área, al punto que hoy puede afirmarse que el documento electrónico tiene mayores niveles de seguridad que el tradicional.

Entre las propuestas efectuadas, el proyecto del nuevo articulo 979, destinado a recoger los instrumentos públicos, reconoce en los apartados 1I y 12 los instrumentos emanados de un sistema automatizado de tratamiento de datos perteneciente a un organismo público, expresados en lenguaje electrónico o natural, emitidos de conformidad con las normas reglamentarias que garanticen su autenticidad atendiendo a la seguridad del sistema y a la inalterabilidad del instrumento, y los instrumentos emanados de un sistema automatizado de tratamiento de datos perteneciente al Poder Judicial nacional y provincial, en las condiciones expresadas en el inciso anterior.

Por lo que se refiere al derecho norteamericano, la viabilidad para presentar documentos electrónicos en juicio está avalada por la legislación federal (Uniforme Business Récord as Evidence Act y Uniform Rules of Evidence).

En líneas generales, aplicables a nuestro ordenamiento, el principio de la libre convicción del Juez en la valoración de la prueba ha de permitir la utilización de documentos electrónicos, ya sea en el proceso civil, penal o contencioso administrativo.

Por lo que respecta a nuestro ordenamiento, habrá que partir, con carácter previo, de la superación de los medios de prueba convencionales; efectivamente, tanto el art. 1215 del Código Civil, como el art. 578 de la Ley de Enjuiciamiento Civil contienen una enumeración de medios de prueba que hoy día, a la vista de los adelantos tecnológicos, no pueden conceptuarse como exhaustivos.

El documento, como objeto corporal que refleja una realidad fáctica con transcendencia jurídica, no puede identificarse ni con el papel, como soporte, ni con la escritura, como unidad de significación.

Para el magistrado Jaime Rouanet, puede admitirse pacíficamente que la «electrónica» puede ser considerada como escritura, a todos los efectos, y que, por tanto, el documento electrónico pertenece a la categoría de los documentos en sentido jurídico. La diferencia con el documento escrito tradicional está en el hecho de que la información memorizada sobre soportes informáticos no es inmediatamente comprensible por el hombre y requiere la intermediación y, en cierto modo, la traducción de la máquina.

El profesor de la Universidad de Roma, Luigi Montesano, entiende que el resultado de una operación informática puede ser conceptuado como prueba documental no escrita, pues resulta subsumible en las ..representaciones mecánicas>* previstas en el art. 2712 del Código Civil italiano.

El documento se nos representa como una materialidad a la que se incorpora una idea, es una cosa, un acontecimiento, un indicio que atestigua, comprueba, ofrece un testimonio de un hecho; más concretamente, es un objeto simbólico, una porción de la realidad material destinada a expresar, a través de signos externos, un significado especifico y determinado.

Criptología

JESÚS Mª MINGUET MELIÁN

Prof. Titular Universidad UNED

> Lo que permite al soberano saber y al buen general intuir, esperar y anticiparse, aquello que sobrepasa los límites del común de los mortales, es el conocimiento previo

Podemos definir **información** como el resultado de conocer hechos, sus causas y sus consecuencias. Adquirimos información cuando conocemos algo que antes no conocíamos. es decir, cuando pasamos del desconocimiento de algo a su conocimiento.

Poseer información es sinónimo de poder. La información puede ser o no útil en un momento determinado, pero casi siempre se considera como algo valioso. Esto ha sido así desde el principio de la historia de la Humanidad, como confirma la frase que inicia este trabajo tomada del libro *El arte de la guerra*, escrito en el siglo V antes de Cristo por el chino Sun Tse.
Si la posesión de información privilegiada siempre ha sido una ventaja competitiva, en la época actual, en la era de la información se ha convertido en algo imprescindible.

Las tecnologías de la información y las telecomunicaciones han permitido la constitución de grandes sistemas de almacenamiento, proceso y transmisión de datos e información. No es concebible ninguna organización, pública o privada, con o sin fines lucrativos, que no disponga de un sistema imformático más o menos grande. De hecho la situación es en muchos casos irreversible. ¿Podemos pensar en una sociedad sin cajeros electrónicos, tarjetas de crédito, despacho automático de billetes de avión o

tren? De hecho las estadísticas demuestran que la mayor parte de las empresas que sufren algún daño grave en su sistema informático, y que no tienen planes de contingencia o de recuperación de negocios, quiebran en el plazo máximo de un año.

EL SISTEMA DE INFORMACIÓN

De hecho el **Sistema de Información** desempeña cada vez un papel más importante en el funcionamiento de las organizaciones, las cuales llegan casi a depender totalmente de ellos. Un Sistema de Información está compuesto por los **Recursos Informáticos** (soporte informático tanto **físicos** como **lógicos**), **Activos de Información** (datos o información) y **Personas** (usuarios informáticos o usuarios finales).

Pero a la vez que los sistemas informáticos se han ido haciendo más complejos, aparecen
más y más puntos vulnerables. El número de posibles atacantes a los sistemas de información crece día a día y con las más variadas motivaciones (beneficios económicos, espionaje, venganza, terrorismo, reto personal, etc. Simultáneamente los medios técnicos pasa intentar vulnerar un sistema informático son muy sofisticados y de su mismo nivel tecnológico.
de ahí que sea imprescindible el pensar en proteger los sistemas de información. Es necesario el practicar la **Seguridad Informática**.

LA SEGURIDAD INFORMÁTICA

Resulta en general muy difícil hablar de seguridad, ya que la seguridad absoluta no existe. Para poder establecer que un sistema informático es seguro sería necesario identificar todas las amenazas a las que puede verse sometido. Por ello quizás sea más apropiado hablar de **vulnerabilidad**.

Según el profesor Valentín San Caja la **vulnerabilidad de un sistema informático** es *la cualidad que le hace susceptible de ser afectado, alterado o destruido por algún hecho o circunstancia indeseados, de recibir algún daño o perjuicio en cualesquiera de las partes o componentes, que afecte al funcionamiento normal o previsto de dicho sistema informático.*

Análogamente define la **seguridad de un sistema informático** como *el estado de protección del mismo, establecido con el fin de evitar la aparición de las distintas amenazas posibles que puedan alterar su normal funcionamiento, o de aminorar las consecuencias negativas de los distintos riesgos, una vez producidos.*

Actualmente se está tendiendo por los responsables de la seguridad de las empresas con grandes sistemas de información a una normalización de la terminología de seguridad informática. Según la Comisión de Seguridad de SEDISI se distinguen los siguientes componentes en un **Análisis de riesgos**:

. **Sistema de información.** Son los Recursos Informáticos y Activos de Información de que dispone la empresa para su correcto funcionamiento y la consecución de los objetivos propuestos por la Dirección.

. **Amenaza.** Cualquier evento que pueda provocar daño en los Sistemas de información, produciendo a la empresa pérdidas materiales o financieras.

. **Vulnerabilidad.** Cualquier debilidad en los SI que pueda permitir a las amenazas causarles daño y producir pérdidas a la empresa.

. **Impacto.** Es la medición y valoración del daño que podría producir a la empresa la materialización de una amenaza sobre los SIs. La valoración global se obtendrá sumando el coste de reposición de los daños tangibles y la estimación, siempre subjetiva, de los daños intangibles.

. **Riesgo.** Es la probabilidad de que una amenaza se materialice sobre una vulnerabilidad del SI, causando un impacto en la empresa.

. **Defensa.** Cualquier medio, físico o lógico, empleado para eliminar o reducir un riesgo. Debe realizarse una valoración cuantitativa de su coste.

AMENAZAS

Podemos dividir las amenazas que se ciernen sobre los recursos informáticos, los activos informáticos y el personal informático en cuatro clases: **Intercepción, Modificación, Interrupción** y **Generación**.

La **Intercepción** se produce cuando un programa, proceso o persona accede a una parte del sistema para la cual no tiene autorización. Es la más difícil de detectar, ya que generalmente no produce una alteración en el sistema.

La **Modificación** intenta, además de la intercepción, cambiar en todo e en parte el funcionamiento del sistema. Es quizás el tipo de amenaza más peligroso.

La **Interrupción** puede ser temporal o permanente e incluye la posibilidad de destrucción de recursos y activos. Es la más sencilla de detectar y la que presenta mayor dificultad para luchar contra ella.

Por último, la **Generación** se refiere a la adición de campos o registros en los activos, en la adición de líneas de código a los recursos lógicos, o en la introducción en el sistema de programas completos (virus, gusanos, caballos de Troya, bombas lógicas, etc.).

Evidentemente, la mayoría de las amenazas participan de las características de más de uno de los grupos estudiados.

EL ACTIVO INFORMACIÓN

El activo información puede adoptar muchos formatos, tanto dentro de los sistemas como fuera de ellos. Así podemos clasificar la información en:

. **Impresa**. Escrita en papel:
. **Almacenada**. En los sistemas o en medios portables;
. **Transmitida**. A través de redes o entre sistemas;
. **Hablada**. En conversaciones.

Pero independientemente de su formato, la clasificación que más nos interesa es la que se relaciona con el valor que la información tiene para la organización. Según este criterio podemos dividir las informaciones en **clasificadas** y **no clasificadas**.

Las **informaciones no clasificadas** son aquellas que su divulgación o uso no autorizado no ocasionan pérdidas significativas para la organización. A su vez se subdividen en: de **Uso general** (información que puede ser conocida y utilizada sin autorización por cualquier persona de la empresa o ajena a ella) y de **Uso interno** (información que no puede ser publicada, pero que puede ser conocida y utilizada por todos los empleados y algunos colaboradores externos autorizados, y cuya divulgación o uso no autorizados podrían originar pérdidas leves y asumibles por la organización).

Los **activos clasificados** se subdividen en: **Confidencial** (información que sólo puede ser conocida y utilizada por un grupo de empleados, que la necesitan para

realizar su trabajo, y cuya divulgación o uso no autorizado podría ocasionar pérdidas significativas, materiales o de imagen) y **Secreta o Reservada** información que sólo puede ser conocida y utilizada por un grupo muy reducido de empleados, generalmente de la alta dirección, y que su divulgación o uso no autorizados podrían ocasionar graves pérdidas materiales o de imagen).

Cada nivel de información debe tener defensas o prevenciones en función de la gravedad del impacto que produciría su vulnerabilidad.

LA SEGURIDAD DEL ACTIVO INFORMACIÓN

Según el *Libro Naranja de los E.E.U.U.* (normas del Truster Computer System Evaluation Criteria) y el **ITSEC** (Information Technology Security Evaluation Criteria) al establecer la seguridad de la información hay que tener en cuenta tres criterios fundamentales: **confidencialidad, integridad y disponibilidad**.

La **confidencialidad** (secreto) protege a los activos de información contra acceso o divulgación no autorizados.

La **integridad** garantiza la exactitud de los activos contra alteraciones, pérdida o destrucción, ya sea accidental o intencionada.

Por último, la **disponibilidad** asegura que los recursos y activos informáticos pueden ser utilizados en la forma y el momento requeridos. También incluye a su posible recuperación en caso de desastre.

La transmisión de datos a través de redes de computadores han creado nuevos problemas de seguridad, por lo que las normas ISO y CCITT añaden dos nuevas características: la **autenticidad** y la **imposibilidad de rechazo**.

La **autenticidad** asegura el origen y el destino de la información.

La **imposibilidad de rechazo** o **no repudio** asegura que cualquiera que envíe o reciba un activo no información no puede alegar ante terceros que no la envió o la recibió.

DEFENSA DE LOS ACTIVOS DE INFORMACIÓN

Las defensas o medidas de seguridad a establecer en un sistema de información se agrupan en cuatro tipos: legales, administrativas u organizativas, físicas y lógicas.

Los informáticos deben conocer la **legislación** vigente, pues a veces imponen obligaciones de seguridad, para conocer que tipos de amenazas deben ser prevenidas especialmente y que tipos de impactos pueden ser perseguidos legalmente. En algunos casos la referencia es a modo de recomendación. En otros la norma es un imperativo legal. Esto es especialmente importante cuando los activos a proteger contienen datos de carácter personal, los que afectan al honor, a la intimidad personal y familiar y a la propia imagen (art. 18.1 de la vigente Constitución Española).

En desarrollo del mandato constitucional se ha promulgado la LORTAD (Ley Orgánica de Regulación del Tratamiento Automatizado de los Datos de carácter personal). Otras normativas vigentes que afectan que afectan a la seguridad informática son la Ley de Facturación Telemática (arts. 4.2.f, 5.2.d, 6.1 y 7.b), la LOT (Ley de Ordenación de las Telecomunicaciones, arts. 5.4 y 24) y el nuevo Código Penal (arts. 197, 256, 264.2, 278 y 400).

Una primera forma de defensa y aplicación de la legislación vigente son las medidas de carácter **administrativo u organizativo**, como la creación de una infraestructura de seguridad informática en los distintos niveles (Comité de Dirección, Comité de Seguridad Informática, Responsable de Seguridad, etc.), normativas de seguridad y planes de seguridad y contingencias.

El siguiente nivel de protección es el **físico.** Sin entrar en detalles este nivel abarca la construcción y control de acceso a los Centros de Proceso de Datos, las medidas de protección contra fuegos, fallos de energía eléctrica o falta de aire acondicionado, los armario de almacenamiento de la cintas de back-up, la protección durante el transporte de los soportes de almacenamiento, las llaves de disqueteras, etc.

En el nivel más cercano a los activos de información se encuentran las medidas de protección **lógicas**: identificación, autorización y autentificación de usuarios, contraseñas (password), claves, cortafuegos (firewalls), cifrado, etc.

Por fin hemos situado en el entorno de la seguridad el tema objeto de este trabajo, la Criptología, la ciencia que permite el cifrado de la información.

CRIPTOGRAFÍA Y CRIPTOANÁLISIS

El ataque a los **datos** ha sido siempre el más sencillo de realizar ya que no es necesaria ninguna especialización para ello. Interceptado el mensaje (o el mensajero) o alcanzada la información el atacante logra su objetivo. Por ello, desde la más remota antigüedad, los que poseían información valiosa (estadistas, militares, diplomáticos, etc.) intentaron hacerla **ininteligible** a toda persona no autorizada mediante su cifrado.

La **Criptografía** (del griego *Kriptos*, secreto u oculto, y *Graphos*, escrito) es *la ciencia que estudia la escritura secreta*, la forma de ocultar el significado de una información.

Pero como el conocimiento de la información puede proporcionar beneficios siempre ha habido personas dispuestas a atacar una información, aunque se encuentre cifrada, por encargo de gobiernos (espías), empresas (espías industriales) o para su propio beneficio (chantajistas, estafadores o ladrones informáticos). Surge entonces la ciencia contraria, el **Criptoanálisis**. Podemos definir el Criptoanálisis como *la ciencia que estudia como esclarecer la escritura secreta u oculta.*

Aunque durante mucho tiempo ambas ciencias se han considerado un arte, no cabe duda que hoy día constituyen conjuntamente una ciencia bien estructurada llamada **Criptología**. Se puede definir la Criptología como *la ciencia que estudia como cifrar y descifrar información.*

Hemos obviado intencionadamente el término información escrita puesto que en estos momentos se está trabajando en la denominada Criptografía visual que permite el cifrado de información gráfica, que por supuesto puede ser un documento escrito. También se utiliza desde hace tiempo el cifrado de los mensajes de voz en teléfonos móviles o líneas especiales, mediante procedimientos digitales o distorsión de ondas. Por lo tanto la Criptología permite el cifrado de todo tipo de información (escrita, sonora y gráfica), aunque principalmente se dedica a la información escrita.

FUNDAMENTOS TEÓRICOS DE LA CRIPTOLOGÍA

Aunque Bauer en su trabajo ha demostrado que todos los algoritmos criptográficos de la historia obedecen a los principios de la ciencia criptográfica, se

considera que el nacimiento, como verdadera ciencia, de la criptografía se basa en dos hechos recientes:

- Los estudios de Shannon sobre los fundamentos matemáticos de la teoría de la comunicación (1948) y su aplicación a los sistemas criptográficos (1949).

- La publicación de Diffie sobre las bases teóricas de la criptografía de clave pública en 1976.

La ciencia criptológica se basa en aspectos de la **Teoría de la Información y de la Codificación,** de la **Teoría de números,** de la **Teoría de la Complejidad Algorítmica** y de la **Teoría de la Probabilidad.**

Dentro de la **Teoría de la información** los aspectos mas fundamentales son los conceptos de entropía, entropía condicional, secreto perfecto, distancia de unicidad, confusión y difusión.

De la **Teoría de números** destacaremos la aritmética modular, los logaritmos discretos, el cálculo de inversos, la función de Euler, el teorema chino del resto y el cálculo aritmético en campos de Galois.

La **Teoría de la complejidad algorítmica** trata de la clasificación de los problemas en función de que se conozca o no un algoritmo para su resolución y del tipo de estos algoritmo en función de su tiempo de computación. Es de destacar que la evolución de la tecnología en el campo de la velocidad de cómputo hace que problemas que eran intratables o computacionalmente incalculables años atrás sean hoy día totalmente resolubles en tiempo y costo admisibles.

Por último, la **Teoría de la probabilidad**, aunque importante para algunos aspectos de la Criptografía. es básica para la práctica del Criptoanálisis.

CRIPTOSISTEMAS

Un **criptosistema** o sistema criptográfico está formado por cinco elementos:

1.- **Espacio de mensajes**. Generalmente denominado **M,** es el conjunto de todos los posibles mensajes $\{m_1, m_2, m_3,...\}$ en claro, es decir inteligibles, formados con caracteres de un cierto alfabeto A, siguiendo sus reglas sintácticas y semánticas.

2.- **Espacio de cifrados**. Denominado **C**, está formado por los mensajes cifrados $\{c_1, c_2, c_3,...\}$ utilizando un alfabeto B que puede o no coincidir con A.

3.- **Espacio de claves**. Denominado K y formado por el conjunto $\{k_1, k_2, k_3,...\}$ de las claves utilizadas para el cifrado.

4.- **Familia de transformaciones de cifrado**. Una transformación E_k aplicada a un mensaje del conjunto **M** obtiene un mensaje cifrado dentro del conjunto **C** dependiendo de la clave k empleada.

5.- **Familia de transformaciones de descifrado**. Una transformación D_k utiliza el parámetro k del conjunto **K** para pasar del mensaje cifrado al mensaje en claro.

Durante mucho tiempo las claves de cifrado y descifrado eran las mismas y las transformaciones para descifrar eran las inversas de las transformaciones de cifrado. Esto no tiene por qué ser así; de hecho lo único que tiene que cumplirse es $E_k(D_k(c))=c$.

Pueden existir infinitos sistemas de cifrado pero para que realmente sea útil en la práctica y resistente a los ataques de los criptoanalistas debe cumplir los siguientes requisitos:

1º Las transformaciones de cifrado y descifrado deben ser, para todo el espacio de claves, computacionalmente eficaces y eficientes.

2º La seguridad del sistema debe depender en exclusiva del secreto de las claves y no del secreto de las transformaciones.

De hecho debe desconfiarse de los sistemas de cifrados propietario de firmas de software que mantienen secreto el algoritmo utilizado. Con gran probabilidad son algoritmos débiles que no resistirán un ataque bien organizado de criptoanalistas expertos. Aunque el algoritmo sea de dominio público, la fortaleza del criptosistema se basa en la imposibilidad de inferir la clave de cifrado de la de descifrado, o al revés.

Se distinguen dos tipos de criptosistemas: de **clave privada** y de **clave pública**.

Los **criptosistemas de clave privada**, también llamados simétricos o de clave única, la fortaleza del sistema está en el secreto de la clave k. La pareja emisor-receptor del mensaje comparten el secreto de la clave. El sistema será útil siempre que sea computacionalmente imposible determinar la clave mediante una ataque sistemático aún conociendo las funciones de cifrado y descifrado. Es de advertir que los avances de las tecnologías de los computadores hace que el concepto de incomputabilidad varíe continuamente.

Los criptosistemas de clave privada proporcionan simultáneamente el secreto y la autenticidad de los mensajes; sabemos que su contenido no ha sido modificado ni conocido por persona no autorizada.

Los **criptosistemas de clave pública**, llamados también asimétricos o de dos claves, disponen de dos claves para cada usuario U (la clave **pública** ub y la clave **privada** uv), siendo computacionalmente imposible obtener una de otra. Las Funciones de transformación E y D son conocidas. Quién quiere mandar un mensaje a U lo hace cifrando con la transformación E_{ub}. U descifra el mensaje con la transformación D_{uv}.

En este tipo de criptosistema se proporciona el secreto con la clave ub, pero no puede garantizar la autenticidad, que necesitaría el cifrado mediante la transformación D_{uv}, que sólo conoce el propietario de la clave uv. De todas maneras establecer las dos propiedades simultáneamente mediante la adición de algunos requisitos.

CRIPTOANÁLISIS

Si queremos comprobar la seguridad de un criptosistema hemos de considerar todos los posibles ataques que puede sufrir los mensajes cifrados por parte de personas que no poseen la clave. De hecho en los congresos internacionales no se admite ningún trabajo sobre un nuevo algoritmo que no vaya acompañado del correspondiente criptoanálisis, y no olvidemos que hoy día el criptoanalista posee uno medios muy poderosos de cómputo.

Una de las técnicas más utilizadas es el análisis estadístico de los mensajes cifrados para determinar la frecuencia de aparición de los diferentes símbolos, el tamaño de las palabras, las palabras más comunes, etc.. Por todo ello los criptosistemas que proporcionan una correspondencia uno a uno entre los símbolos de los alfabetos del mensaje y del cifrado son muy vulnerables al criptoanálisis.

Existen principalmente tres métodos de atacar a los criptosistemas: **ataques a partir sólo del texto cifrado, ataques a partir de algún mensaje conocido** y **ataques por elección del mensaje**.

El ataque por elección del mensaje se produce cuando el criptoanalista tiene acceso al sistema informático para introducir mensajes y observado el resultado privado. Por ejemplo el atacante podría introducir un registro apropiado en una base de datos criptografiada y obtener como se ha cifrado la información. Insistimos por tanto en la aplicación conjunta de diversas defensas o medidas de seguridad (control de acceso, autentificación de usuarios, etc) además de las criptológicas.

También es importante para que los criptoanalistas, aunque lleguen a consumar su ataque y obtengan las claves, estas les sean inútiles, el recordar que la fortaleza de los criptosistemas reside en el secreto de las claves. Por ello aparece un problema que suele traer de cabeza a los responsables de seguridad y administradores de sistemas de información: la **generación, administración y distribución de claves**.

CRIPTOGRAFÍA CLÁSICA

El procedimiento más antiguo para cifrar que se conoce es la **escítala lacedemónica**, que usaban los *éforos* de Esparta para comunicarse con sus generales. Consistía en un cilindro de madera de un diámetro determinado en el se enrollaba una cinta de pergamino, en donde se escribía el mensaje a lo largo de la generatriz. Al desarrollar la cinta el mensaje quedaba cifrado, y solamente quedaba en claro si se enrollaba en otro cilindro del mismo diámetro. Los generales espartanos jamás abandonaban su bastón. Hoy día, aunque desconozcan su uso, los altos cargos militares siguen usando la *escítala*: su bastón de mando.

A través de los tiempos se han empleado diversos métodos para cifrar la información, siendo quizás los más curiosos los cifrarios que fueron muy populares entre los siglos XV y XVII.

El método de **sustitución simple monoalfabeto** consiste en sustituir cada letra del texto en claro por otra letra del alfabeto que forma parte del texto cifrado. El método inventado por Julio César es de este tipo y consistía en sustituir cada letra del alfabeto por la situada tres lugares a la derecha (por supuesto cuando se llegaba a la z

se continuaba con la a). En general los diferentes métodos se expresan mediante la transformación:

$$E(m) = (am + b) \bmod n$$

En la **sustitución homofónica** cada letra del alfabeto se sustituye por uno de un conjunto de símbolos llamados homofónicos, siendo estos distintos para cada símbolo del alfabeto inicial. El objetivo es evitar que siempre se cambie un símbolo por el mismo, destruyendo la frecuencia de caracteres típica de un idioma. Por ejemplo a la letra A se le hace corresponder el conjunto de homófonos {13, 25, 34, 50, 95}; cada vez que se vaya a cifrar la A se toma uno de esos números de una forma aleatoria. El más conocido es el Thomas J. Beale en el que los números homofónicos indicaban la posición de una palabra en la *Declaración de Independencia de los Estados Unidos* cuya primera letra es la que corresponde cifrar.

La **sustitución polialfabeto** utiliza una palabra clave cuyas letras definen los desplazamientos que se aplican al mensaje en claro. Veamos un ejemplo con la clave SOL:

Mensaje P	L	A	N	T	A	
Clave	S	O	L	S	O	L
Cifrado I	Z	L	F	I	L	

Los más conocidos métodos de sustitución polialfabeto son los del disco del Leon Battista Alberti (siglo XV), cuadro de Vignére (siglo XVI), cifrado de Beaufort y Autoclave.

Los **cifrados tipo Vernam** se desarrollaron a partir del método diseñado por Gilbert Vernam de AT&T en 1917. El método consiste en combinar una secuencia aleatoria de números no repetitiva con el mensaje en claro, utilizando la secuencia una sola vez. La operación empleada cuando los mensajes estaban en bits para combinar las secuencias era el "O exclusivo".

La **sustitución poligráfica**, en vez de sustituir una letra por otra, sustituye digramas, trigramas, tetragramas, etc. de letras. De esta forma se destruye la frecuencia de los monogramas. Los métodos más famosos de este tipo son los de Playfair (1854) y Hill (1929).

La **transposición** es un método que no efectúa ninguna sustitución de caracteres; lo que hace es cambiar su posición dentro del mensaje. Por ejemplo la escítala lacedemónica corresponde a este tipo. Otros métodos son la permutación por grupos, el posicionamiento en zig-zag y la distribución en figuras geométricas.

Otros tipos utilizado se basan en **métodos aritméticos** (adición y sustracción, multiplicación y división, cambio de base del sistema de numeración), **transformaciones lógicas booleanas** (solo con aquellas que poseen inversa), **transformaciones matriciales** (se pasan los mensajes a bits y se forman matrices de ceros y unos con las que se operan).

No podemos abandonar este paseo por la historia de la criptografía sin mencionar las máquinas de cifrar que pretendían facilitar la labor de los criptógrafos a la hora de cifrar sus mensajes. Por no hace demasiado larga la lista sólo citaremos la famosa máquina de cifrar alemana de la Segunda Guerra Mundial: la **Enigma**. Por cierto, que los británicos lograron luchar contra ella mediante una máquina para criptoanalizar: el **Colossus**.

CRIPTOGRAFÍA DE CLAVE PRIVADA

La característica de los criptosistemas de clave privada o secreta es utilizar la misma clave para el cifrado y el descifrado, por lo que también se llaman simétricos. Como indicamos anteriormente proporcionan secreto y autenticidad. El secreto quedará garantizado si los comunicantes mantienen la clave común en secreto. La autenticidad se consigue al emplear ambos la misma clave y, por lo tanto, sólo el emisor legitimado puede enviar un mensaje cifrado que al descifrarse quede en claro. El principal problema de estos sistemas es el intercambio seguro de las claves, aunque existen algunos protocolos, como el de Diffie-Hellman, que lo facilitan y añaden seguridad. También hay que limitar el número de corresponsales ya que el número de claves aumenta con el cuadrado del número de nodos. Además casi todos los algoritmos de este tipo han sido vulnerados.

Existen dos esquemas principales de cifrado: el **cifrado en flujo** (se cifra cada uno de los bits del mensaje) y el **cifrado en bloque** (se cifran conjuntos de bits).

El más utilizado actualmente de los cifradores en bloque es el DES (Data Encryption Standard) desarrollado por IBM y estándar del NIST (National Institute of Standards and Technology) para las aplicaciones no clasificadas del Gobierno de USA. Aunque parece ser que todavía no ha sido vulnerado, ha sufrido numerosas críticas

por la escasa longitud de su clave (64 bits). De todas formas ISO considera a este algoritmo como una posible norma bajo del nombre de DEA1 (Data Encryption Algoritm 1).

El algoritmo cifra un bloque de 64 bits de texto en claro en un bloque de 64 bits de texto cifrado usando una clave de 8 octetos (64 bits). El último bit de cada octeto de la clave es un bit de paridad impar. El algoritmo consta de 16 iteraciones en las que se usan las operaciones "O exclusivo", permutaciones y sustituciones.

La única forma conocida de ataque es probar las 72.057.594.037.927.936 (2^{56}) claves distintas, lo que para un ordenador que pudiera probar un millón de claves por segundo supondría unos 2.285 años. Este tiempo se reduciría de forma considerable utilizando supercomputadores con muchos procesadores en paralelo (hasta unas pocas horas) y que sólo están al alcance de ciertas organizaciones.

CRIPTOGRAFÍA DE CLAVE PÚBLICA

Se caracterizan por el uso de dos claves por cada miembro del sistema: la **pública** (que sirve para que el resto de los miembros puedan cifrar los mensajes que quieran dirigirle) y la **privada** (que evidentemente es secreta y sirve para recuperar la información).

Se basan en las llamadas **funciones unidireccionales con trampa**. Una función unidireccional es aquella que es *fácil* de calcular mientras que su inversa es *difícil* de computar por su elevada complejidad. Se denomina función unidireccional con trampa a aquellas funciones unidireccionales que pueden ser invertidas fácilmente si se conoce alguna información adicional extra (**trampa**).

Los **cifrados exponenciales** se basan en el uso de la operación de exponenciación sobre campos finitos. Los más conocidos son el de **Pohling-Hellman** y el **RSA**.

El algoritmo debido a Pohling y Hellman en 1978 se basa en el problema NP-completo de la mochila y opera con un número primo p muy grande, realizándose toda la aritmética en el campo de Galois CG(p) o en el campo de Galois CG(2^n), siendo 2^n-1 un número primo muy grande (número de Mersenne).

Para una clave de 200 bits el número de pasos que necesitaría un atacante para violar el sistema sería de 2,7 x 10^{11}, que a un microsegundo por paso supondría

varios días. Si la clave sube a 664 bits (200 dígitos decimales) el número de pasos asciende a $1{,}2 \times 10^{23}$, lo que supondría actualmente 10^{12} años.

El algoritmo debido a Rivest, Shamir y Adleman (1977) se basa en la factorización de un número resultado de multiplicar dos números primos de gran número de cifras. El método proporciona diferentes niveles de seguridad en función de la longitud e la clave, lo que puede ser muy útil para cifrar en función del nivel de secreto del activo.

De los posibles procedimientos de ataque criptoanálitico el más sencillo es el de factorización del número n. Utilizando el algoritmo de Schroeppel se obtienen los siguientes datos en función de la longitud del número a factorizar y suponiendo que cada paso supone 1 microsegundo de computación:

Dígitos	Nº de pasos	Tiempo
50	$1{,}4 \times 10^{10}$	3,9 horas
100	$2{,}3 \times 10^{15}$	74 años
200	$1{,}2 \times 10^{23}$	$3{,}8 \times 10^{9}$ años
500	$1{,}3 \times 10^{39}$	$4{,}2 \times 10^{25}$ años

APLICACIONES CRIPTOGRÁFICAS

La criptología permite realizar con seguridad muchas aplicaciones informáticas en redes de computadores que están revolucionando la sociedad actual y lo harán mucho más en el futuro cuando se regulen legalmente. Entre ellas destacaremos la **firma digital**, las **elecciones electrónicas**, la **autenticidad, integridad y reutilización** de mensajes, la **certificación y notaría electrónicas**, la **firma de contratos**, demostrar el **conocimiento de secretos** sin proporcionar ninguna información de ellos, la **transferencia electrónica de fondos**, el manejo de **tarjetas inteligentes** en cajeros automáticos, etc.

Para la resolución de estos problemas se emplean los algoritmos de clave pública y privada existentes siguiendo protocolos de funcionamiento bien determinado. Un **protocolo** es una secuencia ordenada de pasos a realizar por dos o más entidades para completar una tarea. Entre todos los casos enumerados elegiremos los más llamativos.

Los cifrados de clave pública permiten generar **firmas digitales** que permiten asegurar que un mensaje proviene de quien dice enviarlo, evitando la suplantación de

usuarios. La firma digital electrónica, que no tiene nada que ver con la digitalización de firmas que se realiza cuando se envían fax directamente generados por un computador, es imposible de falsificar. También se garantiza simultáneamente que el mensaje no ha sido alterado, es decir, se garantiza su integridad. La firma digital se añade al mensaje o puede aplicarse a un mensaje completo. Los sistemas más empleados son la firma digital RSA, la firma digital de El Gamal y la firma DSS (Digital Signature Standard).

El **esquema electoral** permite que muchas personas puedan emitir sus votos en una red de computadores de modo que éstos sean contabilizados, que se mantenga el secreto y que el votante pueda verificar que su voto ha sido atribuido correctamente. Las condiciones para el proceso electoral electrónico son:

1º Existe una mesa que legitima el censo de votantes (L) y otra mesa que hace público el resultado (M).
2º Sólo pueden votar los electores censados.
3º Los votos son secretos.
4º Sólo se puede votar una vez.
5º Cada votante podrá verificar su voto.

El protocolo de votación en una red de computadores sería:

1º El votante A envía un mensaje a la mesa L identificándose.
2º L comprueba si A está censado y si es así le envía un número de identificación i(A) y le borra de la lista de votantes.
3º A elige una identificación secreta s(A), una de las opciones a votar v(A) y envía a M su número de identificación, su voto y su identificación secreta.
4º M localiza si i(A) está en el conjunto de los números de identificación de votantes. Si es así, M elimina i(A) de dicho conjunto y añade s(A) al conjunto de electores que votaron por la opción v(A).
5º Finalizado el proceso electoral, M pública en la red el resultado de la votación y las listas de las identificaciones secretas que votaron por cada una de las opciones.

CONCLUSIONES

Como punto de vista personal, después de todo lo expuesto, termino esta ponencia con las siguientes conclusiones:

1º La Criptografía permite prácticamente impedir la comisión del delito.

2º Algunas asignaturas de los estudios de Informática deben de adaptar sus contenidos a las nuevas necesidades. (Por ejemplo, las Matemáticas deben incluir las teorías en las que se basa la Criptología).

3º Los planes de estudios de las titulaciones informáticas deben incluir asignaturas como los Aspectos Legales de la Informática, Seguridad en Entornos Informáticos, Criptología, etc.

4º Implantación de una Política Criptográfica Nacional por los Organismos correspondientes (Defensa, Agencia de Protección de Datos, Justicia, etc.).

5º La creación por el Estado de Notarías Electrónicas u Organismos de Certificación Electrónica.

BIBLIOGRAFÍA

Bauer, F.L. **Decrypted Secrets,** Ed. Springer, Berlin, 1997.

Caballero, P. **Introducción a la Criptografía.** Ed. Ra-ma, Madrid, 1996.

Comisión de Seguridad de Sedisi. **Guía de Seguridad Informática.** SEDISI, Madrid 1997.

Menezes, van Oorschot, Vanstone. **Handbook od Applied Cryptpgraphy.** CRC Press, N. York, 1997

Morant, Ribagorda y Sancho. **Seguridad y Protección de la Información.** Ed. CERASA, Madrid, 1994.

Nombela, J.J. **Seguridad Informática.** Ed. Paraninfo, Madrid 1997.

Mesa Redonda

Derechos de Autor y uso legal del Software

Presidente: **EMILIO DEL MORAL SERRANO.**
Secretario de ALI.

Introduce y modera: **JESÚS RIVERO LAGUNA**
Catedrático del Dpto. OEI/UPM.

Ponentes: **JOSE M. FERRER SERVER**
Delegado ALI Agencia Proteccion de Datos
AMALIA PELEGRÍN MARTÍNEZ-CANALES
Abogada.
CARLOS DÍAZ DE LA IGLESIA
Director de COMPUTER WORLD.
LUIS JOYANES AGUILAR
Vicedecano Fac. Informática Universidad Pontificia de Salamanca
FELIPE DE ANDRÉS FERNÁNDEZ
Dtor. Gral. Instituto CIBERNOS y ESED

Ponencia presentada en la Mesa Redonda:

Derechos de Autor y uso legal del Software

LUIS JOYANES AGUILAR

Vicedecano de la Facultad de Informática. Universidad Pontificia de Comillas

Derechos de Autor y uso legal del Software

LUIS JOYANES AGUILAR

Vicedecano de la Facultad de Informática. Universidad Pontificia de Comillas

El valor que se puede asignar a la información, tanto directa como indirectamente, ha hecho que esta sea motivo de fuente de materia prima en la sociedad actual y motivo de objeto principal en transacciones comerciales y fuente de poder y a la vez preocupación para los estados.

La posesión de la información puede conducir a muchos beneficios y su no posesión es también causa de muchas desventajas e inconvenientes. Los creadores de información están creando una obra de propiedad valiosa, que se puede concebir para ventas, o puede ser concebida como algo valioso para el creador y para el poseedor, pero que se ponga a disposición de todo el mundo.

Estas circunstancias han creado un complejo y a veces oscuro conjunto de relaciones entre la propia información, sus creadores, propietarios y proveedores, consumidores individuales o beneficiarios de información, y el apartado del estado que busca regular estas interacciones.

El software como elemento más notable fabricado con información tiene categoría de obra intelectual y en consecuencia ha de estar protegido por las leyes y sus creadores han de gozar de los derechos de autor de dichas obras como

reconocimiento a su trabajo y a las inversiones económicas y en tiempo que ha empleado en su realización.

EL PAPEL DEL ESTADO: INFORMACIÓN, ESTADO Y CIUDADANOS

En esencia, el estado puede intervenir de cuatro modos diferentes entre el propietario de la información y el buscador o usuario de la información:

"1. Proteger la información, reconociendo el derecho de propiedad que posee su propietario (proveedor de la información). Es la función de las leyes de Copyright o más generalmente conocida como ley "de propiedad intelectual".

2. El estado debe evitar el uso no autorizado de información recogida legítimamente. Este es el objetivo de las leyes de protección de datos (especialmente datos personales y asuntos financieros de los individuos)

3. El estado ha de garantizar el derecho de acceso a ciertas categorías de información de interés o beneficio para sus ciudadanos. Esta es la función de las leyes de protección de la libertad de información.

4. El estado debe evitar la publicación o diseminación de información y opinión que considere van en detrimento de sus intereses. Esto puede ser por razones de seguridad, moralidad o conveniencia política. Es el área más difícil, dado que entraña el uso de la censura".

Aunque, en general, las cuatro actividades anteriores están relacionadas con los derechos de autor del software, nos centraremos esencialmente, en nuestra ponencia, en el aspecto estricto de la mesa redonda, tanto en el aspecto del software en computadoras y estaciones de trabajo autónomas o en red, como en su uso y difusión dentro de Internet y de las redes Intranets corporativas

EL ROL DEL ESTADO: LA PROTECCIÓN DE LA PROPIEDAD INTELECTUAL

La necesidad de proporcionar algún tipo de protección a los propietarios de la información se ha reconocido durante muchos siglos antes que fuese definido y reconocido el citado concepto como tal. Los orígenes lejanos del

copyright residen en los privilegios garantizados por estados y autoridades eclesiásticas a las imprentas y autores individuales. Los casos más antiguos conocidos se encuentran en Francia e Italia a finales del siglo quince.

Las leyes del copyright se suele considerar opera a dos niveles. En un nivel, se protege a los autores y editores. Es la personificación legal del concepto de información como propiedad y proporciona un mecanismo para prevenir la vulneración de los derechos de propiedades. En el otro nivel, las leyes del copyright regulan las circunstancias bajo las cuales se pueden producir legítimamente la copia y diseminación de la obra.

En la práctica, el copyright toma la forma de garantizar la protección absoluta de un trabajo original durante un período fijo de tiempo que en casi todos los países suele ser el tiempo de vida del autor y los siguientes 50 años a su fallecimiento. Durante ese tiempo, el trabajo sólo puede ser reproducido con el permiso del autor o de sus representantes legales. Estos representantes pueden ser individuos u organizaciones a los que se venden o ceden los derechos por el autor.

La inversión del esfuerzo intelectual del autor junto a la inversión de la experiencia profesional y el riesgo del capital asumido por la editorial están protegidas por las leyes del copyright. Idéntico principio se extiende a otras áreas de la actividad creativa individual. Las leyes protegen, de diversas formas, a diferentes productos como la pintura, la música y, en nuestro caso particular, al software de computadora. La esencia de la ley es que el producto puede ser reproducido y en algunos casos utilizados, sólo con el permiso del creador; por consiguiente, es preciso proporcionar a esa persona (o empresa) la oportunidad de ser indemnizada y composada económicamente y con reconocimiento por su obra intelectual, así como su inversión financiera y tiempo dedicado a la misma.

La protección legal del software se enfrenta con problemas. La protección de los programas y bases de datos se encuentran totalmente protegidos por las leyes españolas y la de otros países como cualquier otro tipo de propiedad intelectual. En la práctica puede conducir a muchas complicaciones. Cuando un usuario compra una copia de un programa de computadora, tal como un paquete de tratamiento de textos, lo que se adquiere es el derecho a usar esa copia. El comprador, normalmente si no es, por convenio expreso, no tiene el derecho a hacer una segunda copia del programa para utilizarla simultáneamente en otro computador. Un principio importante se personifica en esta prohibición; el

computador no obtiene, necesariamente, beneficio financiero directo de realizar la segunda copia para uso personal, sin embargo el propietario de los programas sufre la pérdida por la no venta de la segunda copia. De hecho, es extraordinariamente difícil para los editores de software evitar tales copias por individuos privados y tienden a centrar sus esfuerzo en evitar la explotación ilegal comercial de sus productos por la producción y venta de copias piratas a gran escala. Muchas empresas de software garantizan licencias de estudiantes y corporativas/institucionales (tales como empresas o universidades, cada uno con sus peculiaridades propias: animo/no animo de lucro) que permiten hacer un número determinado de copias de un programa específico para su uso con propósitos específicos. Así, es de agradecer, actuaciones empresariales de empresas y compañías de software que ayudan a la promoción y difusión del software legal con descuentos educativos y licencias corporativas. Tal es el caso de la empresa Microsoft y de la organización BSA.

DERECHO INFORMATICO

Los sucesivos avances de la informática y de las tecnologías de las comunicaciones en todos los países occidentales han hecho necesario la promulgación de normas jurídicas que tienen como objetivo principal reglamentar los diferentes aspectos del uso de las tecnologías de la información. Eso ha hecho que se haya forjado en nuestros día una nueva disciplina Juridica: el derecho de la informática o derecho informático. Son numerosas la Facultades de Derecho y de Informática así como Escuelas Universitarias de Informática que van incorporado en sus currículums asignaturas con el contenido de esta disciplina y con nombres similares.

Sin embargo, es preciso diferenciar los términos informática Jurídica que tiene por objeto la aplicación de la informática al derecho y el derecho de la informática, que consiste en la aplicación del derecho a la informática, y que es nuestro campo de estudio.

El derecho informático es una disciplina inequívocamente Jurídica integrada por las normas del derecho positivo que, disciplinan un objeto peculiar: la informática. Conforman también el ámbito disciplinario del derecho de la informática las proposiciones normativas, es decir, los razonamientos de la ciencia del Derecho dirigidos al análisis, interpretación, exposición, sistematización y crítica del sector normativo que regula la informática.

En la actualidad el derecho de la informática posee idénticos títulos científicos para constituirse en disciplina autónoma como antes lo tuvieron otras materias jurídicas novedosas como, por ejemplo, el derecho aeronáutico, el derecho espacial o el derecho comunitario.

Surgen una serie de problemas que se insertan en la temática del derecho público y que dan lugar a un derecho de la información que corre el riesgo de entrar en conflicto con los derechos sobre la información. Entre esos problemas pueden citarse: (1) Protección de los derechos de quienes han creado un programa informático; es decir, la tutela del software, así como los contratos para la utilización de las computadoras que se insertan en el campo de los derechos sobre la información; (2) La regulación del flujo interno e internacional de datos, y la protección de carácter personal y de las libertades frente a la informática, se engloban dentro de lo que es el derecho, en el derecho a la información. Ambos sectores confirman el objeto general de la informática.

El Derecho Informático lo integran las sentencias de los tribunales sobre materias informáticas y las proposiciones normativas, es decir, los razonamientos de los teóricos del Derecho que tienen por objeto analizar, interpretar, exponer, sintetizar o criticar el sector normativo que disciplina la informática y la telemática. Las diferentes fuentes y estructuras temáticas en el ámbito del Derecho Público (regulación del flujo internacional de datos informáticos, libertad informática o los delitos informáticos) y del Derecho Privado (contratos informáticos, sistemas de protección Juridica de los programas de computadora, software).

La informática Juridica, estudia el tratamiento automatizado de: las fuentes del conocimiento jurídico a través de los sistemas de documentación legislativa, jurisprudencial y doctrinal (Informática Jurídica documental); las fuentes de producción Juridica, a través de la elaboración informática de los factores lógico-formales que concurren en el proceso legislativo y en la decisión judicial (Informática Jurídica decisional); y los procesos de organización de la infraestructura o medios instrumentales con los que se gestiona el Derecho (Informática Juridica de gestión).

TECNOLOGIAS DE LA INFORMACION Y DERECHOS CIVILES

Libertades civiles, en el sentido tradicional, se refieren a aquellas actividades humanas que se hacen totalmente fuera del control del Estado. Derechos civiles, en los países que siguen la tradición del derecho romano, significa derechos ordinarios de la ley privada, tales como el derecho a hacer cumplir un contrato.

Tanto las libertades civiles como los derechos civiles tienen que ver con las relaciones entre los individuos y el Estado. La información, como motivo central de nuestro problema, plantea además una relación directa con el poder. La famosa frase de Bacon "información [o conocimiento es poder", aunque no es el único tipo de poder, hacen que las TI incrementen exponencialmente esa potencia (no es coincidencia que las personas relacionadas con las TI, le llaman el "poder informático").

La ley no es la única influencia en la relación de poder entre los individuos y el Estado y otras instituciones que ostentan el poder, pero sí es de las más importantes.

Dos desarrollos legales específicos son relevantes a las TI y las libertades/derechos civiles, descritos normalmente como protección de datos y "gobiemos abiertos o transparentes" (transparencia administrativa). La protección de datos es una aplicación específica de principios de privacidad (por sí misma, sólo reconocida como un concepto legal desde el final del siglo XIX) a tecnologías de la información, y tiene como propósito la protección de la autonomía individual sobre los datos personales. Las leyes de los "gobiemos transparentes" normalmente toman la fórmula de derechos públicos de acceso a registros del gobierno con el propósito de hacer el gobierno mas responsable ante el gobernado. Intentan dirigir el saldo de la poder de la información. Son intentos, sin embargo, imperfectos (y están muy lejos de la perfección) para evitar la predicción de Ellul de que la tecnología permite al Estado absorber la vida del ciudadano totalmente. Esto se consigue protegiendo la autonomía de la información del ciudadano y haciendo los gobiernos más transparentes. Es quizás significativo que los principios de gobierno abierto y protección de datos no son específicos a la tecnología de la información.

Numerosos son los países que han legislado ya sobre el Derecho a la Intimidad y la Protección de datos, entre ellos España. Nuestro objetivo, obviamente, no es el análisis de las mismas sino cuáles son las repercusiones y los impactos sociales de la aplicación de esas leyes y cómo podrá la sociedad

defenderse ante los ataques que esta sufriendo y seguirá sufriendo por el avance de las TI, desde un punto de vista ético y social. Hoy día, por suerte para todos, están legislados y protegidos los datos personales, el flujo internacional de datos y los contratos de software que casi siempre rigen esas relaciones. Por esta causa analizaremos los siguientes aspectos de las libertades civiles desde un punto de vista puramente social:

- Informática y democracia: La democracia digital
- La protección de la información personal en el ciberespacio
- La frontera electrónica del ciberespacio: un filo de navaja para las libertades civiles
- Los piratas del ciberespacio: ¿Una utopía: defensores de libertades o delincuentes?

Libertad informática

La libertad informática es un nuevo derecho que todas las personas deben tener y que requiere de los Estados el establecimiento de unas garantías que tutelen a los ciudadanos frente a la actual erosión y asalto tecnológico de sus derechos y libertades, en particular, de su derecho a la tutela de su vida privada. España como país democrático consolidado, tiene consagrado este derecho fundamental en su Constitución (art. 18 4).

En las sociedades contemporáneas dominadas por las tecnologías de la Información, todos los ciudadanos, desde su nacimiento, se hallan expuestos a violaciones de su intimidad perpetradas por determinados abusos de la informática y la telemática. Por esta causa se necesita el reconocimiento del derecho a la libertad informática por parte de los Estados, y por ello, prácticamente la mayoría de los Estados occidentales han promulgado leyes que defienden la libertad informática. En jerga legal, se puede decir que debe existir un habeas data que cumple una función paralela, en el seno de los derechos humanos, a la que corresponde el habeas corpus respecto a la libertad física o de movimientos de la persona.

En España esta ley es la LORTAD, promulgada en 1992; para asegurar que los derechos recogidos en la Ley estén amparados y bien tutelados, se creó la Agencia de Protección de Datos.

La LORTAD

La promulgación de la Ley Orgánica 5/1992, de Regulación del tratamiento Automatizado de los Datos de Carácter Personal (LORTAD: BOE, nº 262, de 31 de Octubre de 1992) supuso para España el incorporarse al grupo de Estados que cuentan con normas específicas para la protección de informaciones personales.

El objetivo básico perseguido por la LORTAD es el de garantizar los derechos y libertades de las personas físicas, en particular su intimidad, frente a la utilización de la informática. El texto se promulgó en desarrollo del artículo 18.4 de la Constitución, con rango de Ley Orgánica. Para el cumplimiento de esta finalidad fundamental se estructura un sistema de garantías y medidas cautelares, que pretende recoger las orientaciones del Derecho comparado en materia de protección de datos personales.

La exposición de motivos de la LORTAD concibe la protección de los bancos de datos personales desde una perspectiva funcional; no se limita a su tutela en cuanto nuevos depósitos de informaciones, <<sino también, y sobre todo, como una globalidad de procesos o aplicaciones informáticas que se llevan a cabo con los datos almacenados y que son susceptibles, si llegasen a conectarse entre sí, de configurar el papel personal>.

La LORTAD requirió un órgano de fiscalización y control bajo el nombre de Agencia de Protección de Datos y su Estatuto propio fue aprobado por el Gobierno en el Real Decreto 428/1993 de 26 de Marzo (BOE de 4 de Mayo de 1993); tiene como misiones velar por el cumplimiento de la ley, dictar instrucciones, sancionar infracciones de carácter administrativa previstas en ella, atender las reclamaciones de los interesados y redactar la memoria anual.

Protección y programas de computador

Los programas de computador, como cualquier producto de creación intelectual, necesitan ser protegidos con derechos de autor. Así, el autor o autores de un programa deben tener su remuneración correspondiente y ha de evitarse el plagio que no sólo perjudica a intereses individuales sino también en general a la industria del software que pierde rendimiento en sus inversiones de capital y

trabajo[1]. La disminución de la piratería informática en nuestro país, propiciará un aumento en la venta de programas originales y activará el sector de modo notable.

La mayor parte de países occidentales se están dotando de legislaciones protectoras que equiparan los programas a creaciones literarias, sin tener prácticamente en cuenta la protección industrial que requiere otro tipo de matizaciones relativas a invención y demanda, originalidad e innovación tecnológica. Lo deseable, como mínimo, es unificar y normalizar internacionalmente los derechos de autor, ya que los programas tienen características que no se encuentran en otros productos, y los fabricantes con proyección internacional han tenido problemas, con los sistemas de enjuiciamiento y de interpretación del concepto <<originalidad>> que no se corresponden en todos los países, lo que provoca la falta de uniformidad y, en algunos casos, de protección adecuada.

Los programas, aunque son creaciones intelectuales no materiales, en algunos casos contienen soluciones en cierto modo técnico-industriales. La ley sobre la protección Juridica de programas de ordenador (Ley 16/1993, de 23 de Diciembre) excluye expresamente de la protección: << las ideas y principios en los que se base cualquiera de los elementos de un programa que considere herramientas lógicas, como, un contador, un bucle, etc.>>[2]

Otra idea que comienza a extenderse de modo universal es la de patentar el software, lo que le dotaría de una protección adecuada, como en el caso de la protección del programa objeto como un objeto de fabricación (trade secret) que es admisible. En Estados Unidos se empiezan a admitir las patentes para programas de computador. Davara ve difícil encuadrar el software como objeto de propiedad industrial y también como objeto de propiedad intelectual[3].

En España, la ley de Patentes (Ley ll/1986 de 20 de Marzo, BOE n° 73 de 26 de Marzo) dispone que '< 1. Que son patentables... los programas de

■[1] En esta mesa redonda y, con seguridad, en la sesión de mañana, en la ponencia específica sobre piratería del software, saldrá a colación, con frecuencia, estas consideraciones.

■[2] Carlos Barriuso, Madrid, 1996, p. 179.

■[3] M.A Davara: Derecho informático, Aranzadi, Pamplona, 1993, pp 110y 117.

ordenador>>. Y la ley 22/1987, de 11 de Noviembre, de propiedad intelectual (BOE núm. 275, de 17 de Noviembre de 1987) indica en su artículo 100 que <<los derechos sobre los programas de ordenador, así como sobre sus sucesivas versiones y los programas derivados, podrán ser objeto de inscripción en el Registro de la Propiedad Intelectual>>. Actualmente la Ley sobre la protección Juridica de programas de ordenador regula legalmente los programas de ordenador equiparándolos a obras literarias, protegiéndolos mediante el derecho de autor correspondiente.

Los virus

Como Barriuso[4] ha señalado certeramente, creemos que una de las causas fundamentales de la proliferación de virus, muy bien podría haber sido la falta de protección del software, además de razones lúdicas o de otra naturaleza de tipo fraudulento. Algunos de los virus creados con carácter lúdico han terminado planteando problemas éticos a usuarios y fabricantes, ya que los intereses de algunas empresas fabricantes de software han podido beneficiarse, temporalmente, de los mismos . Sin embargo, si el fantasma del virus planea sobre el usuario, éste se lo pensaría dos veces antes de utilizar copias de software piratas.[5]

Luces y sombras en la libertad informática

La nueva Ley de Protección de Datos defiende correctamente los derechos de las personas y sobre todo da amparo al cumplimiento fiel del ya citado artículo 18.4 de la Constitución española Nuestra respuesta como legos en Derecho sólo podía darse estudiando a los expertos en Derecho Informático, de cuyas fuentes se podría deducir los posibles cambios sociales que afectarían a la fidelidad/no fidelidad al citado artículo 18.4.

■[4] Barriuso, op. Citada., pp. 180-182.

■[5] Barriuso realiza un examen riguroso en la obra ya citada sobre la construcción, uso y difusión de programas específicos de virus informáticos. Así mismo, comenta y analiza de modo muy comprensible para los no legos en derecho, la ley 16/1993 relativa a la protección jurídica de programas de ordenador.

En opinión de los expertos la LORTAD presenta en su haber dos aspectos abiertamente positivos: la definición de los principios básicos, y el reconocimiento y tutela Jurídica de la libertad informática - y un aspecto negativo, discutible e inquietante: sus constantes y significativas excepciones.[6]

Entre los principios básicos que informaran la actuación de los bancos de datos automatizados que procesen informaciones personales, se encuentran los siguientes: la calidad de los datos, la transparencia (obliga a informar a los afectados por la recogida de datos personales sobre la finalidad, obligatoriedad, consecuencias y derechos que implica su tratamiento automatizado), el consentimiento (como garantía de los afectados), la tutela reforzada de los datos sensibles (evitar tratos discriminatorios por motivos de razón, salud, vida sexual), la seguridad (frente a la alteración, pérdida o acceso indebido a los datos personales, el secreto y la cesión (limitada al uso para fines legítimos y con el previo consentimiento del afectado).

El otro aspecto abiertamente positivo de la LORTAD consiste en el reconocimiento y tutela Juridica de la libertad informática. Su función se cifra en garantizar a los ciudadanos unas facultades de información, acceso y control de los datos que les conciernen. Para ello, al tradicional habeas corpus corresponde en las tecnologías del presente el habeas data, que constituye un cauce o acción procesal para salvaguardar la libertad informática.

En el debe de la LORTAD, recoge Pérez Luño determinados fallos e insuficiencias, que son, en esencia, significativas excepciones que limitan el alcance práctico del ejercicio de las libertades informáticas. Pérez Luño considera que se establecen excepciones relevantes referidas esencialmente - a: la información de los afectados; a su consentimiento; a las garantías de los datos sensibles; a la posibilidad de que las Fuerzas de seguridad del Estado puedan informatizar datos sensibles sin control judicial, fiscal o de la propia Agencia de Protección de Datos; a los límites al ejercicio de los derechos de acceso, rectificación y cancelación a los bancos de datos públicos; así como a la restricción del derecho a la información y acceso de los ciudadanos a los datos que les conciernen (habeas data) elaborados por las Administraciones Públicas por motivos tan vagos como «das funciones de control y verificación» de las

■[6] Pérez Luño, Barcelona, 1996, pp 61-64.

mismas y a la supeditación general de la tutela a cuanto afecte a la Defensa Nacional, Seguridad Pública, interés público o intereses de terceros más dignos de protección.

Archivos Robinson o archivos pecera

Uno de los aspectos de la LORTAD que es preciso tener presente por los riesgos que entraña, se deriva de las prácticas abusivas del correo electrónico y del tráfico de datos.

La información es, naturalmente, el símbolo emblemático de la sociedad de la información, pero el hecho constatado de que la información es poder y es decisiva gracias a la informática, hace que el uso de las tecnologías de la información por los poderes públicos sea, si bien licito, motivo de gran preocupación, si no se tiene una garantía plena de protección por las leyes correspondientes - en el nuevo caso español, la LORTAD - y los órganos encargados de velar por su cumplimiento - en el caso español, la Agencia de Protección de datos -.

Mucho mas grave es la situación en la esfera privada. Las sociedades y empresas de hoy miden su dinamismo y empuje por la cantidad y calidad de sus informaciones. La trascendencia económica de la información ha generado un apetito insaciable de obtenerla por cualquier medio y a cualquier precio y es directamente responsable de determinadas prácticas abusivas que hoy acechan a la privacidad de la vida cotidiana[7].

Así, para aumentar la confusión y aprovechar el clásico refrán de "a río revuelto, ganancia de pescadores", se han realizado hasta perversiones del lenguaje Se han acuñado dos términos que en la jerga informática representan ficheros que contienen información sensible a las personas afectadas: archivos Robinson y archivos pecera.

Los archivos Robinson son aquellos en que deberían inscribirse aquellos ciudadanos que no quieran ver perforada su privacidad por la recepción de propaganda no deseada, quedando, de este modo, a salvo del mercado <(blanco»

■[7] Ibid, p. 59.

o <<negro>> de archivos de información. Como resalta Pérez Luño, el propio nombre de los archivos denuncia ya parcialidad del juicio. Es decir, paradójicamente es el ciudadano el que ha de inscribirse en esos archivos, cuando parece lógico que debería ser justo al revés: la empresa interesada en difundir datos personales debería pedir autorización a la persona afectada.

Los ciudadanos de nuestras sociedades tecnológicas dominados por la información, y hoy día, más en concreto por <<los bits>>, se sienten controlados, es como si vivieran en una casa de cristal en la que todas las actividades pueden ser controladas; es el conocido <<síndrome de la pecera».

Muchas personas contemplan la creciente influencia de las computadoras en las sociedades modernas como una amenaza extrema. Cada día más actividades cotidianas - llamar por teléfono, conducir un coche, utilizar una tarjeta de crédito o fichar en la empresa - se registran e investigan, es decir, las personas se sienten "vigiladas" o controladas. Es lo que se ha venido en denominar el auge de la vigilancia o la omnipresencia del «ojo electrónico>.[8] Es el temor siempre fundado al <<Gran Hermano» de Orvvell.[9]

Computadoras, libertad y privacidad

Con los nuevos servicios en línea, ofrecidos por operadores de telefonía, se está abriendo una ventana al mundo, al cine, a los servicios de consumo para permitir charlar con los amigos, etc. Esta situación implica unos riesgos en cuanto a la privacidad de datos íntimos.

Los problemas de computadoras y privacidad se remontan a los años 60, cuando los gobiernos, en primer lugar, comenzaron a almacenar sus archivos en las maquinas de grandes dimensiones en uso por aquel entonces. A medida que la ampliación del control de requisitos al sector privados, las maquinas se convirtieron en depósitos de los detalles más íntimos de la vida de las personas. Cualquiera que abra una cuenta corriente en un banco está dejando una traza o huella electrónica, por uso de servicios tales como pago de un recibo de colegio,

■[8] David Lyon, Madrid, 1995.

■[9] George Orvell, Barcelona 1991.

hábitos de compra, visitas a hospitales, etc. El servicio de teléfonos crea, también, huellas que conducen a familias y amigos. Incluso un número de la seguridad social es un riesgo potencial, dado que es factible, entre otras cosas, que un detective pueda curiosear los datos personales del titular, incluidos datos de impuestos o datos íntimos. Piénsese en el caso, ya citado anteriormente, relativo a las compras actuales en el ciberespacio, donde es muy fácil el delito informático con sólo conocer el número de la tarjeta de crédito de un usuario, y manipularlo adecuadamente

Desde la década de los sesenta, la invasión de la privacidad (intimidad) se ha hecho relativamente fácil. Cada vez más datos personales adoptan formato digital. Los números de carnet de conducir proporcionan enlaces electrónicos a las características físicas de la licencia y al almacén de información del registro de conducir. Las tarjetas de crédito y la tarjetas de cajero automáticos hacen mas asequibles los registros financieros.

Al mismo tiempo, las propias computadoras funcionan a velocidad que eran impensables hace un año; las computadoras personales que contienen un chip Pentium de Intel son 500 voces más rápidos que las máquinas dotadas con un chip de primera generación de PC. Hoy, con 300.000 pesetas se puede comprar prácticamente la misma facilidad de búsqueda y recuperación de datos, que con los mas avanzados sistemas de negocios y de la administración pública de principios de la década actual..

A medida que crece la potencia de las computadoras lo hace también la información disponible. Los servicios comerciales en línea, solicitan de modo rutinario a los miembros presentar perfiles personales junto con sus números de tarjetas de crédito. Estos pueden incluir, no sólo nombres y direcciones sino también aficiones (elementos que se pueden utilizar para crear listados de correos de gran valor para anunciantes y marketing. Dichos servicios, comprueban normalmente las unidades de disco duro de las computadoras de los miembros cada vez que ellos se conectan.

Cada pulsación de su teclado en línea deja su huella en las computadoras centrales del servicio. En poco tiempo, los operadores del sistema pueden construir perfiles detallados de miembros basados en su correo electrónico, los nuevos grupos de Internet, a los que se subsanen, los tipos de software que se descarga en ellos. Tales perfiles pueden venderse a los telecompradores o similares utilizando servicios en línea para enviar mensajes comerciales en función

de la democracia. Estos perfiles son también vulnerables a la penetración desde el exterior.

IMPLICACIONES JURIDICAS Y REGULACION DEL CIBERESPACIO

Los derechos de autor en el caso de programas de computadora es y ha sido uno de los temas centrales en la protección de la propiedad intelectual. Las leyes de Copyright, en el caso del software distribuido por canales comerciales clásicos, han sido aplicadas, y existen también leyes de la propiedad intelectual que protege a los autores contra el delito de piratería y fotocopias no autorizadas. Con todo, existe en la actualidad una serie de delitos que exigen de una rápida regulación nacional e internacional.

Se trata de todos los delitos producidos a través de las redes de comunicaciones y fundamentalmente vía autopistas de la información e Internet, es decir, en el ciberespacio. Las implicaciones legales en el ciberespacio son motivo de atención especial por parte de los Colegios de abogados de todo el mundo, y lógicamente por los correspondientes Parlamentos nacionales y Transnacionales que están comenzando a legislar al respecto.

El ciberespacio como manifestación de la aldea global generada por el entramado de redes de computadoras y la proliferación de nodos en todo el planeta. ha ayudado a la difusión inmediata de los mensajes y permite el acceso a cualquier información introducida en la red. Estados Unidos, pionero en la regulación de los derechos de propiedad intelectual en el ciberespacio, ha creado el Grupo de Trabajo sobre Derechos de propiedad intelectual (IITF Working Group on Intellectual Property Rights) presidido por el Secretario de Comercio Ronald H. Brow. [10]

El ciberespacio ha sido definido en Estados Unidos con el nombre técnico de Infraestructura de la Información y el objetivo principal de las

[10] Este grupo de trabajo ha emitido ya un informe de unas 300 páginas que ha sido publicado en Internet y que puede ser consultado y extraído en el Web cuya dirección electrónica es: http: //www. uspto.gov/web/ipnii .

propuestas legislativas se encaminan en la dirección de aplicar las actuales leyes de la propiedad intelectual al ciberespacio.

Existe un intenso debate respecto a la necesidad de prevenir y sancionar los malos usos en la red. Existen argumentos a favor de la regulación, argumentos en contra y criterios de autorregulación (códigos de conducta y ciberpolítica).

Criterios para la regulación de las leyes en el ciberespacio

Los partidarios de la regulación se apoyan en la tesis de la comisión de delitos difíciles de perseguir por la naturaleza del entorno y la falta de tipificación de las modalidades de comisión y de los medios empleados.

- Delitos informáticos
    - •- Acceso no autorizado a información
    - •- Destrucción de datos (virus, sabotajes informáticos)
    - •- Infracción de los derechos de autor
    - •- Infracción del Copyright de las bases de datos
    - •- Estafas electrónicas
    - •- Interceptación de correo electrónico (e-mail)
    - •- Transferencia de fondos
- Delitos convencionales
    - •- Espionaje (servicios secretos, espionaje industrial, de arte etc)
    - •- Terrorismo
    - •- Narcotráfico
    - •- Otros delitos (tráfico de armas, proselitismo de sectas, propaganda de grupos extremistas...)
- Mal uso de la red
    - •- Usos comerciales no éticos
    - •- Actos parasitarios (obstaculizar comunicaciones ajenas, interrumpir conversaciones de modo reiterado, enviar mensajes con insultos personales etc.

Efectos transfonterizos Los actos o delitos se realizan en un país determinado pero debido a la universalidad de la red tienen sus efectos en otro u otros países. Existen conductas activas o pasivas.

Frente a la corriente reguladora se levantan los partidarios de que ciertas áreas quedan libres del intervencionismo o proteccionismo estatal. Entre los

argumentos mas utilizados figura el derecho a la intimidad y la libertad de expresión.

- Derecho a la intimidad
- Libertad de expresión
- Libertad de acceso a la información

Autorregulación: códigos de conductas y ciberpolicías

Internet en cuanto una red abierta, se ha autoimpuesto unos códigos de conducta en ausencia de una legislación especifica. Existen unos códigos de ética para los usuarios de Internet, cuyo incumplimiento esta castigado con la censura popular. La tónica y el talante de Internet es el respeto entre los usuarios de la red. Ha sido notorio la censura impuesta en la Red a la información publicada por el grupo terrorista ETA. Las pantallas del web de información, con sede en Suiza que da amparo a ETA, fue cegado con lazos azules, por diferentes programas que lanzaron estudiantes y profesionales informáticos, tras el asesinato del profesor y jurista Tomás y Valiente por un miembro de ETA.

Otros códigos que se utilizan en la Red son los sistemas de seguridad informática, aunque éstos desde el punto de vista técnico pueden ser neutralizados.

Por último, van comenzado a nacer los grupos de vigilancia de la Red ciberpolicías, que se dedican a la localización de piratas informáticos (hackers), saboteadores, comisión de delitos informáticos en la red etc., en particular asociaciones y agencias americanas, tales como NSA, First Forum of Incident Response and Securites Teams, CERT (Computer Emergency Response Team). La Administración americana ha aprobado a primeros de Febrero de 1996 una Ley para protección frente a contenidos de carácter ilegal (pornográfico, terrorista etc.)

Situación actual y propuestas legislativas nacionales e internacionales

La situación actual en los países democráticos es de regulación y actualización, en su caso, de las leyes de protección de datos, derechos de autor y cualesquiera otros derechos conexos con la sociedad de la información.

Los estudios, informes y propuestas legislativas o leyes ya vigentes, que van sido considerados, son las relativas a los países o asociaciones internacionales siguientes:

- Estados Unidos
- GATT (Ronda de Uruguay)
- El grupo G7
- La Comisión Europea (Libro Verde sobre los derechos de autor y derechos conexos en la Sociedad de la Información
- España (LORTAD, Agencia de Protección de Datos y el nuevo Código Penal)

La legislación española ha dado un salto cualitativo y cuantitativo en la protección de la propiedad industrial e intelectual, así como en la protección de los datos personales. Los documentos legales más sobresalientes -ya citados - son:

- Ley LORTAD
- Estatuto de la Agencia de Protección de Datos
- Nuevo Código Penal (BOE de 24 Noviembre de 1995, que entró en vigor en mayo de 1996)

La mayor parte de los delitos informáticos que pueden cometerse han sido regulados por el nuevo código penal que, como se ha mencionado entró en vigor en Mayo de 1996(Apéndice B), aunque este no es el caso del ciberespacio, donde todavía existen grandes lagunas legales. Las características más sobresalientes son las siguientes:[11]

1. En los delitos contra la intimidad se introduce la interceptación de correo electrónico o cualquier otro tipo de comunicación o documento que queda asimilada a la violación de correspondencia.

2. También quedan tipificados los actos consistentes en apoderarse, utilizar, modificar, revelar, difundir o ceder datos reservados de carácter personal que se hallen registrados en ficheros o soportes informáticos, electrónicos o telemáticos.

■[11] Javier Rivas. Madrid, 1996. Pp. 367-368.

3. Queda incluida la estafa electrónica, consistente en la manipulación informática o artificio similar que concurriendo ánimo de lucro, consiga una transferencia no consentida de cualquier archivo patrimonial en perjuicio de tercero.

4. En el delito de daños se introduce la destrucción, alteración, inutilización o cualquiera otra modalidad por la que se dañen los datos, programas o documentos electrónicos contenidos en redes, soportes o sistemas informáticos.

5. Respecto a los delitos contra la propiedad intelectual, desaparece la exigencia de que la conducta del tipo básico sea intencionada, es decir, no es necesaria la concurrencia de dolo directo. Con la proliferación de las obras multimedia y el uso de la red, este tipo se aplicará no solo a los programas de computadora, sino también a los archivos con imágenes, gráficos, sonido, vídeo, texto, animación, etc.

6. Finalmente, la fabricación o tenencia de útiles materiales, instrumentos, programas de computadora o aparatos destinados específicamente a la comisión de estos delitos se castigarán con las penas señaladas para los autores. Entrarían dentro de este tipo los programas copiadores, las utilidades empleadas por los hackers y cualquier otro dispositivo.

LA PROPIEDAD INTELECTUAL EN EL CIBERESPACIO

El nuevo Código Penal español es, posiblemente, uno de los mas avanzados en la defensa de la propiedad intelectual en las redes de computadoras, y aunque no se cita expresamente Internet,(con buen acierto, entendemos, pues aunque la publicación del nuevo Código ha sido a lo largo de 1996 y tal vez hubiese permitido la alusión, no sabemos si en el futuro la Red Internet, se seguirá llamando así, se llamará ciberespacio, o cualquier otro término que se pueda acuñar), la virtualidad del nuevo código es que se ha adelantado en la defensa de los derechos de autor y la protección de los datos personales en el ciberespacio.

Pese a esta nueva propuesta legislativa, que se adelanta a muchas iniciativas de otros países occidentales, los temas legales en el ciberespacio

requieren una gran atención, y en particular las leyes del Copyright pueden ser especialmente difíciles. Se dan diversos argumentos en apoyo de estas conclusiones, debido a que el ciberespacio es tan diferente del mundo físico que las leyes de la propiedad intelectual no pueden enfrentarse a las diferencias.

En apoyo de este argumento, se observa que la abrumadora potencia de la conectividad digital, la duplicación instantánea y la distribución de cualquier trabajo es mas fácil hoy que antes. Muchas personas opinan que nunca como ahora, un individuo puede distribuir su propio trabajo mas fácilmente ante una amplia audiencia.

Un usuario en una red o un sistema de correo electrónico o de intercambio electrónico de datos puede hacer hoy esta difusión con una simple pulsación de una tecla o haciendo clic en el botón de un ratón de computadora. Muchas personas destacan las diferencias entre ciberespacio y comunicaciones no informatizadas, dado que cuando originalmente el sistema de Copyright fue desarrollado, esta potente manipulación de propiedad intelectual era impensable.

Otra idea, avalada también por Negroponte, reside en la idea de que las palabras, sonidos o imágenes del ciberespacio no son nada más que una colección de unos y ceros (el mundo de los bits de Negroponte). Estos dígitos no tienen significado (en un disquete, un disco duro etc.) basta que reordenan o procesan por una computadora. Por esta razón, a la duplicación o transferencia de textos e imágenes que se representan por datos no se les puede aplicar las leyes del Copyright.

A pesar de que, como hemos comentado, nuestro Código Penal y nuestra Ley de Protección de Datos (LORTAD) protege los derechos y la propiedad intelectual, y es una ley mas avanzada que las de muchos países occidentales, siguen existiendo una serie de dificultades que trataremos de plasmar en nuestras próximas líneas, síntesis de nuestra investigación.

Haremos abstracción de los derechos de propiedad tradicionales recogidos en las leyes de cada estado y nos centraremos en los problemas sociológicos que plantean en el ciberespacio.

Copyright en el ciberespacio

Los temas de Copyright dominan el ciberespacio. Esto es así, debido a que casi todo lo que se transmite a través de una BBS, un servicio en línea o una red, es propenso a la protección de Copyright. La naturaleza del medio es tal que virtualmente todo el discurso (plática, articulo...) es una expresión que ha sido fijada en un medio tangible tal como se define por la ley de Copyright. Mientras que una llamada telefónica corta no implica Copyright?, el equivalente electrónico (una asistencia o una sesión o charla chat) usuario a usuario, una carta, un artículo en correo electrónico (e-mail), su equivalente electrónico, sí lo implica. A continuación haremos una revisión de las implicaciones del Copyright de diferentes actividades de telecomunicación.

Correo electrónico (e-mail), noticias de grupos (newsgroups), charlas (chats)

El momento en que se almacena un correo electrónico en un dispositivo de almacenamiento se debe considerar como el principio de la propiedad del remitente, al igual que si se tratara de una carta. No debería ser necesario ningún símbolo de Copyright (g) dado que en cada correo electrónico figura la dirección de la persona o institución remitente. En consecuencia, la difusión del contenido del correo-e implica una autorización de su autor, o al menos su referencia. Por esta causa, no debería ser posible el envío de un texto no autorizado por la red, aunque ya es usual la publicación de capítulos o extractos del mismo en Internet; tampoco puede ser enviado como correo electrónico, dado que en este caso el emisor no ha sido el autor del texto y, por consiguiente no tiene derechos legales sobre el mismo. Ha sido de actualidad la publicación en Internet del libro biográfico sobre Miterrand cuyo autor fue el medico personal del presidente francés y cuyo tema central era la ocultación de su enfermedad a los franceses. Su secuestro legal, fue vulnerado por una ciberteca (cafetería con conexión a Internet) que lo difundió a través de la red y su autor se encuentra en pleitos con la Justicia de Francia.

El envío de un mensaje a un mensaje base o desde o hacia un servicio de Noticias de Grupos (Newsgroups) es muy similar al envío de un correo electrónico, por lo que las leyes del Copyright deberían aplicarse de igual modo.

En este caso, sin embargo, existen particularidades a tener en cuenta por su naturaleza. Estas noticias o mensajes suelen o deben incluir un mensaje de Copyright o de autorización, de reproducción, reenvío, copia etc., total o parcial, dado que normalmente se dirigen a una numerosa población. Al contrario que un correo-e, un mensaje de un servicio de Noticias de Grupos suele ser una compilación o trabajos colectivos que constan de muchos mensajes. Los grandes proveedores de Información, como CompuServe, (Red de información de Estados Unidos, conectada a su vez a Internet y que tiene cinco millones de abonados en todo el mundo), están comenzando a difundir sus mensajes con logos de Copyright, o logos especiales o sin ellos, para significar su autorización o denegación a su reproducción.

Imágenes digitales

Las imágenes digitales se han vuelto muy populares en las BBS (tablones electrónicos de anuncios) y en servicios en línea y se distribuyen y circulan a través de las redes. Estas imágenes adoptan la fórmula de archivos informáticos que se pueden transferir a y desde grandes sistemas o servidores de información y visualizados con software especial.

Cada archivo de una imagen ha de estar protegido por un Copyright a menos que se renuncie al mismo. A menos que se posea el Copyright de la misma, la copia, o creación de la imagen con un escáner digital, se esta violando la ley de propiedad intelectual. En la actualidad, un gran porcentaje probablemente una mayoría - de archivos de imágenes disponibles en los diferentes sistemas telemáticos, representan la violación del Copyright de alguien. Especialmente predominantes son las imágenes de sexo escaneadas de revistas para adultos o capturadas de películas pornográficas.

En este punto, y ante el incontenible avance de los sistema multimedia, sobre todo en computadoras PC domésticos y la definición de software multimedia en la red, se exige un comportamiento ético de todos los usuarios de la informática, ya que en este caso no sólo esta implicada la pérdida económica de unos derechos de autor protegidos por las leyes, sino que estos usos indebidos implican unos riesgos sociales muy altos, al promover la difusión gratuita, masiva - y por consiguiente - "fácil" de escenas de sexo y - naturalmente también - de violencia, que sin la ayuda de la Red, no saldría probablemente de los ámbitos usuales de la distribución comercial escrita o visual.

Charlas en directo

Las charlas o tertulias en directo (line chat, "charlas en vivo") es otro de los foros usuales en la Red que requiere, no solo la protección del Copyright de los textos utilizados para sus directrices, participantes, etc. sino también una protección al derecho de opinión, y naturalmente evitar el insulto y los malos modos en dichas tertulias o charlas.

Naturalmente, los participantes en estas tertulias no consideran protegidas sus expresiones, a menos que sean transcritas o capturadas en discos de computadora/audio.

En el momento en que la escritura, tecleado en computadora o copia se produzca, las leyes de Copyright han de amparar esta situación, proporcionando a las personas intervinientes en la tertulia una protección inmediata. Los personajes participantes en una popular tertulia radiofónica española han publicado en un disco compacto, un disco con el texto y voz de sus charlas, en el último trimestre de 1995.

Software

La protección de los derechos de autor en la creación del software, están amparados por las leyes correspondientes. Existen, sin embargo, determinados tipos de software y situaciones de implantación que requieren un uso legal especial y sobre todo en estos casos, el uso de unos principios éticos por parte del usuario, que permitirá el desarrollo y avances comerciales de productos software y redundara en beneficios sociales para empresas y diseñadores/creadores de programas.

Los programas, o mas general el software, se pueden clasificar en diferentes grupos, cuyo uso implica una serie de considerandos legales y sociales que tratamos a continuación, centrándonos esencialmente en los programas que se pueden encontrar en el ciberespacio y su agrupamiento en diferentes clases, basado en los derechos de licencia que conceden sus autores o propietarios legales.

Programas comerciales

La mayoría de los programas existentes se han escrito, comercializado y distribuido con la intención de ser utilizados por las personas que pagan por su uso y bajo un acuerdo (contrato) estricto de licencia por el mismo. Este acuerdo normalmente prohibe hacer copias en mayor número de las compradas o con los propósitos especificados en el acuerdo. Es normal que el software con fines educativos se adquiera a bajo coste, precisamente para facilitar su uso y difusión en la comunidad educativa para fines de formación o investigación. Las bajas tarifas que dan los fabricantes a las universidades y otras instituciones educativas suelen requerir el compromiso formal de las instituciones educativas de que solo usaran ese software con fines educativos.

La adquisición de este tipo de software esta protegida por las leyes antipiratería y de protección de los derechos de autor. Su facilidad de copia ilegal exige un compromiso ético de las empresas, instituciones y particulares para el cumplimiento. Naturalmente, como sucede con tantas actividades de la vida este compromiso ético no es asumido por todo el mundo, por lo que han nacido asociaciones nacionales e internacionales (13SA. SEDISI...) para velar por la protección legal del software, así como jueces y policías especializados en este tipo de delitos.

Este software comercial no entraña grandes problemas éticos ni comerciales, dado que su adquisición y transferencia esta siempre condicionada a su pago por cheque, tarjeta de crédito, dinero electrónico etc. Aquí los únicos problemas que se plantean son puramente técnicos, dado que la transmisión del numero de tarjeta de crédito a través de la red entraña graves riesgos de seguridad, si la transacción no se hace con empresas que dispongan de medios de seguridad fiable que permitan el cifrado de información sensible y en consecuencia la protección absoluta, evitando el delito informático.

Los programas etiquetados bajo este nombre suelen ser los mas usuales en el ciberespacio; son programas de libre difusión, que el usuario puede utilizar y probar libremente durante un tiempo determinado y transcurrido ese tiempo, si desea continuar usándolo, ha de pagar unas tasas al autor, (normalmente pequeñas, comparadas con los precios de programas comerciales). Este método se ha hecho muy popular como medio de difundir programas escritos por autores independientes o pequeñas empresas (comienza ya a ser frecuente también su uso

por grandes empresas). Cuando un programa se distribuye como Shareware, los usuarios, normalmente, tienen derecho a realizar copias de prueba para su uso. Si deciden continuar utilizando el software, transcurrido el período de prueba, han de registrar su uso con el autor, normalmente por el procedimiento del envío al mismo de unas tasas de registro.

Este sistema de distribución entraña una buena política de marketing idónea para las personas y empresas citadas, que asumen un grave riesgo comercial, al estar casi siempre su uso en manos de la ética del usuario y de su voluntad para entender y colaborar en estas practicas comerciales.

Los autores de programas pueden decidir que sus trabajos tengan el carácter de dominio público; en este caso, no existe ninguna restricción para la distribución, duplicación o cualquier otra manipulación del software. Este tipo de software es usual en investigadores, aficionados y programadores noveles que altruísticamente, por afán de notoriedad o simplemente por un lógico afán de promoción personal (quede otra forma le seria muy difícil dar a conocer su trabajo), suelen ser las personas que sitúan en la Red, software de dominio público.

CONCLUSIONES

Existe otra variedad de problemas que afectan a las leyes de la propiedad intelectual y que afloran cuando están involucradas comunicaciones &rectas (en línea) entre computadoras. Especialmente, el advenimiento creciente de los sistemas multimedia que permiten digitalizar audio y vídeo, está planteando nuevos problemas para la protección del software basado en esta tecnología. Las conclusiones más inmediatas son el entrelazado existente entre la naturaleza legal del software y su protección, y la ética del usuario y de las empresas, considerando - lógicamente - que la ética ha de ser una de las virtudes de las empresas, que utilizan ese software, y que tienen muy fácil, en ocasiones vulnerar la legalidad, cometiendo delitos de uso ilegal, pero difícilmente detectables.

En consecuencia, y dado que el software es y seguiría siendo uno de los productos estratégicos de la economía mundial y - por ende - de la sociedad de finales de este siglo y del próximo, se requiere de los gobiemos nacionales leyes que protejan esos productos ante usos indebidos o fraudulentos, tanto a nivel local como transnacional, y, además, la necesidad de una ética profesional,

fundamentalmente de los informáticos y de las empresas distribuidoras o consumidoras de software, que ampare el correcto uso de los mismos.

BIBLIOGRAFIA

BARRIUSO, c.: Interacción del derecho y la informática. Dykinson: Madrid, 1996.

CAVAZOS, E.: Intelectual Propertes in Cyberspace. Copyright Law in a New World, página Web en Internet: http://mitpress.mit..edu/

DAVARA, M. A.: Derecho Informáhco. Pamplona: Aranzadi, 1993.

DAVARA, M. A.: De las Autopistas de la Información a la Sociedad Virtual. Pamplona: Aranzadi, 1996.

FEATHER, J.: The Information Society. London: Library Association Publishing, 1996.

JOYANES, L.: Cibersociedad. Los retos sociales ante un nuevo mundo digital. Madrid: McGraw Hill, 1997.

JOYANES. L.: CIBERSOCIEDAD . ¿Realidad o utopía?. Madrid: UPSA Madrid, 1996.

JOYANES, L.: Cibersociedad Implicaciones ético-sociales de la sociedad digital del siglo XXI. . Madrid: UPSA. Libro de actas del III Congreso Internacional Ethicomp'96.

JOYANES, L.: "Cambio tecnológico y nueva sociedad de la información" en Cuademos de Realidades Sociales, Madrid, nn. 49-50, 1997.

PÉREZ-LUÑO, A. E.: Manual de informática y derecho. Barcelona: Ariel, 1996.

PESO, E. y RAMOS, M. A.: Confidencialidad y seguridad de la información: La LORTAD y sus implicaciones socioeconómicas. Madrid: Díaz de Santos, 1994.

LEGISLACIÓN

1.Propuesta de directiva del Consejo de las Comunidades Europeas 92/c 156/03 de 15 de abril de 1992 relativa a la protección jurídica de las bases de datos (COM (92) 24 final-Syn 393)

2.Ley sobre la protección Jurídica de programas de ordenador; Ley 16/1993, de 23 de diciembre; de incorporación al derecho español de la directiva 91/250/CEE de 14 de mayo de 1991.

3.Ley 22/1987, de 11 de noviembre, de propiedad intelectual BOE núm. 275, de 17 de noviembre de 1987.

4.La constitución Española de 29 de diciembre de 1978, artículo 20.

5.Ley Orgánica 5/1992 de 29 de octubre de regulación del tratamiento automatizado de los datos de carácter personal. BOE de 31 de octubre de 1992.

6.Real decreto 428/1993, de 26 de marzo, por el que se aprueba el estatuto de la agencia de protección de datos. (BOE de 4 de mayo de 1993).

BIBLIOWEB (Referencias electrónicas: URLs)

The European Information Society.
http://www.ispo.cec.be/infosoc

Comisión Europea (Representación en España).
http://www.uji.es/euroinfo

Electronic Frontier Foundation.
http://www.eff.org

Organización Mundial de la Propiedad Intelectual.
http://www.ompi.org

Propiedad intelectual en el ciberespacio.
http://www.mitpress.mit.edu/
http://www.ustpo.gov/web/ipnii/

National Science Foundation.
http://www. nsf.gov

Fundesco.
http://fundesco.es

Rivas y Rodríguez (abogados) - Legislación
http://www.asertel.es/cs/leyes.htm
http://www.onet.es

Law Journal
http://www.ljx.com/

Estudio Legal. Wells, St. John, Roberts, Gregory & Matkin P.S.
http://www.ior.com/~malhotra/copy.html

Dimensión Jurídica de la Protección Criptológica de la Información

JOSÉ MARIA MOLINA

Secretario de la Asociación Española de Criptología

1.-INTRODUCCIÓN.

El Estado como conjunto de poderes públicos ejerce un poder que garantiza la convivencia de los ciudadanos y la integridad del territorio en el que se asienta, que limita su orden jurídico.

La función básica del Estado es la ordenación de la sociedad mediante el Derecho.

El dato o conjunto de datos elaborados y orientados para la consecución de un fin, medio para la obtención del saber, es la información. Instrumento valioso para el ejercicio del poder a lo largo de la historia.

Pero no toda información es poder; incluso en determinadas circunstancias, un exceso de información puede constituir una amenaza para el conocimiento.

La necesidad de un tratamiento abundante de información con garantías de rapidez y fidelidad ha encontrado la respuesta en la moderna tecnología que se ocupa del proceso y almacenamiento de informaciones mediante soportes

automatizados: la informática. La transmisión de datos a distancia mediante redes determinó la aparición de la telemática.

Ninguna organización resultará más vulnerable a la pérdida de su activo de conocimiento que las que incorporen más conocimiento. Igualmente ocurren con las tecnologías de la información, lo que conlleva una necesidad de seguridad directamente proporcional a la naturaleza de ambas realidades.

En la seguridad de la información y las comunicaciones el medio históricamente más eficaz y preponderante de los que intervienen en la misma es el derivado de la aplicación de la Criptología como forma de ocultación, disimulo o cifrado de la información.

La fuerza latente y consiguientemente, el riesgo que subyace en la pérdida o alteración de la información, amplificado por su abundante tratamiento, almacenaje y transmisión derivada de la aplicación de las nuevas tecnologías, requiere protección y demanda instrumentos que garanticen su seguridad.

En este sentido la seguridad de la información y la Criptología como elemento esencial de la misma, actúan como coadyuvantes del poder de la información, que como todo poder, ha de ser juridificado.

Tanto el derecho como el poder son principios reguladores de la acción social, ambos son interdependientes y complementarios. La combinación de estos dos factores de ordenación constituye la esencia de lo que se ha denominado el "arte de la política".

De otra parte, el Estado como toda organización, tiene una primera exigencia ética: procurar su propia subsistencia, lo que logra a través de la ordenación de la convivencia y garantía de su integridad mediante el Derecho.

En todo ello tiene una incidencia directa y determinante las Nuevas Tecnologías de la Información y concretamente la Informática.

Información, política, poder, derecho y tecnología son conceptos que, actualmente, aparecen en íntima conexión. Su interelación se puede ver en la aplicación de la Criptología.

En una sociedad basada en la información y el conocimiento, presidida por la tecnología y, en concreto, en cualquier ámbito relacional cibernético, la Criptología se puede considerar como un "instrumento de ordenación", que posibilita una ordenada convivencia en el mundo de las redes telemáticas.

La paz del Estado o de cualquier otra organización puede verse amenazada por egoismos individuales, intereses de determinados grupos, o por egoismos de otros estados u organizaciones, mediante la destrucción o confusión de los sistemas de tratamiento de información de los adversarios o competidores y la protección de los propios, en una pluralidad de grados e intensidades que pueden llegar, a desequilibrar la balanza competitiva, afectar al tráfico jurídico, alterar la libre competencia, atentar contra derechos y libertades o afectar a la estabilidad, pudiendo llegar, incluso, a poner en peligro la propia existencia del estado u organización a que se refiera.

Grados e intensidades de amenazas que exigen un correlativo de protección y que aplicado a la seguridad de la información nos situaría en los distintos niveles de exigencia criptológica.

2.- CRIPTOLOGÍA Y DERECHO.

El uso, no uso, o utilización inadecuada de la Criptología como instrumento para la ocultación de información, produce efectos que pueden redundar en la protección de derechos fundamentales, también puede incidir en las libertades de expresión e información, en la averiguación y prevención del delito e incluso afectar a los Derechos Humanos.

La protección criptológica concreta que se utilice en una determinada organización ha de ser el resultado de la consideración previa, de una serie de parámetros relacionados con la importancia que se dé al activo de información y conocimiento, -y concretamente a la dimensión de su protección-, las posibilidades reales de poder gestionarlo de una u otra forma, combinado con la conveniencia de hacerlo de determinada manera, atendiendo al conjunto de circunstrancias internas y externas, y utilizando los medios tecnológicos disponibles en el momento histórico a que se refiera.

Las consecuencias para el ciudadano y sus derechos individuales, para la Sociedad y para el Estado de abordar la protección criptológica de la información

de una u otra forma, hace que la seguridad de la información sea un tema político esencial a nivel mundial y demanda su regulación jurídica que permita el juego conjunto de Individuo, Sociedad y Estado, en armónica combinación dentro de los sistemas democráticos avanzados.

2.1.- La información en la Constitución Española de 1.978.

La Criptología es un instrumento para hacer eficaz un mandato jurídico, que determina la confidencialidad de la información a que se refiera. Por ello, como paso previo, es oportuno hacer una breve reflexión sobre la situación de la información desde una perspectiva nuestra Carta Magna, como referente supremo del ordenamiento jurídico.

Comunmente se habla de información y de su necesidad de ser protegida casí como una consecuencia obvia de su naturaleza y el imperativo de los tiempos. Pero no toda información tiene la misma consideración, ni toda información necesita ser protegida de igual forma. Diferente es la fundamentación jurídica que da soporte a la protección de la información pública y de la información privada.

La transparencia de las informaciones públicas es consustancial con los regímenes democráticos, existiendo una profunda vinculación entre el principio de publicidad de las decisiones gubernamentales y los propios fundamentos de la democracia que, como forma de gobierno, excluye por principio la opacidad de las decisiones.

Junto a una transparencia de los asuntos de gobierno, existen restricciones justificadas, dirigidas a la preservación de los intereses generales, que operan con un caracter excepcional y como límites de la misma.

Ambos principios, el de transparencia y opacidad conviven en tensión permanente y cuyo resultado ideal debería ser el punto crítico de equilibrio entre la publicidad o transparencia como normal general y el impresindible secreto en determinados casos y asuntos concretos.

Partiendo de la base de que el secreto, aplicado a los asuntos públicos, es un concepto negativo, por suponer una renuncia a las exigencias de la democracia, se ha de caminar, hacia el secreto estrictamente necesario.

Los principios y valores constitucionales son incompatibles con las interpretaciones restrictivas de la transparencia de las acciones gubernamentales y consiguiente relegación del secreto.

Las libertades de expresión e información son derechos fundamentales en el mundo actual y nuestra Constitución las recoge en el artículo 20.

Pero estas libertades no pueden ser consideradas de naturaleza supraconstitucional e ilimitadas. Todo derecho tiene sus límites que se derivan de forma indirecta de la propia Constitución y que han de justificarse por la necesidad de proteger, o preservar, otros bienes constitucionalmente protegidos, como el honor, la intimidad ,la propia imagen o la protección de la juventud y de la infancia.

Los límites referidos a la seguridad del Estado no están expresamente recogidos en el artículo 20, pero su derivación implícita, consecuencia de la consideración de la seguridad estatal como presupuesto del Estado de derecho y, por tanto, de la efectividad de las libertades, se aprecia en la interpretación conjunto del artículo 20, en relación el el artículo 10.2 y el 105, b), todos ellos de la Constitución.

Por cuanto se refiere a la información privada, los grandes efectos producidos por aplicación de las nuevas tecnologías de la información y las comunicaciones y su utilización masiva, sitúan en posición de vulnerabilidad al ciudadano y las organizaciones que lo integran. A lo que los ordenamientos jurídicos responden con la figura del secr4eto de las comunicaciones.

El secreto de las comunicaciones en nuestro ordenamiento jurídico se configura como una garantía de los particulares de que su esfera de libertad debe ser respetada por los poderes públicos.

El artículo 18 de la Constitución, dedicado a regular en general la intimidad de las personas como derecho fundamental, dedica su apartado 3, a garantizar el secreto de las comunicaciones y dice:

"Se garantiza el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial".

La seguridad de las comunicaciones es el auténtico talón de Aquiles de la sociedad de la información. La consideración de la seguridad de la información, en sí misma, como un bien jurídico protegible se empieza a abrir camino entre la doctrina.

El secreto de las comunicaciones está referido sólo a las comunicaciones privadas y tiene un carácter "formal", en el sentido de que se predica de lo comunicado (STC 114/1.984, de 29 de noviembre).

Y aunque el precepto constitucional subraya especialmente las postales, telegráficas y telefónicas, tiene un carácter omnicomprensivo y es aplicable a cualquier medio o servicio que sirva para la transmisión de las mismas.

De todo lo indicado y de la literalidad de los artículos 20 y 18.3 de la Constitución se deriva que en la información pública el principio general es la transparencia y la excepción el secreto, mientras que en la información privada el principio general es el secreto y la excepción la transparencia. De donde deviene una protección sistemática de las comunicaciones privadas y excepcional de las públicas.

Para que este secreto sea real y efectivo se requiere además, una protección criptológica al nivel adecuado que así lo gartantice.

2.2.- Protección criptológica y LORTAD.

De la simbiosis entre informática y comunicaciones surge una nueva relación entre datos y personas que necesita una protección con mayor profundidad que la intimidad.

La Ley Orgánica número 5/1.992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de carácter personal, comunmente conocida como LORTAD, viene a dar respuesta al mandato constitucional del artículo 18.4 de la Constitución, dirigido a la limitación del uso de la informática para garantizar el honor, la intimidad personal y familiar de los ciudadanos y el legítimo ejercicio de sus derechos.

La Ley, limitadora del uso de la informática, en lo concerniente al ámbito de los "ficheros de datos" de carácter personal, considera que su existencia y utilización supone un riesgo para los derechos de la personalidad.

Trata de prevenir violaciones de la privacidad, derivadas del tratamiento de datos considerados como una globalidad de procesos informáticos.

La adopción de las medidas de seguridad necesarias, dentro del marco reglamentario respecto a las condiciones de integridad y de seguridad corresponden al responsable del fichero.

la Criptología tiene su aplicación en hacer efectivo el mandato legal, dentro de las medidas de seguridad y en unión de otros procedimientos.

La Ley recoge una serie de principios de protección de datos, pero no recoge suficientemente los mecanismos para una protección efectiva. No contempla la seguridad en la transmisión de datos, con los problemas que implican las comunicaciones y su vulnerabilidad.

El artículo 9 de la LORTAD, referido a la seguridad de los datos, dice:

"1.- El responsable del fichero deberá adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal 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.

2.- No se registrarán datos de carácter personal en ficheros automatizados que no reunan las condiciones que se determinen por via reglamentaria con respecto a su integridad y seguridad y a las de los centros de tratamiento, locales, equipos, sistemas y programas.

3.- Reglamentariamente se establecerán los requisitos y condiciones que deban reunir los ficheros automatizados y las personas que intervengan en el tratamiento automatizado de los datos a que se refiere el artículo 7 de la ley".

En un futuro Reglamento se deberá contener los distintos niveles de protección y las medidas específicas de seguridad, entre ellas las de naturaleza criptológica.

Pero la Criptología tiene múltiples y variadas aplicaciones, partiendo de su condición de tecnología de doble uso para utilización civil y militar, pasando por su repercusión en la libertad informática o sus efectos en la contratación electrónica y firma digital y, en definitiva, las consecuencias para usuarios y consumidores.

2.3.- Criptología y libertad informática.

La libertad informática tiene su orígen en el "derecho de autodeterminación informativa" surgido de la Sentencia de 13 de abril de 1.983, del Tribnal Constitucional alemán, sobre la Ley del Censo de Población, cuya evolución ha venido a configurar el concepto de "libertad informática" como hoy se entiende: libertad de controlar el uso de los propios datos, como un "habeas data", derecho de puesta al día, rectificación y exactitud, derecho de secreto para los datos "sensibles" o derecho de autorización para su difusión.

Será la dimensión de la libertad informática relativa al secreto de los datos sensibles el punto de mayor conexión con la Criptología, al configurar el secreto del dato sensible un ámbito de confidencialidad que necesita ser protegido de forma eficaz, tarea que corresponde a la Criptología.

Dado el caracter omnicomprensivo del secreto de las comunicaciones recogido en el artículo 18.3 de la Constitución, las comunicaciones telemáticas han de considerarse amparadas por el mismo, lo que viene a reforzar el secreto del dato sensible, propio de la libertad informática, y constituir un plus de confidencialidad.

2.4.- La Criptología como medida de prevención.

La protección y seguridad de la información se puede conseguir con la aplicación de medidas de naturaleza física, lógica, organizativa, legal, criptológica... Entre ellas, las medidas jurídicas tienen como carácterística que ofrecen una protección que actúa "a posteriori" y que dada la naturaleza de la información y las características de las nuevas tecnologías sobre las que opera la informática, resultan insuficiente, al ser irreversible el daño causado.

La seguridad de la información, para que sea eficaz, necesita medidas que "a priori" impidan el exito de las amenazas contra la información.

La plenitud del ordenamiento jurídico exige que, además de la protección jurídica se disponga de mecanismos que garanticen de forma eficaz, en determinadas circunstancias, las consecuencia irreparables de eventuales violaciones, lo que se lleva a cabo a través de las medidas de prevención.

Estas medidas requieren además de una eficacia operativa, un soporte jurídico legitimador de su aplicación.

La Sentencia del Tribunal Supremo de 10 de diciembre de 1.980 dice que "La protección de los derechos no se contrae a la reparación de los perjuicios originados, sino que han de extenderse a las medidas de prevención que razonablemente impidan ulteriores lesiones".

La Ley Orgánica 1/1.982, de 5 de mayo, de Protección Civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen dice que la tutela judicial frente a las intromisiones ilegítimas, -entre las que están el emplazamiento de cualquier aparato para grabar o reproducir la vida íntima de las peronas-, "comprenderá la adoptación de todas las medidas necesaria para poner fín a la intromisión ilegítima de que se trate y restablecer al perjudicado en el pleno disfrute de sus derechos, así como para prevenir o impedir intromisiones ulteriores". (art. 9.2).

De igual modo se habla de medidas de prevención en la Ley 9/1.968, de 5 de abril, sobre Secretos Oficiales, modificada por la Ley 48/1.978, de 7 de octubre y Reglamento de Secretos Oficiales aprobado por Decreto 242/69, de 20 de febrero.

La Criptología como instrumento esencial de protección de la información es una medida de prevención para el cumplimiento real y efectivo de determinados derechos, preservación de legítimos intereses y garantía de libertades.

3.-DEONTOLOGÍA CRIPTOLOGICA.

El uso de la Criptología como medida de prevención, no ha de aplicarse a ultranza convencidos de que cuanto más criptología mejor.

El uso de la Criptología a un nivel determinado en un ámbito concreto viene determinado por la necesidad de protección; la cual, a su vez, tiene su origen en el peligro de violación de la información a que se refiera.

La Criptología como instrumento para la ocultación de la información no es inócua. Utilizada de forma abusiva o fraudulenta, puede no solo atentar contra

la libertad de información, sino contribuir a la creación de una atmosfera cargada de secretismo, porpiciando una cultura de opacidad radicalmente incompatible con la transparencia que exige una sociedad democrática, llegando incluso a obstaculizar el norma funciomaiento de la sociedad y del Estado, a través de la creación de reductos impenetrables.

En esa difusa frontera entre valoración de información, niveles de protección y complejidad tecnológica, el papel de la ética ocupa un lugar destacado.

Pero en la estructura de convivencia cibernética donde está presente la Criptología, el papel de la ética debe verse reforzado por acuerdos deontológicos que como códigos de conducta sean aceptados por la sociedad con su propia fuerza vinculante.

La proporcionalidad ha de presidir cualquier proceso de protección y será un indicativo no solo de eficacia, sino de salud social.

El Teletrabajo

EMILIO SUÑÉ LLINÁS

Profesor Titular de la Facultad de Derecho de la Universidad Complutense de Madrid

1.- CONCEPTO, NATURALEZA Y CLASES.

1.1.- Concepto de teletrabajo.

El teletrabajo ha sido definido en un informe de la Comisión Europea, de la siguiente forma: *La palabra "teletrabajo" designa aquellas actividades ejercidas lejos de la sede de la empresa (se le denomina también en ocasiones trabajo a distancia), a través de la comunicación diferida o directa por medio de las nuevas tecnologías*[1].

Esta definición es aproximativa, puesto que existen muchas variantes de teletrabajo, cada una con sus peculiaridades específicas, a las que se aludirá en la clasificación.

Una definición más prolija, que acaso revista más las características de

[1] "Le travail à domicile dans l' Union Europeenne". Rapport du groupe de travail ad hoc. Rapporteur Jane Tate. Ed. Comisión Europea (D.G. de Empleo, Relaciones Industriales y Asuntos Sociales).

una descripción, se ofrece en la obra que lleva por título *"El Teletrabajo"*[2]. Es la siguiente:

"El teletrabajo es una forma flexible de organización del trabajo, que consiste en el desempeño de la actividad profesional sin la presencia física del trabajador en la empresa durante una parte importante de su horario laboral. Engloba una amplia gama de actividades y puede realizarse a tiempo completo o parcial. La actividad profesional en el teletrabajo implica el uso frecuente de métodos de procesamiento electrónico de información, y el uso permanente de algún medio de telecomunicación para el contacto entre el trabajador y la empresa".

En el mismo libro se recoge una ingeniosa (aunque no exacta) definición de uno de los pioneros en el estudio del teletrabajo. Se trata de Jack NILLES, cuando decía que *"el teletrabajo es la posibilidad de enviar el trabajo al trabajador, en lugar de enviar el trabajador al trabajo"*. Tal definición responde genéricamente al trabajo a domicilio, y aún más, al trabajo a distancia, cualquiera que sea su forma.

ORTIZ CHAPARRO ofrece también una definición muy breve, sin los tintes humorísticos de la de NILLES, pero sin duda más exacta. Dice: *"Teletrabajo es trabajo a distancia, utilizando las telecomunicaciones y por cuenta ajena"*[3]. Pese a la brevedad, tal definición es todavía larga en exceso, puesto que la idea de trabajo por *cuenta ajena* no es inherente al teletrabajo, como enseguida se verá, al hacer referencia a la naturaleza jurídica de las relaciones de teletrabajo.

1.2.- Naturaleza jurídica del teletrabajo.

Lo más normal es que estemos en presencia de una relación laboral como otra cualquiera, al cumplirse ordinariamente los requisitos del artículo 1.1 del Texto Refundido del Estatuto de los Trabajadores, que literalmente dispone:

La presente ley será de aplicación a los trabajadores que voluntariamente presten sus servicios retribuidos por cuenta ajena y dentro del ámbito de organización y dirección de otra

■[2] GRAY, M.; HODSON, N.; GORDON, G. Y OTROS: "El Teletrabajo". Ed. BT Telecomunicaciones, ECTF y Fundación Universidad Empresa, Madrid, 1995.

■[3] ORTIZ CHAPARRO, F.: "El teletrabajo. Una nueva sociedad laboral en la era de la tecnología". Ed. McGraw&Hill, Madrid, 1995. Pág. 38.

persona, física o jurídica, denominada empleador o empresario.

Cuestión distinta es la dificultad de prueba que reviste la existencia de dicha relación laboral, puesto que las empresas normalmente preferirán contratos con los teletrabajadores, bajo la forma de una estricta relación mercantil entre la empresa contratista y un trabajador autónomo, que sería el teletrabajador. Ahí está precisamente uno de los principales problemas del teletrabajo, puesto que escapa con facilidad del marco de las relaciones laborales, y en este sentido es una vía para que más y más relaciones jurídicas de arrendamiento de servicios e incluso de obra, se inscriban en el marco civil/mercantil y no en el laboral, lo que concita un razonable recelo de las organizaciones sindicales hacia el teletrabajo.

En todo caso, conviene curarse en salud frente a los prejuicios de cualquier signo, que suelen ser abundantes, ante el teletrabajo. Como dice muy bien ORTIZ CHAPARRO[4], "el teletrabajo *sólo es una forma de trabajo* determinada. Por lo tanto, no es paro, trabajo *basura* ni subempleo, pero tampoco tiene por qué ser milagro".

1.3.- Clases de teletrabajo.

Más adelante se entrará con mayor grado de detalle en la problemática específica del teletrabajo, en cuanto relación laboral. Ahora corresponde terminar la presente introducción, con una referencia a las clases de teletrabajo, lo cual permite hacerse una idea clara acerca de la complejidad (y variedad) de naturaleza jurídica de las relaciones de teletrabajo.

Personalmente soy poco partidario de las clasificaciones, salvo que se revelen útiles para la determinación del Derecho aplicable a determinada institución. Desde este punto de vista, habría que distinguir las siguientes variedades de teletrabajo:

a) Relación laboral.
b) Arrendamiento de servicios o de obra civil.
c) Como forma de organización interna empresarial.
d) En cuanto forma de organización interempresarial.

■[4] ORTIZ CHAPARRO, F. Op. cit. Pág. XVI

Por el momento ya se han efectuado suficientes referencias a las variedades señaladas con las letras a) y b). Por lo que se refiere a la c); es decir, al teletrabajo como forma de organización interna empresarial, puede permitir la descentralización de determinadas actividades, lo que no supone más que su realización en centros de trabajo de una empresa, distintos de su sede principal. Por lo que se refiere a la variante d), relativa al teletrabajo en cuanto forma de organización interempresarial, en realidad escapa al concepto mismo de teletrabajo, puesto que se refiere a las conexiones telemáticas entre empresas, en cuanto forma de colaboración, mediante el intercambio electrónico de datos que permite, por asociación, una mayor competitividad de las PYMEs, frente a las grandes empresas; si bien, en este caso, estamos más en presencia de telesocios, que de teletrabajo propiamente dicho.

Si atendemos a otro criterio clasificatorio, el del *lugar donde el teletrabajo se desarrolla*, habremos de distinguir dos grandes formas, que son el *teletrabajo a domicilio* y el *teletrabajo prestado a través de telecentros*. Todo ello sin perjuicio de que también exista un *teletrabajo móvil*, que además va a ir *in crescendo*, a medida que arraiguen los entornos de comunicaciones personales, basados en la combinación de la informática multimedia, con las telecomunicaciones móviles.

-Por lo que se refiere al teletrabajo a domicilio, hay que señalar de nuevo la existencia de variantes, en las que se observa el entrecruzamiento entre las relaciones laborales y las mercantiles. Las principales variantes son las siguientes:

Teletrabajo a tiempo completo y para un solo empresario. Este supuesto se inserta en el ámbito de las relaciones laborales. Es una variante muy indicada para trabajos administrativos de no muy alta cualificación, como el proceso de textos, grabación de datos, atención de llamadas telefónicas, etc.

Empleados que prestan a domicilio una parte de su trabajo. Se trata sin duda de una relación laboral, cada vez más en boga y que afecta incluso a altos ejecutivos. En el fondo profundiza la tendencia a la flexibilidad en la prestación de trabajo, que comenzó en la jornada y ahora sigue en extremos tales como la prestación de parte de la misma en el propio domicilio, posibilidad que se hace más factible gracias al avance tecnológico, al teletrabajo en suma.

Teletrabajo *"free-lance"*. Lo practican aquellos teletrabajadores que se ponen al servicio de varios clientes. Sin descartar que en algún caso muy concreto

la relación pueda ser de naturaleza laboral, lo normal es que se configure bajo la forma de arrendamientos de servicios o de obra sujetos al Derecho Civil/Mercantil, en los que el teletrabajador es un empresario autónomo.

-Teletrabajo prestado a través de telecentros. Los telecentros, como su nombre indica, son centros de teletrabajo, que se instalan preferentemente en las zonas rurales, a fin de contrarrestar el proceso de abandono del medio rural, que propicia el carácter urbano de la economía productiva moderna. Las modernas tecnologías y fenómenos con ellas asociados, como el amplísimo desarrollo de los sectores terciario y cuaternario, así como la posibilidad del teletrabajo, permiten contrarrestar el clásico fenómeno de la despoblación rural, sobre todo cuando se concentran los medios tecnológicos que facilitan el teletrabajo en los referidos telecentros. Se trata de iniciativas que han tenido mucho éxito en los Países Nórdicos y que por el interés público que supone la conservación del medio rural, están siendo apoyadas por los Estados y por la Unión Europea.

A nivel terminológico los telecentros de ámbitos rurales, se suelen denominar *telecottages*, mientras que los centros de teletrabajo pertenecientes a una sola empresa que descentraliza su actividad por este procedimiento, se suelen denominar *oficinas-satélite*. No cabe olvidar tampoco que los modernos edificios de oficinas de alquiler, cuentan con una dotación de servicios de tratamiento de la información y de telecomunicaciones, que los convierte a su vez en telecentros.

Para concluir diré que tengo para mi que aún cuando los telecentros han contribuido, sin duda, al desarrollo inicial del teletrabajo, no son hoy indispensables, en la medida en que la disminución del coste de la tecnología, y sobre todo de las telecomunicaciones, no les otorga ya ventajas tan apreciables, sobre el desarrollo del teletrabajo en el propio domicilio del teletrabajador.

-El teletrabajo móvil tiene gran importancia para el personal dedicado a actividades de mantenimiento, inspección y, por supuesto, ventas. En esta última actividad se observa, de nuevo, la dificultad de separar lo laboral de lo mercantil, puesto que la venta móvil, que puede incrementar su eficacia con un adecuado sistema de telecomunicaciones, se lleva a cabo por representantes de comercio, en cuyo estatuto jurídico se ha producido, tradicionalmente, un difícil deslinde entre lo propiamente mercantil y lo laboral. En el informe sobre el teletrabajo,

publicado por la D.G. Vª de la Comisión Europea[5], a modo de complemento del Libro Blanco de DELORS[6] sobre *Crecimiento, Competitividad y Empleo,* se precisa que en los Estados Unidos, año 1994, siete millones de personas podían ser calificadas como "trabajadores móviles", mientras que en el ya muy próximo año 2000, se espera que dicha cifra ascienda a veinticinco millones de personas.

2.- PROS Y CONTRAS DEL TELETRABAJO.

2.1.- Ventajas del teletrabajo.

Algunas de las principales ventajas del teletrabajo han sido enumeradas por DI MARTINO y WIRTH[7], en un interesante artículo sobre la cuestión, cuya enumeración se adoptará como punto de partida para el presente estudio:

-Flexibilidad y economía de costes en la empresa. Me veo en la obligación de matizar, no obstante, que este *pro*, lleva aparejado un *contra*, y es que tales ventajas para la empresa se construyen a menudo sobre la precariedad de los trabajadores, puesto que al escapar el teletrabajo, con mayor facilidad, del Derecho Social, en esta misma medida y sólo en ella, interesa a muchas empresas. Con el teletrabajo hay un riesgo cierto de crear nuevas bolsas de *trabajadores de segunda* y de potenciar discriminaciones tradicionales, como las de mujeres y discapacitados. El tema es muy complejo y, en el curso del presente estudio se volverá sobre el mismo. Por ahora adelanto que el recurso al teletrabajo como forma de escapar al Derecho Social es difícil de evitar, sobre todo habida cuenta de que el teletrabajo está propiciando una nueva redistribución del trabajo a nivel planetario, contra la que no es fácil luchar. La excesiva insistencia en sujetar las

■[5] "Suivi du livre blanc. Le télétravail. Le secteur informel". En Europe Sociale, suplemento 3. Luxemburgo, 1995.

■[6] Jacques DELORS fue uno de los pioneros en el estudio del teletrabajo. Según comenta Alain VEYRET, en noviembre de 1980, DELORS, por entonces Director del Centro de Investigación Trabajo y Sociedad de la Universidad París Dauphine, ya había visto en el teletrabajo una fórmula para impulsar el reequilibrio territorial en Francia.

■[7] DI MARTINO, V. y WIRTH, L.: "Teletrabajo: Un nuevo modo de trabajo y de vida". En Revista Internacional del Trabajo, vol. 109, 1990, nº 4.

relaciones con los teletrabajadores nacionales al Derecho Laboral, puede propiciar el empleo de teletrabajadores de países en vías de desarrollo, con la consiguiente generación de desempleo en el propio Estado.

-Aumentos de la productividad. Como señalan los referidos DI MARTINO y WIRTH: *"Estos aumentos se atribuyen a la inexistencia de interrupciones y a una mejor concentración; a un incremento de la motivación y la satisfacción en el trabajo; a una entrega y disposición de ánimo superiores; y a un suplemento de energía en el trabajo gracias a la ausencia de tiempo perdido y de la tensión provocada por los desplazamientos cotidianos"*. El panorama idílico descrito por DI MARTINO y WIRTH, quienes destacan los *pros*, pero no los *contras* del teletrabajo, ha de ser matizado en el sentido de que el teletrabajo en buena medida aumenta la productividad a cuenta de la desprotección social y del *stress* (asimismo comprobado) de madres de familia que no tienen otra forma razonable de trabajar, al menos de forma compatible con el cuidado de los hijos.

Más allá de lo expresado por DI MARTINO y WIRTH, la importancia de los aumentos de productividad debidos al teletrabajo es trascendental, pues uno de los grandes problemas de la sociedad postindustrial, es que hasta el momento no se ha dado una *revolución de la productividad* análoga a la que derivó de la aplicación de los esquemas manageriales tylorianos, al sistema fabril propio de las sociedades de *segunda ola*. El crecimiento continuo que posibilitó aquella *revolución de la productividad*, que a su vez hizo posible destinar amplios excedentes a la cobertura de necesidades sociales, no se ha reproducido hasta ahora en el sector terciario, característico de la sociedad postindustrial, hasta el punto de que DRUCKER ha llegado a afirmar que *"el nuevo reto al que se enfrenta la sociedad capitalista es la productividad de los trabajadores del saber y de los servicios"*[8].

Aún cuando las cifras adolecen de un importante grado de imprecisión, los aumentos de productividad asociados al teletrabajo oscilan alrededor del 30%; de ahí que importantes multinacionales, como ATT, Pacific Bell, British Telecom, IBM Rank Xerox, o ICL, entre muchas otras, hayan apostado decididamente por el teletrabajo, que no para de extenderse por importantes sectores de la economía, ajenos a la informática y las telecomunicaciones, tales como banca, seguros, ventas, consultoría, formación, editorial, etc.; todo ello por no hablar de las

[8] DRUCKER, P. F.: "La sociedad postcapitalista". Ed. Apóstrofe, Barcelona, 1993. Pág. 89.

experiencias de teletrabajo en el seno de la Administración Pública, que se ha producido tanto en los Estados Unidos, como en los países más emblemáticos de la Unión Europea.

-Facilita la contratación y conservación del personal. Así por ejemplo, dicen los autores citados que permite retener a trabajadores que se plantean la posibilidad de dejar de trabajar, como algunas mujeres una vez que han sido madres, o insertar en el mercado laboral a trabajadores con pocas posibilidades de desplazamiento, como los que viven en zonas rurales. Igualmente se puede plantear como un *puente*, transitorio o no, para los trabajadores que desean independizarse, sin que ello suponga una radical desvinculación de su anterior empresa.

-Empleo para los minusválidos. Es cierto que incrementa sus posibilidades de encontrar trabajo; pero también lo es, en mi opinión, que ello fomenta una clara tendencia a hacer del teletrabajo un *ghetto* para trabajadores se *segunda categoría*, en el que se concentrarían minusválidos físicos y amas de casa. En mi opinión el teletrabajo es muy positivo, a condición de que se adopten las medidas necesarias para contrarrestar, en lo posible sus efectos marginalizantes, para determinadas capas de la población.

-Desarrollo rural. Sin duda el teletrabajo permite compatibilizar la residencia en el medio rural, con el desempeño de múltiples trabajos en los sectores terciario y cuaternario. Sobre este extremo existe un breve artículo de FRANCESCH y BARRERA[9], vinculados el primero a la Xunta de Galicia y el segundo al Foro del Teletrabajo de la Comisión Europea, en el que se da cuenta del proyecto de creación de un telecentro, en los municipios de Silleda-Vila de Cruces, en el marco del proyecto SABRE de la Unión Europea. Por lo demás, he de apostillar que el teletrabajo, al vincularse al desarrollo rural, tiene una importancia medioambiental máxima, al evitar la despoblación de tales zonas.

-Reducción del tiempo de desplazamiento. Es una ventaja evidente. Y debo apostillar que añade otros puntos positivos de orden ecológico, al exigir un menor consumo de energía. El efecto ecológico de la extensión del teletrabajo es

[9] FRANCESCH, O. y BARRERA, E.: "Teletrabajo y desarrollo rural". En la revista El Campo, 1993.

ciertamente significativo, en cuanto a reducir las emisiones de CO^2, que es el causante del efecto invernadero. En el libro de GRAY, HODSON y GORDON, se cita un párrafo de un discurso de George BUSH, del año 1990, muy significativo sobre las causas del impulso del teletrabajo, por parte de la Administración USA: *"Veinte minutos diarios de desplazamiento hacia y desde la oficina suponen al cabo del año la pérdida en la carretera de dos semanas estresantes de 40 horas laborables cada una. Si el 5% de los trabajadores que se desplazan diariamente en Los Angeles lo hicieran un solo día a la semana, se ahorrarían 205 millones de millas de viaje al año y se evitaría que 47.000 toneladas de productos contaminantes entraran en la atmósfera. El teledesplazamiento supone, pues, un ahorro de energía, una mejora de la calidad del aire y un aumento de la calidad de vida. No es un mal negocio".*

Datos parecidos, en este caso relativos a Madrid (1992), figuran en el proyecto TELEURBA, de la D.G. XIII de la Unión Europea. Se estima que si el 5% de la población madrileña empleada en el sector de la información y del conocimiento, practicase el teletrabajo, dejarían de emitirse 800 toneladas de gases contaminantes a la atmósfera y se ahorrarían 215.000 millones de pesetas, en cuanto coste del tiempo que se pierde en desplazamientos.

La positiva correlación entre teletrabajo, calidad de vida en las ciudades y medio ambiente, se extiende a otros aspectos, tales como la mejora de imagen de las empresas que lo adoptan, precisamente por su favorable repercusión ambiental, o la desaceleración en las necesidades de construcción de nuevas infraestructuas, para los transportes urbanos e interurbanos.

-Flexibilidad de la jornada laboral de los teletrabajadores. Sin duda se trata de una ventaja, que se da tanto más cuanto mayor es la cualificación de los teletrabajadores.

-Otros puntos positivos no referenciados por los autores aludidos, son la reducción de los costes fijos de la empresa, y de los gastos del propio teletrabajador, la menor repercusión de situaciones externas graves, como huelgas del transporte, etc. Veamos algunos de ellos:

-Reducción del tamaño de las oficinas. Si en Madrid, por ejemplo, en una zona céntrica, el coste del metro cuadrado de oficina, se sitúa alrededor de 250.000 ptas. y se estima que un trabajador medio ocupa 20 m^2, resulta que por cada trabajador que pase a régimen de teletrabajo, los costes de establecimiento disminuyen en 5 millones de pesetas, si es en propiedad, o en unas 500.000

ptas./año, aproximadamente, si el régimen es de alquiler. Es cierto que el teletrabajador también ocupa espacio en su propia casa, o que el espacio fuera del centro de las grandes ciudades, también tiene unos costes; pero ni mucho menos comparables a los anteriores.

-Menos gastos por parte del teletrabajador. No se trata sólo de ahorrar en gastos de desplazamiento, sino también en múltiples aspectos, que van desde el menor coste de las comidas o la reducción de exigencias en cuanto a vestimenta. Tales ahorros se estiman en aproximadamente un diez por ciento del salario bruto.

2.2.- Inconvenientes del teletrabajo.

Frente a los *pros* que se acaban de comentar, sobre todo al hilo de la obra de Vittorio DI MARTINO y Linda WIRTH, el teletrabajo tiene aspectos negativos igualmente numerosos. Aparte de los reseñados como contrapeso a las ventajas apuntadas por los autores referidos, cabe añadir los siguientes:

-Poca proclividad de los sindicatos. Lo que en si mismo es un inconveniente, pues todo aquello que en el ámbito laboral no cuente con el beneplácito de los sindicatos es problemático. Una de las posturas más radicales fue la expresada por la Confederación Alemana de Sindicatos en su 13° Congreso (1986), que llegó a postular la prohibición del *"trabajo a domicilio por ordenador"*. Los sindicatos achacan al teletrabajo el aislamiento del trabajador, lo que en el fondo se traduce en mayores dificultades para su sindicación tradicional. Sin duda es cierto; pero los sindicatos, al igual que las demás organizaciones sociales, también han de evolucionar para adaptarse a los nuevos retos de la sociedad de la información, de acuerdo con el viejo dicho: "*renovarse o morir*". Es importante, entre otras cosas, que también los sindicatos incorporen a su organización, las nuevas herramientas y posibilidades que ofrece la sociedad de la información. Para la mayor tranquilidad sindical, diré que en Dinamarca el nivel de afiliación sindical de los teletrabajadores, es idéntico al del resto de los empleados por cuenta ajena.

-Seguridad e higiene en el trabajo. Es un *handicap* compartido con las demás formas de trabajo a domicilio, puesto que en ocasiones las dependencias de la casa tienen un acondicionamiento escaso o nulo para el trabajo. Parece claro que en aquellas dependencias del propio domicilio donde se desarrolla teletrabajo, debiera estar autorizada a entrar la Inspección de Trabajo. El control de tales

actividades es importante, por cuanto que es difícil determinar incluso quién trabaja; si bien reitero que no se trata de problemas específicos del teletrabajo y ni siquiera se dan en todas las formas de éste. Son más bien *contras* del trabajo a domicilio en general, que están llamados a adquirir mayor amplitud, por la expansión del teletrabajo.

-Tendencia a potenciar la discriminación de sectores sociales desfavorecidos. En los países donde el teletrabajo a domicilio es usual, así como en general sucede con el trabajo a domicilio, lo usual es que en tales tareas, el 80% de la población ocupada pertenezca al sexo femenino. Es bien conocido que ello puede dar lugar a una tendencia a hacer del teletrabajo un *trabajo periférico*, a modo de una especie de *trabajo de segunda* para amas de casa, a partir de una cierta idea de complemento de ingresos, más que de salario igual. Un esquema parecido podría reproducirse con los minusválidos físicos. Es obvio que el Legislador y la Administración deben estar prevenidos y adoptar las medidas oportunas frente a posibles efectos indeseables del teletrabajo. De todas formas insisto que el teletrabajo, por si mismo es un avance con efectos globales claramente positivos. Sus mayores inconvenientes son los clásicos; pero por eso mismo conocidos y evitables, del trabajo a domicilio.

En el teletrabajo existe una peligrosa tendencia dual, en el sentido de que los efectos positivos tienden a acentuarse más en los profesionales de alta cualificación, mientras que los negativos aparecen con mayor frecuencia entre los trabajadores menos cualificados.

-Riesgo de discriminaciones laborales. No ya sólo en el clásico sentido salarial, sino también en otros, pues no cabe duda de que el alejamiento de los teletrabajadores de la sede física de la empresa, es un inconveniente para que se les aplique en condiciones de igualdad un sistema de promoción profesional y de recompensas materiales o morales por el trabajo bien hecho. La Dirección debe ser especialmente cuidadosa a este respecto. Otros aspectos críticos son la justicia en la asignación de tareas y la participación efectiva del teletrabajador en las ventajas sociales de la empresa.

-En general, tiene el riesgo de producir un aislamiento de los trabajadores; si bien en algunos casos, como en el teletrabajo móvil de los viajantes de comercio, se produce el efecto contrario de aumentar su vinculación a la empresa, al mejorar los medios de comunicación que tienen con la misma. En general, el inconveniente del aislamiento se reduce si se establece la obligación de

que el teletrabajador acuda con periodicidad regular a la sede de la empresa, lo que se debe aprovechar para convocar reuniones de equipos y, como muy bien precisa Francisco ORTIZ; para llevar a cabo actos *rituales* destinados a mantener viva la implicación recíproca entre el teletrabajador y la empresa.

-Difícil separación entre trabajo y vida privada.

-Necesario replanteamiento de los sistemas de gestión, sobre todo en cuanto a supervisión de recursos humanos. En la obra, ya citada, de GRAY, HODSON, GORDON y otros, se dan algunos interesantes consejos para la dirección a distancia, que en síntesis se resumen en asegurar un intercambio eficaz de información entre la empresa y sus teletrabajadores. Básicamente se trata de planificar los contactos, lo que tiene efectos positivos tales como el mantenimiento e intensificación del rendimiento de los teletrabajadores, así como impedir que éstos se sientan aislados, lo que refuerza el sentimiento de pertenencia y lealtad a la empresa. De hecho no hay ningún consejo especial, como no sea que se debe aprender a adaptar las actividades ordinarias de dirección y control al entorno del trabajo a distancia. Incluso permite a los managers aprender que tampoco en el trabajo de factoría pueden permitirse no controlar conscientemente los flujos de información, extremo que en demasiadas ocasiones pasa desapercibido.

En todo caso las viejas técnicas de Dirección y control por supervisión directa, se ven forzosamente desplazadas por la moderna Dirección por Objetivos, apta para controlar el trabajo a través de los resultados; así como por el desarrollo de sistemas teleinformáticos de control y el desplazamiento progresivo de las tradicionales formas jerárquicas de organización, a las nuevas formas de organización reticular o matricial. La vinculación del teletrabajo a la Dirección por objetivos, hace que su éxito dependa en buena medida de las aptitudes de la Dirección de la empresa para gestionarlo. En el fondo el teletrabajo requiere la potenciación de la mayor parte de las funciones de la Dirección, incluido su liderazgo.

Todo lo anterior tiene multitud de implicaciones, como la reducción de cargos intermedios, imprescindibles en formas tradicionales de organización jerárquica; pero superfluos en las modernas organizaciones reticulares.

De hecho, el teletrabajo condiciona la entera estructura laboral de la empresa, que al derivar hacia estructuras reticulares, disminuye el tamaño de su

organización física, tanto en cuanto a edificios, como por lo que hace referencia a personal. La tendencia apunta hacia una estructura más compleja, que directa o indirectamente afecta a los recursos humanos. El personal de oficina decrece, al tiempo que aumenta el teletrabajo en régimen laboral y el *outsourcing*, tanto con empresas subcontratadas, como con trabajadores (normalmente teletrabajadores) autónomos.

El teletrabajo también condiciona importantes cambios organizativos, en el sentido de introducir mayor racionalidad en el aprovechamiento del espacio físico de la empresa, que ya hemos visto como tiende a reducirse, pero también a utilizarse mejor. La presencia de los teletrabajadores en la empresa, sólo determinados días a la semana, condiciona que los espacios y recursos materiales y humanos a ellos asociados (personal de secretaría, p. e.), ya no se asignen *en propiedad*, sino que se convierten en recursos compartidos. Ello redunda en un nuevo inconveniente del teletrabajo, derivado de la pérdida de lo que muchos directivos mediocres, pero no por ello menos abundantes, consideran símbolos de *status*.

-El teletrabajo forma parte de una cultura de *tercera ola*, todavía no suficientemente arraigada. El teletrabajo no solo requiere de organizaciones innovadoras, sino que se basa muy directamente en la responsabilidad y autonomía del trabajador, así como en la flexibilidad de la prestación laboral. Son muchas cosas las que hace falta renovar, incluido lo que técnicamente se llama *"el ambiente"* de la Jurisdicción de lo Social, en el que la cultura de *segunda ola* es dominante, lo que facilita, por ejemplo, que cualquier atisbo de flexibilidad en las condiciones de trabajo, por parte de la empresa, se vuelva contra ella, bajo forma de derechos adquiridos de los trabajadores. Y eso es rigurosamente incompatible con las necesidades de la postcontemporánea Economía del Conocimiento. De todas formas, la más importante de las barreras a superar, es la falta de una cultura tecnológica ampliamente extendida entre la población. Se trata probablemente de un obstáculo del mismo nivel que el que ha representado, hasta tiempos recientes, el coste exagerado de las telecomunicaciones, derivado de las periclitadas estructuras monopolísticas.

En concreto, el Informe BRETON (Francia), destaca la inercia social y organizativa, como uno de los principales obstáculos al desarrollo del teletrabajo. Estas inercias existen tanto en las empresas como en los trabajadores y sobre todo en los mandos intermedios y empleados menos cualificados.

3.- TELETRABAJO Y DERECHO LABORAL.

Ya se ha visto cómo el teletrabajo, por su propia naturaleza, es conflictivo desde el punto de vista de la difícil calificación de las relaciones jurídicas que genera, sobre todo cuando se presta única y exclusivamente a domicilio. Otros problemas son los que tienen que ver con aspectos de seguridad e higiene y no se puede olvidar que la extensión del teletrabajo, propiciada por el impulso tecnológico, así como su internacionalización, pueden poner en entredicho el planteamiento mismo del Derecho Social, en los países más desarrollados. Vayamos por partes:

3.1.- Teletrabajo y trabajo a domicilio.

La regulación del trabajo a domicilio, a falta de otra más específica, resulta aplicable en determinadas condiciones al teletrabajo; pero no siempre y ni siquiera siempre que se desarrolla en el domicilio del teletrabajador. Antes de entrar en mayores precisiones, conviene poner de manifiesto la regulación básica del trabajo a domicilio que, como es sabido, se halla en el artículo 13 del TR del ET, que reza como sigue:

Artículo 13. Contrato de trabajo a domicilio.

1. Tendrá la consideración de contrato de trabajo a domicilio aquel en que la prestación de la actividad laboral se realice en el domicilio del trabajador o en el lugar libremente elegido por éste y sin vigilancia del empresario.

2. El contrato se formalizará por escrito con el visado de la oficina de empleo, donde quedará depositado un ejemplar, en el que conste el lugar en el que se realice la prestación laboral, a fin de que puedan exigirse las necesarias medidas de higiene y seguridad que se determinen.

3. El salario, cualquiera que sea la forma de su fijación, será, como mínimo, igual al de un trabajador de categoría profesional equivalente en el sector económico de que se trate.

4. Todo empresario que ocupe trabajadores a domicilio deberá poner a disposición de éstos un documento de control de la actividad laboral que realicen, en el que debe consignarse el nombre del trabajador, la clase y cantidad de trabajo, cantidad de materias primas entregadas, tarifas

acordadas para la fijación del salario, entrega y recepción de objetos elaborados y cuantos otros aspectos de la relación laboral interesen a las partes.

5. Los trabajadores a domicilio podrán ejercer los derechos de representación colectiva conforme a lo previsto en la presente Ley, salvo que se trate de un grupo familiar.

Sin perjuicio de que más adelante aclare por qué he subrayado algún requisito del trabajo a domicilio, establecido por el artículo 1 ET, es previo señalar que no es nada fácil determinar cuándo estamos en presencia de un trabajador a domicilio y cuándo de un trabajador autónomo. La Jurisprudencia existente, que no es especialmente abundante, se verá muy enriquecida con la expansión del teletrabajo, materia sobre la que todavía no he tenido ocasión de analizar ninguna sentencia dictada en España. No obstante sí existe Jurisprudencia sobre el trabajo a domicilio, y en ella se observa la dificultad de deslindar lo Civil/Mercantil de lo Laboral, en estos supuestos, en los que pesan mucho las circunstancias de cada caso concreto. En principio a favor de la relación laboral juegan la existencia de circunstancias tales como un salario más o menos fijo, mientras que en su contra pesa, por ejemplo, la afiliación de los trabajadores a domicilio al régimen de Autónomos de la Seguridad Social, o el hecho de que el trabajo sea llevado a cabo por varias personas. Véanse, por ejemplo, la Sentencia del extinto Tribunal Central de Trabajo de 9 de marzo de 1994 (base de datos de Jurisprudencia de La Ley), o la STS de 12 de septiembre de 1988 (base de datos de Jurisprudencia de Aranzadi).

A la vista de tales Sentencias parece razonable concluir que una empresa adecuadamente asesorada desde el punto de vista jurídico, casi siempre estará en condiciones de evitar la calificación laboral de las relaciones de trabajo a domicilio, y por ende de las de teletrabajo que se inscriban en dicha categoría. En este sentido, el empresario tendrá que cuidar que quede bien documentada la situación, puesto que el artículo 8.2 del TR del ET, exige la forma escrita de los contratos de trabajo a domicilio y no hay que olvidar que el párrafo 11 del mismo artículo presume la existencia de contrato de trabajo, *entre todo el que presta un servicio por cuenta y dentro del ámbito de organización y dirección de otro que lo recibe, a cambio de una retribución a aquél.*

A colación del subrayado del artículo 13.1 ET, diré que no está ni mucho

menos claro que el teletrabajo llevado a cabo en el propio domicilio, tenga siempre y en todo caso la consideración jurídico-laboral de *trabajo a domicilio*. Antonio FERNANDEZ-BORRELLA[10] pone de manifiesto Jurisprudencia de otros países, con legislación parecida a la española, de la que interesa destacar el caso de Alemania, donde se aplica la legislación de trabajo a domicilio, cuando este es el caso, a teletrabajo realizado *fuera de línea*, como suele suceder, aunque no siempre, en el supuesto de proceso de textos; si bien en el caso de trabajadores que efectúan tareas *on-line*, y por lo tanto directamente controlables por el empleador, se considera aplicable la legislación laboral general y no la del trabajo a domicilio. Este criterio ha sido el mantenido en una sentencia del año 1984, dictada por el Tribunal Central de Trabajo de Munich.

Que la calificación jurídico-laboral del teletrabajo como trabajo a domicilio o no, dependa de algo tan legal y a la vez tan peregrino, como que determinada actividad se realice *en línea* o *fuera de línea* nos hace ver la necesidad de ir a una regulación específica de la materia, con la expresa advertencia de que deben evitarse, en una economía global, los afanes hiperreguladores, tan característicos de la legislación laboral. Incluso entiendo que la iniciativa debiera partir de otros ámbitos y señaladamente de la Unión Europea, bajo forma de Directiva; o mejor aún de la OIT, con carácter de Convenio Internacional y no de mera recomendación. De hecho problemas muy parecidos, como señala el propio FERNANDEZ-BORRELLA, se han planteado en países ajenos a la UE, como Suiza, donde se ha dispuesto expresamente la ampliación de la Ley sobre trabajo a domicilio, a los teletrabajadores, o Japón, donde en principio el proceso de textos tampoco entra en la Ley sobre industrias domésticas, salvo en casos especiales (p.e. cuando el trabajador recibe el material en soporte informático). Las vacilaciones que ello origina, han hecho que en Japón también se haya abogado por la extensión de la referida Ley a los teletrabajadores.

No se trata aquí de entrar en mayores detalles sobre el trabajo a domicilio, cosa que pueden hacer y hacen sin duda mejor los especialistas en Derecho del Trabajo. Me limitaré a hacer unas breves indicaciones que resultan de especial interés a nuestros efectos:

■[10] FERNANDEZ-BORRELLA BALLESTEROS, A.: "El teletrabajo". Tesina presentada en el I Master en Informática y Derecho, dirigido por el que suscribe, en la Facultad de Derecho de la Universidad Complutense de Madrid, 1996. Pág. 23.

-En esta materia, la Ley de Contratos de Trabajo de 1944 se entiende vigente, si bien degradada al rango reglamentario. Dada la ancestralidad y contexto de la referida norma, razón de más para que se proceda a una regulación, aún cuando sea somera, del teletrabajo.

-Cuando el teletrabajo tenga la calificación jurídica de trabajo a domicilio, es especialmente importante cumplir con la obligación de su formalización escrita, pues de no ser así y salvo prueba en contrario, se presume celebrado a jornada completa y por tiempo indefinido. Por lo demás, en principio se estima que el trabajo a domicilio puede llevarse acabo bajo cualquier modalidad de contratación legalmente prevista; si bien se considera incompatible con los contratos de prácticas o aprendizaje, al estar lógicamente unidos con la vigilancia y control directos por parte del empresario, que como antes se ha dicho, excluye el trabajo a domicilio.

-Por lo que a seguridad e higiene se refiere, el teletrabajo que se lleva a cabo en el propio domicilio, por más que no tenga, en ocasiones, la calificación técnica de trabajo a domicilio, presentará una problemática idéntica a la del trabajo a domicilio en sentido técnico, por lo que le serán de aplicación los criterios jurisprudenciales ya asentados en este ámbito. El cuanto al régimen del teletrabajo en telecentros, no parece que presente dificultades dignas de mención, en el aspecto ahora considerado.

-Cuando el teletrabajo tenga la consideración técnica de trabajo a domicilio, al no ser de aplicación a éste las reglas sobre jornada y horarios (artículo 3 del Real Decreto 2001/1983), en caso de que se requiera la telecomunicación con la empresa en determinados días y/o horas, es de fundamental importancia hacerlo constar así en el contrato de trabajo.

3.3.- Otras cuestiones a tener en cuenta en los contratos de teletrabajo.

Conforme se ha precisado, lo primero es tener claro si se desea establecer una relación regida por el Derecho Laboral o no. De no ser así es más importante todavía algún tipo de formalización escrita de la relación, normalmente a través de la emisión de presupuestos y facturas de los trabajos realizados, por parte del teletrabajador, que deberá reunir las demás características habituales en los Autónomos, como hallarse afiliado al correspondiente régimen especial de la Seguridad Social, trabajar para varias empresas, no estar retribuido con conceptos

fijos que pudieran ser interpretados como *salario*, sino por obra determinada, en la que deberá facturar el IVA que corresponda, etc.

En el supuesto de que la relación sea con un trabajador autónomo, es lógicamente incompatible con otros conceptos, tales como jornada o vacaciones retribuidas, a fin de que no se estime que la correspondiente relación jurídica se haya establecido en fraude a la Ley laboral.

Cuando la relación que se establezca sea efectivamente laboral, las cláusulas del contrato deberán contener estipulaciones al menos sobre los siguientes extremos:

-Aunque no se suela indicar, acaso lo primero sea plantearse la conveniencia o no del teletrabajo transfronterizo y, en consecuencia, incluir o no cláusulas acerca de la legislación aplicable.

-Determinar a quién corresponde la provisión del material necesario para el teletrabajo, que normalmente será al empresario. Este material no tiene la consideración de retribución en especie. Por lo demás, las obligaciones de seguridad e higiene, afectan sin duda al empresario en razón de la calidad y seguridad del material que éste entregue al teletrabajador.

-Definir las condiciones de uso de tal material, sobre todo en relación con el material informático. No se olvide que el software, por ejemplo, sólo puede ser usado en las condiciones previstas en el correspondiente contrato de licencia.

-Dejar claro que la responsabilidad por el mal uso de los programas corresponde al teletrabajador, quien además estará obligado a adoptar precauciones razonables contra los virus informáticos, y en general sobre seguridad de la información; si bien el coste de los medios y procedimientos de seguridad, es razonable que corra a cargo de la empresa, pues no en vano se establece en su interés.

-Determinar asimismo la imputación de costes de la línea telefónica, al ser esta susceptible de una pluralidad de usos.

-Ver si la empresa se hace cargo de parte de los suministros del domicilio del teletrabajador, cual puede ser el caso de la electricidad.

-Dejar claras las obligaciones del trabajador, en cuanto a desplazamientos a la sede de la empresa, y si los costes del mismo corren o no a cargo del teletrabajador.

-Establecer el derecho de la empresa a visitar e inspeccionar el lugar de teletrabajo, que deberá estar determinado dentro del domicilio. Si bien estas cláusulas tienen el riesgo de que la empresa puede incurrir en responsabilidad si el teletrabajo se efectúa en condiciones de seguridad que no puedan estimarse adecuadas. Igualmente pueden establecerse previsiones sobre posibles cambios en el lugar donde se desarrolla el teletrabajo, salvo que se trate de *trabajo a domicilio* en sentido técnico, pues ya se ha visto que la determinación del lugar de la prestación es de la exclusiva competencia del teletrabajador.

3.4.- Teletrabajo y Derecho Internacional Privado del Trabajo.

Como suele ser habitual en los procesos de globalización económica, los Estados tienen poco margen de maniobra para obstaculizar legalmente el desarrollo del teletrabajo, pues las medidas restrictivas que eventualmente pudieran adoptar, tienen un riesgo cierto de volverse en contra de la Economía Nacional. Es, pues, muy difícil que cunda el desafortunado ejemplo portugués de prohibición del teletrabajo transnacional.

Hoy por hoy resulta de aplicación a las relaciones de teletrabajo transnacional, el artículo 5 del Título Preliminar del Código Civil, que señala: *"Se aplicarán a las relaciones contractuales la ley a que las partes se hayan sometido expresamente, siempre que tenga alguna conexión con el negocio de que se trate; en su defecto, la ley nacional común a las partes; a falta de ella, la de la residencia habitual común, y en último término, la ley del lugar de celebración del contrato".*

Es evidente que cuando un país, lejos de obstaculizar, promueve legalmente el desarrollo del teletrabajo, emprende una acción que tiende positivamente a la creación de empleo, pues mejora las condiciones de competitividad del teletrabajo de sus nacionales; mientras que en caso contrario fuerza a las empresas a contratar teletrabajadores extranjeros, a fin de escapar de una legislación restrictiva. En todo caso, de lo que no hay duda, es de que el efecto económico de la legislación, será tanto más negativo, cuanto más restrictiva sea aquella para el teletrabajo.

Cuando el teletrabajo se sujeta específicamente al Derecho Laboral, la

Ley aplicable al correspondiente contrato, viene dada por el artículo 10.6 del Código Civil, cuyo criterio prevalente sigue siendo el sometimiento expreso de las partes: *"A las obligaciones derivadas del contrato de trabajo, en defecto de sometimiento expreso de las partes y sin perjuicio de lo dispuesto en el apartado 1 del artículo 8, les será de aplicación la ley del lugar donde se presten los servicios".*

Por lo demás, sólo corresponde señalar que el artículo 8.1 proclama el principio de territorialidad de las leyes de *policía*, circunscritas a materias concretas, tales como seguridad e higiene o Inspección de trabajo.

3.5.- El teletrabajo como motor del replanteamiento del Derecho Social.

El mundo desarrollado y sobre todo los países que integran la Unión Europea viven cada día la discordancia que se produce entre sus avanzados sistemas de protección social, todavía muy vinculados al trabajo por cuenta ajena y el handicap de competitividad que ello supone, en el marco de una economía global. Se trata de una cuestión difícil de resolver adecuadamente, tanto por sus implicaciones políticas, en el marco de la dialéctica entre liberalismo y socialismo, como por cuanto que sustancialmente en ella se dilucidan intereses. De una parte el capitalismo salvaje, considera el trabajo como un estricto factor de la producción al que quisiera ver plenamente sometido a la ley de la oferta y de la demanda. De otra el sindicalismo clásico se ha especializado en proteger a la élite de trabajadores fijos a toda costa, e incluso a sabiendas de que la hiperprotección social es un freno para la competitividad de la economía nacional y, por ende, para la generación de empleo.

Conciliar tales intereses no es fácil, sobre todo habida cuenta de sus implicaciones políticas y de las no poco importantes dosis de irracionalidad que todos tienen en la defensa de sus respectivas posturas. La realidad y expansión del fenómeno del teletrabajo, no hace sino agudizar estas contradicciones. Por una parte las empresas recurren y recurrirán todavía más a esta fórmula, porque abre una vía de escape a la legislación laboral y no tanto por sus ventajas intrínsecas, que sin duda las tiene. Por otra parte, si se quiere someter al teletrabajo al régimen general del Derecho Social, se producirá el efecto, poco deseable desde el punto de vista de la economía nacional, de que más y más actividades van a ser realizadas allende nuestras fronteras. En la sociedad de la información el

teletrabajo es una realidad, destinada a un continuo crecimiento.

Michael CHARPENTIER[11], ofrece las siguientes cuentas, que son suficientemente significativas al respecto. Dice:

"Mas del 50% del empleo en Europa tiene que ver actualmente con el sector de la información. El 80% de los nuevos empleos se crean por pequeñas empresas en los sectores de la información y de los servicios. Los conceptos habituales de agricultura, industria y servicios no ayudan a clarificar el cambio que se ha producido. Incluso en los sectores primario y secundario el mayor porcentaje de valor añadido deriva de procesos de información, relacionados con la sociedad del conocimiento".

Cifras parecidas las ofrece Francisco ORTIZ CHAPARRO, quien precisa, al respecto del sector servicios en las sociedades avanzadas y singularmente en Estados Unidos:

"En ellas, el número de los trabajadores ocupados en el sector terciario supone, como mínimo, el 50 por 100 de la población ocupada y, dentro de ellos, el número de los que trabajan en la información supera al de los que trabajan en las demás profesiones. Esta desproporción a favor de los trabajadores de la información se incrementa día a día"[12].

"Actualmente el 80 por 100 de la fuerza laboral estadounidense trabaja en este sector. (...) La oficina de estadísticas laborales americana pronostica que todo el trabajo neto creado hasta el año 2005 lo será en el sector de los servicios"[13].

Frente a esta realidad, el problema, como muy bien apunta SAENZ DE MIERA, en el prólogo a una importante obra sobre la cuestión[14], es que *"el paradigma de la revolución industrial puede estar ya sobrepasado en términos tecnológicos y*

■11 CHARPENTIER, M.: "Networked Europe". Actas del Congreso Europeo sobre Teletrabajo y Nuevas Formas de Trabajar, Berlín, 1994.

■12 ORTIZ CHAPARRO, F. Op. cit. Pág. 3.

■13 ORTIZ CHAPARRO, F. Op. cit, Pág. 10.

■14 GRAY, M.; HODSON, N.; GORDON, G. Y OTROS: "El Teletrabajo". Ed. BT Telecomunicaciones, ECTF y Fundación Universidad Empresa, Madrid, 1995.

económicos, pero sigue vivo, en buena medida, en términos sociales". El propio SAENZ DE MIERA observa que en el nuevo paradigma *"las telecasas, como en la época de las sociedades agrícolas, surgen ahora como unidades de producción económica y no sólo como unidades de consumo".*

En otro orden de cosas y ya en relación con la redistribución internacional del trabajo que se opera a raíz del teletrabajo, debo decir que se trata de un hecho, en el que se han especializado varios países caribeños y asiáticos, fundamentalmente, así como Irlanda en el ámbito de la Unión Europea, debido en todo caso a sus menores costes salariales (en ocasiones hasta diez veces inferiores a los de los países más desarrollados), y en el último supuesto a la identidad idiomática con el mayor demandante internacional de teletrabajo, que lógicamente es Estados Unidos. La internacionalización del teletrabajo tiene la ventaja adicional que las diferencias horarias entre países, facilitan que se pueda trabajar por este procedimiento, las 24 horas del día.

Como respuesta a los nuevos retos que surgen del todavía incipiente mercado global del trabajo, se está pensando ya en el entero replanteamiento del sistema de protección social, que lo simplifique, y sobre todo, lo desvincule definitivamente del trabajo por cuenta ajena; puesto que los sistemas de protección social directamente vinculados a éste, son un factor distorsionante para la buena marcha de la economía. De hecho si la universalización de las prestaciones sanitarias públicas ha terminado desvinculándolas del trabajo por cuenta ajena, al igual que ha sucedido con las pensiones no contributivas, o en la práctica con el PER, por ejemplo, no hay razón para que no se pueda pensar en una desvinculación del entero sistema asistencial con respecto al trabajo por cuenta ajena, lo que redundaría además en una enorme simplificación del mismo

La Comisión Europea, en apenas una página de su informe, antes citado, sobre el teletrabajo[15], incluye una sugerente referencia esta idea, que por su moderada extensión, reproduciré de forma literal:

"Un estudio en profundidad del contexto prestacional de los teletrabajadores, así como de otros trabajadores flexibles, confirma la opinión de un creciente número de responsables políticos de todas las partes de Europa según la cual ha llegado el momento de poner en marcha

■[15] Op. Cit. Pág. 61.

una reforma radical y una simplificación de los sistemas de protección social.

La individualización de los derechos sociales sería el elemento clave de toda reforma (...).

Una iniciativa más decidida y más radical consistiría en suprimir todos los subsidios y controlar los recursos, para sustituirlos por una renta mínima de base, entregada a modo de derecho de ciudadanía a todo hombre, toda mujer y todo niño, cualquiera que sea su edad o nivel de renta. Los estudios preliminares llevados a cabo en el Reino Unido por el Grupo de Investigación sobre la Renta de los Ciudadanos, dan a entender que un cambio de esta envergadura es realista desde un punto de vista económico, a condición de que se supriman las deducciones fiscales y asimismo permitiría un importante ahorro en el ámbito administrativo.

Una renta mínima garantizada favorecería el proceso de flexibilización de los mercados de trabajo, al permitir a los trabajadores entrar y salir con mucha mayor facilidad de la población ocupada, así como cambiar su horario de trabajo de un día a otro o de una semana a otra. Igualmente permitiría entrar y salir con mucha mayor facilidad de la enseñanza a tiempo completo o parcial a cualquier edad, y contribuiría así al objetivo de la educación permanente para todos[16]".

Personalmente entiendo que la propuesta es suficientemente sugestiva y provocadora, como para que no haga falta abundar más en ella. Es obvio que habría que matizar bastantes cosas; pero prefiero que cada cual saque sus propias conclusiones. En cualquier caso, no es descabellado plantearse un sistema único y autónomo de protección social, que lógicamente habría de estar vinculado al sistema fiscal y, por lo tanto, sería dependiente del nivel de renta de cada país. A mi juicio, en los Estados más desarrollados es plenamente factible y tiene la enorme ventaja de no provocar distorsiones en el mercado de trabajo.

4.-INICIATIVAS DE LA UNION EUROPEA SOBRE TELETRABAJO.

El 12 de mayo de 1995 (DOCE nº C213/51, de 17 de agosto), el Diputado del PPE Joaquín SISÓ, formuló una pregunta escrita a la Comisión, a

[16] La traducción es del autor.

colación de las encuestas realizadas en el marco del proyecto TELDET[17], que revelaban que la penetración del teletrabajo en las organizaciones europeas se sitúa alrededor del 5%, mientras que el número de teletrabajadores en el ámbito de la Unión se estima en 1.250.000. En la pregunta se ponía de manifiesto también que la expectativa de la Unión es que en el año 2000 existan 10.000.000 de teletrabajadores en su ámbito. A colación de lo anterior SISÓ CRUELLAS preguntaba sobre los sectores con mayores posibilidades de creación de empleo bajo forma de teletrabajo, así como sobre los esfuerzos que está haciendo la Comisión para informar a las organizaciones europeas sobre el potencial del teletrabajo y para ayudar al necesario cambio de organización.

En su respuesta, el Comisario Sr. FLYNN, señalaba que más que sectores específicos del teletrabajo, existe una penetración horizontal del mismo en diferentes sectores. No obstante, apuntaba una serie de actividades muy características del teletrabajo, tales como el tratamiento de datos y de textos, la programación, las tareas de secretaría y administración, la contabilidad, las ventas, la comercialización, la investigación y la asesoría.

Por lo demás apuntaba el Sr. FLYNN que desde 1993 la Comisión estudia las acciones necesarias para estimular el teletrabajo transfronterizo, e igualmente el teletrabajo fue definido como prioridad por el Consejo Europeo de Corfú (junio de 1994) en el informe *"Europa y la sociedad global de la información"*. Idéntica idea está presente en el plan de acción de la Comisión sobre el camino de Europa hacia la sociedad de la información.

A lo dicho por el SR. FLYNN, hay que añadir que estas iniciativas de la Comisión y del Consejo, arrancan del Libro Blanco de DELORS[18] (diciembre de 1993). De hecho, la antes citada reunión del Consejo de Corfú, en la que se aprobó el informe *"Europa y la sociedad global de la información"*, es el resultado de los trabajos en desarrollo del Libro Blanco, llevados a cabo por la Comisión Bangemann, que debe su nombre al Comisario de Industria Martin BANGEMANN.

■[17] TELDET es un Consorcio Europeo, cuyo nombre es acrónimo de "Telework developments and trends".

■[18] "Crecimiento, competitividad, empleo. Retos y pistas para entrar en el siglo XXI". 1994.

En el Informe BANGEMANN se insiste en la necesidad de fomentar el teletrabajo, con el objetivo de que al finalizar el año 1996, esta fórmula afecte al 2% de los trabajadores del sector terciario y en el año 2000 existan en Europa diez millones de teletrabajadores.

Sí destaca el Sr. FLYNN, que desde 1992 la Comisión ha impulsado un foro para la promoción del teletrabajo a nivel comunitario (ECTF), en cuyo marco se llevó a cabo la Conferencia europea *"Teletrabajo 1994. Nuevas maneras de trabajar"*, que se celebró en Berlín el 3 y 4 de noviembre de 1994. Igualmente, en el contexto del programa de acción social a medio plazo 1995-1997, se prevé la presentación por la Comisión de una comunicación sobre el impacto social y en la salud del teletrabajo.

De todas formas, la promoción europea del teletrabajo es más antigua de lo que señala el Comisario FLYNN en su respuesta al europarlamentario español Joaquín SISO, puesto que arranca del programa ORA (*"Opportunities for Rural Areas"*), iniciado en 1991, en el que se inscribe el III Programa Marco de I+D, en cuyo proyecto SYNERGY se recomendó la creación del antes aludido Foro Europeo de Telemática y Teletrabajo (ECTF).

Por lo que se refiere a otros proyectos y programas que inciden sobre la materia, y también al margen de lo indicado por el Comisario FLYNN, hay que destacar que en el marco de las propuestas del Libro Blanco de DELORS, se ha llevado a cabo el proyecto TELEURBA, en el que se estudia la relación entre tráfico rodado y teletrabajo, en cuatro grandes capitales europeas, entre las que se encuentra Madrid.

Hay que mencionar asimismo el proyecto PRACTICE, en el que figuran recomendaciones para la regulación del teletrabajo por los Estados miembros; mientras que en el proyecto ATTICA existe una clara referencia a la coordinación de las legislaciones nacionales, por lo que no es descartable, a medio plazo, que se promulgue una Directiva sobre la materia.

Por último, a nivel de programas de la UE que contemplan el teletrabajo, hay que mencionar el programa RACE, sobre comunicaciones avanzadas, o las importantes subvenciones a la implantación del teletrabajo, previstas en el IV Programa-marco (843 millones de Ecus).

El teletrabajo es, pues, una cuestión de extrema importancia en los modernos procesos de globalización, cuya clave se halla en el sector cuaternario. Por lo tanto, en el desarrollo del sector de la información y del conocimiento, se dilucida quiénes, por la seriedad de sus planteamientos y no por vaporosas aspiraciones, van a ser *"vagón de cabeza"* de la economía global, o por el contrario se van a tener que conformar con lugares más mediocres, e inclusive con la *cola del convoy*. *"Ser alguien"*, en el mundo de hoy, no depende tanto de tamaños o de *"potencial bruto"*, como de saber situarse estratégicamente en la Economía del Conocimiento. La Unión Europea lo tiene razonablemente claro. España, por su cuenta, también dispone de un considerable margen de maniobra; por ejemplo para dotarse de una legislación bien calibrada, que lejos de impedir, facilite nuestra competitividad, en el mercado global del teletrabajo.

Auditoría Jurídica de los Entornos Informáticos*

EMILIO DEL PESO NAVARRO

Licenciado en Derecho y en Informática.
Socio IEE. Informáticos Europeos Expertos

1. Introducción

Hasta no hace mucho tiempo la comprobación de la gestión y el control a posteriori de la actividad económico-financiera de cualquier organización ya sea ésta pública o privada se hacía sólo mediante la Auditoría de Cuentas: sin embargo, debido al alto grado de informatización de las empresas, esto ya no iba siendo suficiente.

Se hacía preciso conocer qué ocurría dentro de esas enormes "cajas negras" que son los sistemas de información.

Con la Auditoría de Cuentas tradicional se podía conocer cómo se abastece de información el sistema informático y cual es el resultado del tratamiento dentro del mismo pero no lo que sucede entre esa entrada y esa salida de información, conocemos los "inputs" y los "outputs" pero no cómo se han

Esta ponencia está basada en el Capítulo: El Marco Jurídico de la Auditoría Informática del libro Auditoría Informática que la Editorial Rama publicará próximamente.

generado estos últimos y si han sido objeto o no de alguna manipulación antes de hacerse "visibles".

El examen de lo que acontece en esas "cajas negras", que es lo que en realidad son los sistemas informáticos, se puede lograr gracias a la Auditoría Informática.

La definición de la Auditoría Informática rara vez se encuentra libre de estar involucrada en los intereses del colectivo que la facilita.

A continuación vamos a facilitar dos definiciones que entendemos se encuentran libres de esa dependencia.

Una definición podría ser la siguiente: "Se entiende por Auditoría Informática una serie de exámenes periódicos o esporádicos de un sistema informático cuya finalidad es analizar y evaluar la planificación, el control, la eficacia, la seguridad, la economía y la adecuación de la infraestructura informática de la empresa."

Como fácilmente se puede comprender esta definición reduce considerablemente el ámbito sobre el que puede trabajar la Auditoría Informática.

El profesor de la Universidad Carlos III, RAMOS GONZÁLEZ propone la siguiente definición: "La Auditoría Informática comprende la revisión y la evaluación independiente y objetiva, por parte de personas independientes y teóricamente competentes del entorno informático de una entidad, abarcando todas o algunas de sus áreas, los estándares y procedimientos en vigor, su idoneidad y el cumplimiento de éstos, de los objetivos fijados, los contratos y las normas legales aplicables; el grado de satisfacción de usuarios y directivos; los controles existentes y análisis de los riesgos."

Como juristas somos partidarios de un concepto amplio de la Auditoría Informática pues si ésta queda reducida simplemente a un control de los aspectos informáticos de los sistemas de información difícilmente puede cumplir uno de los objetivos que esperamos de la Auditoría Informática; la detección de irregularidades, por ahora las llamaremos así, que se pueden producir tanto dentro de los sistemas de información como en la entrada y en la salida a los mismos.

Si admitimos un concepto amplio de Auditoría Informática los objetivos de ésta pueden ser los siguientes:

a) Colaboración con la Auditoría de Cuentas

Como ya hemos expuesto antes, la Auditoría de Cuentas tradicional ya no es suficiente para ejercer el control de la actividad económico-financiera de las organizaciones debido al alto grado de informatización de las mismas y por eso necesita de la Auditoría Informática para llevar a cabo su cometido.

b) Auditoría de los propios sistemas informáticos

Este objetivo reduce la auditoría a la propia informática, pero no nos engañemos pues en sí misma puede ser riquísima: auditoría del desarrollo, auditoría de la explotación, auditoría del mantenimiento, auditoría de la explotación, auditoría de la calidad, auditoría de la seguridad, etc.

c) Auditoría jurídica de los entornos informáticos

Este último objetivo es el que como juristas más nos interesa pues significa, entre otras cosas una importantísima colaboración en la persecución del delito informático, en sus diferentes modalidades, algo difícilmente de conseguir y asimismo puede servir de herramienta poderosa a la hora de obtener la prueba del fraude detectado.

Las principales áreas en que puede trabajar este último tipo de auditoría, por supuesto en íntima relación con el que figura en el apartado b), son las correspondientes a: los datos de carácter personal, los programas de ordenador, las bases de datos y la multimedia, los fraudes y delitos informáticos, los contratos informáticos y electrónicos, el intercambio electrónico de datos, la transferencia electrónica de fondos, el documento electrónico, la red Internet, los seguros informáticos y los dictámenes y peritajes informáticos.

A continuación vamos a examinar brevemente cada una de esas áreas enumerando en unos casos los puntos más importantes a comprobar y en otros simplemente explicando en que consiste al objeto de que el lector sea el que fije los asuntos a verificar.

No tratamos en estas líneas de establecer unas listas de comprobación más o menos completas sino introducir al lector en este vasto y apasionante campo prácticamente aún sin desarrollar.

2. La protección de los datos de carácter personal

El artículo 18.4 de nuestra Constitución emplaza al legislador a limitar el uso de la informática para garantizar el honor, la intimidad personal y familiar de sus ciudadanos y el legítimo ejercicio de sus derechos.

Fruto de este mandato constitucional fue la promulgación de la Ley Orgánica 5/1992 de 29 de octubre de Regulación del Tratamiento Automatizado de los Datos de carácter personal (LORTAD). Se trata de una Ley de las que en el Derecho Comparado se vienen denominando leyes de protección de datos, aunque en realidad su objeto no sea la protección de los datos sino la protección de la intimidad y privacidad de las personas titulares de esos datos, afectados según la terminología de la Ley.

Antes de la entrada en vigor de la LORTAD, los datos de carácter personal venían siendo unos datos de segunda categoría muy por detrás de los datos económicos o contables. Su comercialización y cesión era algo habitual.

La LORTAD cambia el panorama y estos datos adquieren un nuevo protagonismo aunque aún existe en muchos sectores de la sociedad falta de información y, en algunos casos, también falta de interés por protegerlos debidamente.

El conocimiento por parte de los auditores informáticos de esta nueva realidad puede colaborar en gran manera a la legalización de las situaciones que aún no lo están prestando con ello un gran servicio a las organizaciones evitándoles situaciones incómodas, multas y en casos extremos la inmovilización de sus ficheros.

El Estatuto de la Agencia de Protección de Datos (Real Decreto 428/1993, de 26 de marzo) ha sido una de las primeras normas españolas en incluir en su texto la Auditoría Informática. Así el artículo 28 titulado: Funciones inspectoras, en su punto 1 al enumerar las competencias de la Inspección de Datos en su apartado e) dice: "Realizar auditorías de los sistemas informáticos

con miras a determinar su conformidad con las disposiciones de la Ley Orgánica 5/1992."

Estas mismas auditorías las deben realizar como medida preventiva en sus respectivas organizaciones tanto los auditores informáticos internos como externos.

Otra norma complementaria de la LORTAD, la Instrucción 1/1995 de 1 de marzo de la Agencia de Protección de Datos relativa a la prestación de servicios de información sobre solvencia patrimonial y crédito regula la auditoría informática de la seguridad en los sistemas que almacenen o procesen información relativa al cumplimiento o incumplimiento de obligaciones dinerarias.

"Norma cuarta". Forma de comprobación.

1. Los sistemas que almacenan o procesan información relativa al cumplimiento o incumplimiento de obligaciones dinerarias deberán acreditar la efectiva implantación de las medidas de seguridad exigidas por el artículo 9.1 de la Ley Orgánica dentro del año siguiente a la publicación de la presente Instrucción. Para los ficheros que se inscriban con posterioridad a esta Instrucción el plazo se computará a partir de la fecha en que aquélla se haya efectuado en el Registro General de Protección de Datos."

Recordamos que el artículo 9 de la Ley de encuentra pendiente de desarrollo. El punto 1 del artículo enumera lo que se pueden considerar unos principios de seguridad a los que deben someterse los ficheros recayendo la responsabilidad de la adopción de las medidas necesarias en el responsable del fichero.

El punto 2 de la norma cuarta de la Instrucción, especifica que la implantación de dichas medidas de seguridad se demostrará mediante la correspondiente auditoría.

"2. La implantación, idoneidad y eficacia de dichas medidas se acreditara mediante la realización de una auditoría proporcionada a la naturaleza, volumen y características de los datos personales almacenados y tratados, y la remisión del informe final de la misma a la Agencia de Protección de Datos."

La Auditoría la pueden realizar tanto auditores internos como externos. No consideramos acertada la posibilidad de que la auditoría la pueda realizar la auditoría interna de la propia organización dada la trascendencia exterior que el informe de auditoría puede tener lo que hace imposible que exista la independencia necesaria aunque dicho departamento sea independiente del órgano responsable del tratamiento y gestión de los datos pero no de la propia organización.

"3. La auditoría podrá ser realizada:

Por el departamento de auditoría interna del responsable del fichero, si cuenta con un departamento formalmente constituido, profesionalmente cualificado e independiente del órgano responsable del tratamiento y gestión de los datos.

Por un auditor externo, profesionalmente cualificado e independiente del responsable del fichero."

Los puntos 3 y 4 se refieren a como debe ser realizada la auditoría y lo que debe contener el informe.

"4. La auditoría deberá ser realizada de acuerdo con las normas y recomendaciones de ejercicio profesional aplicable en el momento de su ejecución.

5. El informe de auditoría deberá dictaminar sobre la adecuación de las medidas y controles destinados a garantizar la integridad y confidencialidad de los datos personales almacenados o tratados, identificar sus deficiencia o insuficiencias y proponer las medidas correctoras o complementarias necesarias. Deberá, igualmente incluir los datos, hechos y observaciones en que se basan los dictámenes alcanzados y recomendaciones propuestas."

3. La protección jurídica de los programas de ordenador

Antes de analizar que debemos examinar al auditar, desde el aspecto jurídico, los programas de ordenador consideramos importante explicar que se entiende por programas de ordenador y cual es su lugar entre las diferentes clases de bienes jurídicos dignos de protección en nuestro ordenamiento jurídico.

En una primera aproximación un programa de ordenador se puede considerar como el conjunto de materiales elaborados conceptualmente para la solución de un problema de tratamiento automatizado de datos.

El Texto Refundido de la Ley de la Propiedad Intelectual , aprobado por Real Decreto Legislativo 1/1996 de 12 de abril, en su artículo 96.1 lo define 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 fuere su forma de expresión o fijación.

A los mismos efectos, la expresión programas de ordenador comprenderá también su documentación preparatoria. La documentación técnica y los manuales de uso de un programa gozarán de la misma protección que este Título dispensa a los programas de ordenador."

Entre la categoría de los bienes, los programas de ordenador presentan peculiaridades que los diferencian de los bienes con una entidad material y susceptibles por tanto de una aprehensión física. Nuestro Código civil divide los bienes en corporales e incorporales .

Un programa de ordenador, como una creación de la mente que es, no puede ser incluido en ninguna de estas dos categorías por lo que hay que acudir a una nueva que es la que se ha creado para este tipo de bienes, la de los bienes inmateriales.

Un bien inmaterial es:

fruto o creación de la mente para que se haga perceptible para el mundo exterior es necesario plasmarla en un soporte puede ser disfrutado simultáneamente por una pluralidad de personas.

Por todo ello la apropiación en los bienes inmateriales, por sí sola, no es suficiente para garantizar su goce exclusivo del mismo; para ello es preciso, desde el punto de vista jurídico, que el Derecho prohiba a todos los demás la utilización o la explotación del mismo y otorgue al titular un derecho en exclusiva.

Un programa de ordenador, como se desprende de lo expuesto, es un bien inmaterial y en función de tal hemos de procurar su protección jurídica.

La protección jurídica de los programas de ordenador, en principio, se puede instrumentar utilizando las siguientes instituciones jurídicas conocidas: estipulaciones contractuales, secreto comercial, derecho de patentes, derecho de marcas y derecho de autor. El sistema elegido ha sido el último. No obstante, la protección que el derecho otorga a los programas de ordenador es compatible con la protección que se le pudiera otorgar por otra vía.

Los programas de ordenador de las organizaciones pueden tener los siguientes orígenes: uso libre (freeware), programa a prueba (shareware), licencia de uso, desarrollo propio, desarrollo a medida, compra de programas y origen ilícito (piratería de programas).

Según sea su origen el auditor deberá hacer unas u otras comprobaciones teniendo en cuenta que si el origen no ofrece una garantía total existe el peligro de que los mismos introduzcan virus en los sistemas de información.

La persecución de la piratería de programas se puede realizar por la vía civil y por la penal.

En esta última vía las infracciones del derecho están tipificadas en los artículos 270, 271 y 272 del Código Penal (Ley Orgánica 10/1995 de 23 de noviembre) pudiendo llegar las penas de prisión a cuatro años y las multas a veinticuatro meses para los casos más graves.

4. Las bases de datos y la multimedia

Una base de datos, como dice DAVARA RODRÍGUEZ, a quién seguiremos en este apartado, es un depósito común de documentación, útil para diferentes usuarios y distintas aplicaciones, que permite la recuperación de la información adecuada, para la resolución de un problema planteado en una consulta.

JAMES MARTIN define la base de datos como una colección de datos interrelacionados almacenados en conjunto sin redundancias perjudiciales o

innecesarias; su finalidad es la de servir a una aplicación o más, de la mejor manera posible; los datos se almacenan de modo que resulten independientes de los programas que los usan; se emplean métodos bien determinados para incluir datos nuevos y para modificar o extraer los datos almacenados. Dícese que un sistema comprende una colección de bases de datos cuando éstas son totalmente independientes desde el punto de vista estructural.

Una base de datos se compone de un contenido y de una estructura de ese contenido.

El contenido de una base de datos puede ser: textos, gráficos, sonidos, imágenes fijas é imágenes en movimiento.

En lenguaje informático a esto se le suele denominar media a la que específicamente nos referiremos más adelante.

Lógicamente cada uno de estos contenidos tendrá un titular de los derechos de autor sobre los mismos.

Pero con independencia de esto, que es importante y que habrá de tenerse en cuenta a la hora de crear una base de datos, lo que aquí tratamos de buscar es la protección jurídica de esa estructura para la que ha sido necesaria una obra de creatividad al seleccionar, clasificar y ordenar sus respectivos contenidos. En definitiva se trata de una obra de creatividad intelectual y por tanto objeto de protección. Hay veces, sin embargo, que no se trata de una creatividad intelectual, y no obstante su valor económico es grande.

Las primeras bases están protegidas por el derecho de autor y las segundas por un derecho "sui generis" al que se refiere la Directiva de la Unión Europea 96/9/CE del Parlamento Europeo y del Consejo de 11 de marzo de 1996.

Es importante analizar la función de los diferentes autores que participan en la creación, desarrollo y explotación de una base de datos, sus

relaciones contractuales y la protección jurídica de la titularidad de las bases de datos.[1]

En un principio en una base de datos participan: el creador o promotor, el distribuidor y el usuario.

Creador o promotor es toda aquella persona física o jurídica que partiendo de una idea selecciona, clasifica, y ordena un determinado tipo de información creando una base de datos, la mantiene y la actualiza.

Distribuidor es asimismo toda persona física o jurídica que comercializa el producto.

Por último, usuario es toda persona física o jurídica que utiliza y consulta la base.

Entre creador o promotor y distribuidor existe una relación contractual en la que el primero se compromete a la creación, mantenimiento y actualización de la base y el segundo a su comercialización aunque en algún caso podría llegar a su distribución gratuita.

Los contratos entre el distribuidor y el usuario suelen ser de los denominados de adhesión en los que el primero fija las condiciones y el segundo simplemente se adhiere a ellas.

La protección jurídica en nuestro ordenamiento jurídico viene dada por el vigente Texto Refundido de la Ley de la Propiedad Intelectual de 12 de abril de 1996 y por la Directiva de la Unión Europea, a la que antes nos referíamos, que en su momento ha de ser incorporada a nuestro ordenamiento jurídico.

En definitiva lo que se protege en una base de datos no es simplemente el almacenamiento de obras, su ordenación y recuperación sino que es todo el procedimiento de creación y el resultado final de la misma, en cuanto a

[1] Para ampliar el tema ver: JORGE PÁEZ MAÑÁ. Bases de Datos Jurídicas. Cindoc. Madrid 1995.

su contenido, análisis, almacenamiento, clasificación, selección y ordenación que caracteriza a la base de datos en sí.

Como hemos dicho anteriormente en lenguaje informático se denomina media a las diferentes clases de archivos que se pueden utilizar en un sistema:

Siguiendo a MILLÉ estos pueden ser los siguientes:

a)Archivos de textos. Estos contienen la descripción numérica de la información redactada mediante signos alfanuméricos.

b)Archivos gráficos. Contienen la descripción numérica de un diseño.

c)Archivos sonidos. Contienen la descripción numérica de una onda sonora.

d)Archivos de imágenes fijas. Contiene la descripción numérica de una imagen formada por pixeles ordenados en columnas y filas.

e)Archivos de imágenes en movimiento. Contienen la descripción numérica de imágenes en movimiento y se llaman corrientemente videos.

Estos archivos se pueden procesar simultáneamente y almacenar en el mismo soporte. Esta combinación de archivos permite producir creaciones multimedia.

Multimedia se puede definir como la combinación de todo tipo de señales de voz, datos, imágenes y escritura. Es un concepto global que abarcará una gran diversidad de servicios.

Entre las obras multimedia encontramos:

a)Videojuegos. Se suele tratar de obras creadas como multimedia y no suelen incorporar elementos de obras ajenas.

b)Educación y entretenimiento. Programas de enseñanza y de entrenamiento.

c)"Edutainment". Productos que enseñan al usuario mientras juega.

d)Revistas.

e)Publicidad.

f)Simuladores.

Las obras multimedia suelen ser producto de un equipo, se trata de obras colectivas y su titularidad suele tenerla una persona jurídica.

En gran número de casos una obra multimedia será una obra derivada pues se trabajará sobre una obra ya existente de la que se deberán tener los derechos correspondientes salvo que se trate de obras de dominio público.

Para la creación de obras multimedia se suelen utilizar las llamadas herramientas, por ejemplo: lenguajes de autor. De estas herramientas se deberá tener licencia para su uso.

Igualmente se suelen utilizar gráficos, fotografías, etc. que existen en archivos creados al efecto y también habrá de contratarse su utilización.

Puede suceder también que se incluyan obras de vídeo con interpretación de artistas con los que habrá que contratar la necesaria autorización.

En resumen el mundo de la multimedia es un sector en gran auge que como todo lo nuevo plantea problemas en las relaciones entre los intervinientes que el derecho deberá resolver en aquello que aún no esté contemplado en el ordenamiento jurídico.

La extensión de Internet ha hecho aumentar considerablemente los productos multimedia y los problemas de propiedad intelectual que esto conlleva.

5. Los delitos informáticos

Fraude puede ser definido como engaño, acción contraria a la verdad o a la rectitud. La definición de delito puede ser más compleja.

Muchos estudiosos del Derecho Penal han intentado formular una noción de delito que sirviese para todos los tiempos y en todos los países. Esto no ha sido posible dada la íntima conexión que existe entre la vida social y la jurídica de cada pueblo y cada siglo, aquélla condiciona a ésta.

Según el ilustre penalista CUELLO CALÓN los elementos integrantes del delito son:

a)el delito es un acto humano, es una acción (acción u omisión)

b)dicho acto humano ha de ser antijurídico, debe lesionar o poner en peligro un interés jurídicamente protegido

c)debe corresponder a un tipo legal (figura de delito), definido por la ley, ha de ser un acto típico.

d)el acto ha de ser culpable, imputable a dolo (intención) o a culpa (negligencia) y una acción es imputable cuando puede ponerse a cargo de una determinada persona

e)la ejecución u omisión del acto debe estar sancionada con una pena.

Por tanto, un delito es: una acción antijurídica realizada por un ser humano, tipificado, culpable y sancionado con una pena.

Se podría definir el delito informático como toda acción (acción u omisión) culpable realizada por un ser humano, que cause un perjuicio a personas sin que necesariamente se beneficie el autor o que, por el contrario, produzca un beneficio ilícito a su autor aunque no perjudique de forma directa o indirecta a la víctima, tipificado por la ley, que se realiza en el entorno informático y está sancionado con una pena.

Contemplado el delito informático en un sentido amplio se pueden formar varios grandes grupos de figuras delictivas claramente diferenciadas:

a)delitos contra la intimidad
b)delitos contra el patrimonio
c)falsedades documentales.

El Código Penal vigente, al que nos referiremos a partir de ahora, fue aprobado por la Ley Orgánica 10/1995 de 23 de noviembre.

Delitos contra la intimidad

El Título X, Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio, dedica su Capítulo Primero, que comprende los artículos 197 al 200, al descubrimiento y revelación de secretos.

Este Capítulo, aparte de otras materias, viene a regular, en sede penal, las infracciones que se cometan en el ámbito de la Ley Orgánica 5/1992, de 29 de octubre, LORTAD.

El artículo 197, en su punto 1, contempla la figura de quien para descubrir los secretos o vulnerar la intimidad de otro se apodera de mensajes de correo electrónico o cualesquiera otros documentos. Aquí entendemos que, a tenor de lo que dispone el artículo 26 de la Ley, se encuentra comprendido cualquier tipo de documento electrónico.

En el mismo punto también se comprende la interceptación de las comunicaciones, la utilización de artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen o de cualquier otra señal de comunicación. Pensamos que entre lo anterior se encuentra el pinchado de redes informáticas. Es importante advertir que en este punto no se hable para nada de datos de carácter personal ni de datos automatizados, a los que se refiere el mismo artículo en el punto siguiente, sino a secretos y a vulneración de la intimidad en general.

El punto 2 del artículo se refiere específicamente a datos de carácter personal pero abarcando no sólo como actualmente hace la LORTAD,

los ficheros informáticos, electrónicos o telemáticos sino también los ficheros convencionales.

"Las mismas penas se impondrán al que, sin estar autorizado, se apodere, utilice o modifique, en perjuicio de tercero, datos reservados de carácter personal o familiar de otro que se hallen registrados en ficheros o soportes informáticos, electrónicos o telemáticos, o en cualquier otro tipo de archivo o registro público o privado. Iguales penas se impondrán a quien sin estar autorizado, acceda por cualquier medio a los mismos y a quien los altere o utilice en perjuicio del titular de los datos o de un tercero."

En los puntos siguientes del artículo las penas se agravan si los datos se difunden, revelan o ceden. Asimismo se sanciona a quien conociendo su origen ilícito y sin haber tomado parte en el descubrimiento los difunda, revele o ceda.

El hecho de que quien cometa el delito sea el encargado o el responsable del fichero agrava la pena.

Existen unas circunstancias agravantes que se dan en función de:

a)el carácter de los datos: ideología, religión, creencias, salud, origen racial y vida sexual

b)las circunstancias de la víctima: menor de edad o incapaz.

El hecho de que se persiga un fin lucrativo igualmente eleva la pena.

La condición de autoridad o funcionario público agrava las penas dada la situación de privilegio en que actúa (art. 198).

Delitos contra el patrimonio

Los delitos contra el patrimonio y contra el orden socioeconómico figuran en el Título XIII.

Es importante, en el dominio en que nos movemos, lo que se dice en el artículo 239, al tratar de las llaves falsas, al considerar llaves las tarjetas, magnéticas o perforadas, y los mandos o instrumentos de apertura a distancia.

Así las tarjetas magnéticas sustraídas a sus propietarios se considerarán llaves falsas. Es importante esta consideración en relación con el artículo 238 en el que para calificar un delito de robo con fuerza en las cosas es necesario que concurra alguna de varias circunstancias entre las que se encuentra el uso de llaves falsas.

Entre los delitos contra el patrimonio se encuentran: la estafa informática, las defraudaciones, los daños informáticos y la propiedad intelectual.

Estafas informáticas (art. 248.2)

La estafa se puede definir[2] como el perjuicio patrimonial realizado con ánimo de lucro mediante engaño.

El engaño es elemento necesario de este delito. Consiste según CUELLO CALÓN, en aprovecharse del error provocado o mantenido por el agente en la persona engañada.

Hasta la entrada en vigor del nuevo Código Penal ha sido difícil reconducir determinados fraudes informáticos hacia la figura de la estafa debido a la inexistencia del elemento de engaño a una persona.

El punto 2 del artículo 248 dice: "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 tercero."

Defraudaciones (art. 256)

Se considera defraudación el uso, sin consentimiento de su titular, de cualquier equipo terminal de telecomunicación.

■[2] EUGENIO CUELLO CALÓN. Derecho Penal II (Parte Especial. Volumen segundo). Bosch. Barcelona 1972. pág. 914.

Daños informáticos (art. 264.2)

Según el artículo 264.2 se sanciona "al que por cualquier medio destruya, altere, inutilice o de cualquier otro modo dañe los datos, programas o documentos electrónicos ajenos contenidos en redes, soportes o sistemas informáticos."

Entre esas situaciones se pueden incluir los famosos virus informáticos, bombas lógicas, "hackers" y "crackers".

Propiedad intelectual (arts. 270, 271 y 272)

Los delitos relativos a la propiedad intelectual e industrial, al mercado y a los consumidores se contemplan en el Capítulo IX.

"Artículo 270. Será castigado con la pena de prisión de seis meses a dos años o de multa de seis a veinticuatro meses quién, con ánimo de lucro y en perjuicio de tercero reproduzca, plagie, distribuya o comunique públicamente, en todo o en parte, una obra literaria, artística o científica, o su transformación, interpretación o ejecución artística fijada en cualquier tipo de soporte o comunicada a través de cualquier medio, sin la autorización de los titulares de los correspondientes derechos de propiedad intelectual o de sus cesionarios.

La misma pena se impondrá a quien intencionadamente importe, exporte o almacene ejemplares de dichas obras o producciones o ejecuciones sin la referida autorización.

Será castigada también con la misma pena la fabricación, puesta en circulación y tenencia de cualquier medio específicamente destinada a facilitar la supresión no autorizada o la neutralización de cualquier dispositivo técnico que se haya utilizado para proteger programas de ordenador."

Es interesante advertir que no sólo se sanciona la fabricación o puesta en circulación sino la simple tenencia de un dispositivo para saltarse las llaves lógicas o las famosas "mochilas".

Se elevan las penas si el beneficio obtenido es cuantioso o el daño causado es grave y además se inhabilita al autor del delito para el ejercicio de la profesión relacionada con el delito cometido (art. 271).

Estos artículos son, en sede penal, la respuesta a esa lacra de nuestro tiempo que es la piratería informática.

Ésta resulta muy dañina para el desarrollo informático pero entendemos que sólo con la amenaza de una sanción penal no se soluciona el problema. Es necesaria una labor educativa pues hasta que no hayamos convencido al infractor que cuando está copiando ilegalmente un programa de ordenador es como si estuviese robando la cartera a otra persona difícilmente se hallará solución. Insistimos resulta vital esa labor educativa.

Delitos de falsedades

Las falsedades se contemplan en el Título XVIII del Código. La asimilación que hace el artículo 387 de las tarjetas de débito y de crédito a la moneda es muy importante de cara a la defensa de éstas frente al ataque criminal de que están siendo objeto.

En el artículo 386 se sanciona su falsificación y puesta en circulación.

A la falsificación de los documentos públicos oficiales y mercantiles y de los despachos transmitidos por los servicios de telecomunicación se dedica la Sección 1ª del Capítulo II de este Título (arts. 390 a 395 y 400). El artículo 26 permite la aplicación de estos artículos cuando los documentos sean electrónicos.

Dada la dinamicidad de los sistemas informáticos resulta muy importante aunque a veces resulte muy difícil obtener las pruebas necesarias.

6. Los contratos informáticos

El contrato informático, según DAVARA RODRÍGUEZ[3] "es aquél cuyo objeto es un bien o un servicio informático - o ambos - o que una de las prestaciones de las partes tenga por objeto ese bien o servicio informático."

No existe un numerus clausus de los contratos informáticos y pueden seguir multiplicándose, lo que viene sucediendo en función de los avances técnicos y de su mayor utilización por la sociedad.

Los contratos informáticos se suelen dividir en tres grandes grupos: "hardware", "software" y servicios.

Entendemos que esta división no responde ya a la realidad y para una mayor clarificación del problema y una mayor homogeneidad esta clasificación se debe ampliar del siguiente modo:

1.Contratación del "hardware"
2.Contratación del "software"
3.Contratación de datos
4.Contratación de servicios
5.Contratos complejos.

Hasta el presente, el tercer grupo dedicado a los servicios venía siendo una especie de cajón de sastre donde iban a parar todos los contratos que no se referían específicamente al "hardware" o al "software". Así contemplábamos en ese grupo la comercialización de los datos y una serie de contratos de cierta complejidad que comprendían en sí mismos aspectos de "hardware", de "software" y de servicios.

[3] MIGUEL ÁNGEL DAVARA RODRÍGUEZ. Derecho Informático. Aranzadi. Pamplona. 1993. pág. 211.

I Contratación del "hardware"

El objeto de la contratación en esta clase de contratos es el "hardware", o sea, la parte física del ordenador y de sus equipos auxiliares.

Este tipo de contratos no suele presentar problemas específicos. Los contratos más usuales son los siguientes:

a) compraventa
b) arrendamiento
c) arrendamiento financiero ("leasing")
d) mantenimiento.

II Contratación del "software"

Ya nos hemos referido a esta categoría de bienes anteriormente y a sus especiales peculiaridades. Los contratos más corrientes son los siguientes:

Desarrollo de software

Se trata del caso en que una persona física, un colectivo o una empresa crean un "software" específico, a medida para otro. El tipo de contrato puede ser: de servicios o de obra, mercantil o laboral.

Licencia de uso

Es el contrato en virtud del cual el titular de los derechos de explotación de un programa de ordenador autoriza a otro a utilizar el programa, conservando el cedente la propiedad del mismo. Esta autorización, salvo pacto en contrario, se entiende de carácter no exclusivo e intransferible.

Adaptación de un software producto

Se trata de la contratación de una licencia de uso de un producto estándar que habrá que adaptar a las necesidades del usuario.

Mantenimiento

El contrato de mantenimiento, en principio, tiene por objeto corregir cualquier error detectado en los programas fuera del período de garantía. Se consideran varios tipos de mantenimiento: correctivo, de adaptación, perfectivo y preventivo.

Garantía de acceso al código fuente

Es aquél que tiene por objeto garantizar al usuario el acceso a un programa fuente en el caso de que desaparezca la empresa titular de los derechos de propiedad intelectual. Consiste en el depósito del programa fuente en un fedatario público, que lo custodia, por si en el futuro es preciso acceder al mismo.

III Contratación de datos

El valor de la información en esa sociedad del saber a la que nos referíamos antes cada día aumenta. La comercialización de las bases de datos es ya muy importante y la apertura de esas autopistas de la información, de las que tanto se escribe, hará crecer exponencialmente ese mercado.

Los principales contratos son los siguientes:

Distribución de la información

El contrato de distribución, según PÁEZ MAÑÁ[4] "consiste en la comercialización de la base de datos, durante un cierto período de tiempo a cambio de un precio, lo que origina la obligación por parte del titular de la base de aportar los datos que deben hacerse accesibles a los futuros usuarios, en una forma adecuada para su tratamiento por el equipo informático del distribuidor, y ceder a este último, en exclusiva o compartidos con otros distribuidores, los derechos de explotación que previamente haya adquirido por cesión o transmisión de los autores de las obras."

[4] JORGE PÁEZ MAÑÁ. Bases de datos jurídicos. CSIC. Madrid. 1994. pág. 186.

Suministro de información

Mediante este contrato el usuario puede acceder, siempre que lo precise, a las bases de datos del distribuidor.

Compra

Es un contrato por el que el titular propietario de una base de datos vende a otro una copia de ésta con la posibilidad de que el adquirente, a su vez, pueda no sólo usarla sino mezclarla con otras propias para después comerciar con ellas. Todo ello, por supuesto, respetando lo dispuesto en la Ley 5/1992 (LORTAD).

Cesión

Es un caso parecido al anterior salvo que sólo se permite el uso por el cesionario de la base sin que se le permita la transmisión posterior.

Compra de etiquetas

En este caso no se permite al comprador la reproducción de las etiquetas y sí su empleo para envíos por correo.

IV Contratación de servicios

Los contratos de servicios informáticos más importantes son los siguientes:

- Consultoría informática
- Auditoría informática
- Formación
- Seguridad informática
- Contratación de personal informático
- Instalación
- Comunicaciones
- Seguros
- Responsabilidad civil.

V Contratos complejos

Los contratos complejos son aquéllos que contemplan los sistemas informáticos como un todo incorporando al objeto del mismo, tanto el "hardware" como el "software" y algunos servicios determinados. Los más usuales son los siguientes:

Contratación global o parcial de servicios informáticos ("outsourcing")

Se trata de la subcontratación de todo o de parte del trabajo informático mediante un contrato con una empresa externa que se integra en la estrategia de la empresa y busca diseñar una solución a los problemas existentes.

Contrato de respaldo ("back-up")

Su finalidad es asegurar el mantenimiento de la actividad empresarial en el caso de que circunstancias previstas pero inevitables impidan que siga funcionando el sistema informático.

Contrato de llave en mano ("turn-key-package")

En esta clase de contratos el proveedor se compromete a entregar el sistema creado donde el cliente le indique y asume la responsabilidad total de diseño, realización, pruebas, integración y adaptación al entorno informático del cliente tanto lógico como físico.

Contrato de suministro de energía informática

Como señala GETE-ALONSO y CALERA[5] es: "aquél mediante el que una parte - el suministrador - poseedor de una unidad central que permanece en sus locales, pone a disposición del usuario la misma, lo que le permite el acceso al "software", a cambio de un precio."

■[5] MARÍA DEL CARMEN GETE-ALONSO y CALERA. La contratación en materia informática. La Ley núm. 3005. Madrid. mayo 1992 pág. 10.

Es muy importante el examen de los contratos por el auditor. Desgraciadamente muchos contratos informáticos existentes no tienen validez legal alguna. El objeto del contrato en algunos casos no está claramente determinado y hemos tenido que corregir algunos que solían terminar etc. etc.

7. El Intercambio Electrónico de Datos

En la época en que vivimos todas las organizaciones, tanto privadas como públicas, deben mejorar su productividad examinando los diferentes factores que pueden influir en los resultados.

Entre estos factores se encuentra como de especial importancia la reducción de costes, la agilización administrativa y la eliminación de errores. Esto se puede mejorar eliminando intermediarios entre el origen y el destino de los datos.

Fruto de esta necesidad de comunicarse con rapidez y seguridad en el mundo actual nace el Intercambio Electrónico de Datos conocido internacionalmente por sus siglas en inglés EDI (Electronic Data Interchange) que es un sistema informático que permite las transacciones comerciales y administrativas directas a través del ordenador, sin necesidad de realizar ningún trámite. Significa ahorro de tiempo y de papel.

Podemos definir el EDI como el intercambio de datos en un formato normalizado entre los sistemas informáticos de quienes participan en transacciones comerciales o administrativas.

Un sistema de este tipo ha de cumplir tres requisitos básicos:

- el intercambio se ha de realizar por medios electrónicos
- el formato tiene que estar normalizado
- la conexión ha de ser de ordenador a ordenador.

En un sistema EDI son las aplicaciones informáticas de las empresas o de las Administraciones Públicas las que "dialogan" entre sí sin necesidad de intervención humana.

Significa, y esto es lo que nos interesa, el reemplazo del papel, como elemento sustancial de la vinculación y comunicación negocial por un soporte informático.

Las razones que se pueden esgrimir para la implantación del EDI son:

- Precisión
- Velocidad
- Ahorro
- Beneficios tangibles
- Satisfacción del cliente.

El EDI es aplicable en el comercio, la industria, el transporte y las diferentes Administraciones Públicas.

La aceptación legal del EDI es un tema de suma importancia, sin duda detrás de la organización del mismo subyace un entendimiento entre las partes que intervienen que están dispuestas a aceptar una serie de obligaciones y de renunciar a ciertos derechos a efectos del buen funcionamiento del sistema.

Estos derechos y obligaciones se plasman en los correspondientes contratos: el contrato de intercambio de información y el contrato con las compañías de comunicaciones.

8. La transferencia electrónica de fondos

Una Transferencia Electrónica de Fondos (a partir de ahora TEF) puede significar muchas cosas. Si consideramos un concepto amplio de la misma puede abarcar todo tipo de envíos de fondos que se realicen por medios electrónicos.

Se puede definir como la transferencia de fondos que de forma automática es ejecutada inmediata y simultáneamente a la orden dada por el titular de la cuenta bancaria por medio de un sistema electrónico.

Podemos considerar que existen cuatro tipos principales de TEF que han ido apareciendo en el tiempo, conviven y son operativos en la actualidad:

- Transferencias entre entidades financieras
- Transferencias entre otras organizaciones y las entidades financieras
- El usuario colabora y mediante las tarjetas de plástico y los cajeros automáticos obtiene una serie de servicios bancarios
- Se potencia el sistema con terminales en los puntos de venta y el banco en casa.

Por su gran trascendencia social nos referiremos a continuación al fenómeno de las tarjetas de plástico.

Las tarjetas de plástico o tarjetas como medio de pago, por ahora las denominaremos así, con su continuo y ascendente desarrollo, se están convirtiendo en un medio de pago cada vez más importante en el tráfico mercantil sustituyendo poco a poco al dinero papel y el cheque.

La Unión Europea siempre sensible a aquellos problemas que puedan tener alguna trascendencia de cara a la creación del mercado único y asimismo a la constitución de la Europa de los ciudadanos ha dedicado una Comunicación, dos Recomendaciones y una Directiva a los sistemas de pago electrónico, su normalización e interoperabilidad.

Aunque existen notas comunes entre los diversos tipos de tarjetas, la diferenciación entre ellas viene dada por su contenido contractual (derechos y obligaciones) con independencia de la denominación que les otorgue la entidad emisora.

Tarjetas propiamente de crédito

Son aquellas, que como su nombre indica, proporcionan un crédito al titular de la misma.

Tarjetas de débito

Emitidas por Entidades de Crédito permiten a sus usuarios realizar compras en los establecimientos comerciales y a la vez ofrecen una gama de operaciones bancarias. En principio no están limitadas a un solo establecimiento comercial vinculando necesariamente la tarjeta a una cuenta

corriente bancaria. Estos dos tipos de tarjetas nos permiten utilizar los cajeros automáticos y los terminales puntos de venta.

El Código Europeo de Buena Conducta en materia de pago electrónico contenido en la Recomendación de 8 de diciembre de 1987 respecto a los contratos dice:

"a)Los contratos celebrados entre los emisores o su representante y los prestadores o los consumidores revestirán la forma escrita y deberán ser objeto de una petición previa. Definirán con precisión las condiciones generales y específicas del acuerdo.

b)Se redactarán en la/s lengua/s oficiales del Estado miembro en que se haya celebrado.

c)Cualquier tarifación del baremo de cargas se fijará con transparencia teniendo en cuenta las cargas y riesgos reales y no supondrá ningún obstáculo a la libre competencia.

d)Todas las condiciones, siempre que sean conforme a la Ley, serán libremente negociables y se establecerán claramente en el contrato.

e)Las condiciones específicas de rescisión del contrato se precisarán y comunicarán a las partes de la celebración del contrato."

En síntesis lo que se busca en esta Recomendación es transparencia y que dadas las condiciones en que se establecen estos contratos, la parte más fuerte no salga beneficiada.

En el mundo empresarial la implantación de estas nuevas tecnologías por parte de las Entidades Financieras ha favorecido una evolución histórica en el concepto de lo que era la tesorería en las empresas que ha pasado de ser una tesorería puramente administrativa a ser una tesorería de gestión que puede y debe generar beneficios por sí misma.

El conocimiento inmediato de posiciones y operaciones y la transferencia casi instantánea permite reducir provisiones y al mismo tiempo situar el dinero en el lugar donde más produzca.

9. La contratación electrónica

En una primera aproximación al tema por contratación electrónica o contratación por medios electrónicos se puede entender todo intercambio electrónico de datos o documentos cuyo objeto sea la contratación.

Sin embargo en todos ellos no se pactan las cláusulas del contrato en el mismo momento del intercambio electrónico. Así vemos en los epígrafes anteriores que tanto el intercambio electrónico de datos (EDI) como la transferencia electrónica de fondos (TEF) son el resultado de un macrocontrato anterior realizado por el sistema tradicional en el que las partes han fijado los términos del mismo y en el que muchas veces lo que hacen es renunciar a una serie de posibles derechos.

En este epígrafe nos referiremos a otro tipo de contratación electrónica; aquélla en la que el contrato se establece en el momento de la transacción electrónica sin que necesariamente con anterioridad se haya pactado nada entre las partes contratantes.

M. SCHAUS[6] dice que en la formación del contrato estas nuevas tecnologías influyen desde tres ópticas diferentes:

- desde el grado de inmediatez
- desde la calidad del diálogo
- desde la seguridad.

Desde el grado de la inmediatez

En nuestro derecho existe disparidad de criterios entre el Código civil y el de Comercio a la hora de determinar en qué momento se perfecciona el contrato.

■[6] M. SCHAUS. Formación de contratos. Comunicación de la oferta y de la aceptación al oferente. La validez de los contratos internacionales negociados por medios electrónicos. CECO. Madrid. 1988 pág. 21 y ss.

El artículo 1262 del Código civil dice: "El consentimiento se manifiesta por el concurso de la oferta y de la aceptación sobre la cosa y la causa que han de constituir el contrato. La aceptación hecha por carta no obliga al que hizo la oferta sino desde que llegó a su conocimiento. El contrato en tal caso, se presume celebrado en el lugar en que se hizo la oferta."

Por su parte en el artículo 54 del Código de Comercio se señala: "Los contratos que se celebren por correspondencia quedarán perfeccionados cuando los contratantes hubieren aceptado su propuesta."

Desde la calidad del diálogo

Entre los diferentes procedimientos existentes hoy día el que mayor se asemeja a un diálogo es la videoconferencia. En ella los interlocutores pueden apreciar no sólo el contenido del mensaje sino también la entonación, gestos y silencios.

El teléfono ofrece idénticas posibilidades excepto que los interlocutores no pueden verse.

Desde la seguridad

Desde el punto de vista jurídico el concepto de seguridad se refiere a la autentificación de la identidad del usuario y a las huellas que deja la transacción y que pueden ser utilizadas como prueba.

Vemos que del grado del cumplimiento de estos tres aspectos, admitiendo que se dan en la contratación electrónica, depende en gran parte su inclusión cómo una nueva forma de contratación, con sus peculiaridades, pero dentro de una ortodoxia contractual.

A fin de comprobar si existe un acuerdo de voluntades entre las partes contratantes a los efectos del art. 1261 del Cc. es importante clasificar los diferentes tipos de contratación electrónica que se pueden presentar en función de como actúa la parte contratante emisora y la parte contratante receptora. Para simplificar consideramos que ambas partes actúan de la misma forma, aunque no supondría ningún problema que esto no fuese así.

Sin desear ser exhaustivos consideramos que se pueden presentar los siguientes casos:

a)Comunicación entre dos ordenadores personales

b)Comunicación entre varios ordenadores personales a través de un Centro de Compensación

c)Comunicación entre dos sistemas informáticos

d)Comunicación entre varios sistemas informáticos mediante un Centro de Compensación.

Los casos b) y d) simplemente los apuntamos para dejar constancia de su existencia.

En los casos a) y b) el ordenador se limita a transferir una información que contiene una expresión de voluntad contractual.

En principio, salvo que existan problemas de autentificación, entendemos que esta voluntad transmitida forma parte de un negocio jurídico válido.

El problema se complica en los casos c) y d) cuando los que están en comunicación son dos sistemas informáticos (ordenadores) y lo que se transmite no se limita a ser sólo una información que incorpora una voluntad contractual sino que ésta puede venir alterada por una serie de aspectos que incorpora el propio sistema informático.

Problemas que se nos pueden presentar en la contratación electrónica y a la que no nos podemos referir por falta de espacio son: identidad de los contratantes, extensión o no de este tipo de contratación a todos los contratos , ¿cuándo y dónde se concluye el contrato?, autentificación, factor tiempo y confidencialidad.

Los avances tecnológicos y la adaptación del Derecho a estas nuevas situaciones deben superar los obstáculos que la generalización de esta forma de contratación presenta.

10. El documento electrónico

Es corriente identificar documento con soporte papel y escritura, pero vamos a demostrar que esto no siempre es así.

Para ROUANET MOSCARDÓ[7] un documento es: "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 voluntades (hecho voluntario, arte o negocio) o ser el resultado de una actividad o de un procedimiento."

PRIETO CASTRO define el documento como el objeto o materia en que consta por escrito una declaración de voluntad o de conocimiento o cualquier expresión del pensamiento, según resulta de los preceptos de la legislación positiva.

Los conceptos anteriores tienen en común que hablan de un escrito, aunque el último admite la excepcionalidad de que no lo sea.

Escribir, según el Diccionario de la Lengua Española, es: "Representar las palabras o las ideas con letras u otros signos trazados en papel u otra superficie."

Por tanto, el documento no ha de ser siempre papel, sino que puede ser otro objeto o materia y la representación de las palabras o las ideas puede hacerse por otros signos distintos de las letras.

Dichos signos pueden ser la codificación binaria y la superficie distinta del papel puede ser un soporte informático.

■[7] JAIME ROUANET MOSCARDÓ. Valor probatorio procesal del documento informático. Congreso sobre Derecho Informático. Facultad de Derecho. Zaragoza. 1989. Pág. 116.

De todo ello podemos deducir que el documento electrónico pertenece a la categoría de los documentos en sentido jurídico.

El problema para una aceptación generalizada de este tipo de documento puede estar en la necesidad de la seguridad de que la traducción del lenguaje máquina a un lenguaje natural sea el correcto y no en la propia esencia del documento.

Coincidimos con DAVARA RODRÍGUEZ cuando dice que el problema de la firma, que conlleva, en muchos casos, la autenticación del documento, puede ser sin duda, el caballo de batalla para una total aceptación a efectos probatorios de este tipo de documentos.

Un documento escrito está compuesto de datos y de impresión en un soporte. La impresión comprende, la mayoría de las veces, la representación de un hecho y la firma.

La firma suele tener tres funciones: identificativa, declarativa y probatoria.

Esto significa que sirve para identificar quién es el autor del documento, declarar que el autor de la firma asume el contenido del mismo y permitir verificar si el autor de la firma es efectivamente aquel que ha sido identificado como tal en el acto de la propia firma.

Notas importantes de la firma son la habitualidad y ser autógrafa u ológrafa, puesta de puño y letra por el firmante.

Hasta el presente este ha sido uno de los principales sistemas de autentificación, aunque no el único; pero en el futuro tendrá que ser sustituido en numerosas ocasiones. Los avances tecnológicos están obligando a que la firma manuscrita sea sustituida por otro sistema, en este caso electrónico.

Una firma digital o electrónica es una señal digital representada por una cadena de bits. Este tipo de firma ha de ser secreta, fácil de producir y de reconocer y difícil de falsificar.

En el caso de la firma manuscrita el fedatario público da fe de la autenticidad del documento. El empleo de la firma digital obliga a la aparición de

una nueva figura: el fedatario público. Éste ha de ser capaz de verificar la autenticidad de los documentos que circulan a través de las líneas de comunicaciones.

En cualquier caso los avances tecnológicos que se están produciendo quizás en un futuro cercano hagan aconsejable darle un carácter autónomo a este tipo de prueba con todos los problemas que esto pueda traer.

11. El fenómeno Internet

Los medios de comunicación y algunas empresas interesadas por obtener nuevos mercados han comenzado a hablar de Internet como si se tratase de un fenómeno que acabase de producirse.

Pero esto no es así, si queremos bucear en los orígenes de Internet tenemos que retroceder a finales de 1969. En aquella época, recordemos en plena guerra fría entre los países occidentales y la URSS y sus naciones satélites, el Departamento de Defensa de los Estados Unidos estaba preocupado por las consecuencias que podría tener para los intereses americanos un corte en sus sistemas de comunicaciones que cada vez iban alcanzando mayor importancia para la defensa del país tanto en el aspecto preventivo como de reacción ante un hipotético ataque enemigo.

Para obviar el posible problema los investigadores norteamericanos pensaron que los sistemas de comunicaciones debían tener una estructura de tela de araña de forma que si una vía quedaba bloqueada se pudiese seguir enviando la información a través de las restantes.

Fruto de esta necesidad nació ARPANET (Advanced Research Project Agency) con fines militares y estrecha colaboración con el mundo universitario, no hay que olvidar las generosas inversiones que realiza el Departamento de Defensa norteamericano en algunas de las más prestigiosas universidades del país.

ARPANET empezó conectando los ordenadores de cuatro instituciones universitarias: la Universidad de California en Santa Bárbara, la Universidad de California de los Ángeles, el Instituto de Investigaciones de la Universidad de Stanford y la Universidad de Utah. Su orientación investigadora

atrajo a una gran cantidad de científicos de centros docentes y de investigación que encontraron en la Red un medio revolucionario de mantenerse al día y de divulgar conocimientos así como resolver dudas y de esta forma pasó a ser una gran red de redes. Posteriormente terminó por escindirse en una red de carácter militar y el resto una red de carácter civil.

El crecimiento de esta tela de araña que poco a poco iba envolviendo el globo terráqueo hizo que se incorporaran como usuarios gentes de distinta procedencia especialmente del mundo universitario y esto iba creando una propia filosofía de lo que ya se empezó a llamar Internet. La falta de mercantilismo, una ética propia y de algún modo ciertos tintes ácratas configuraban el comportamiento dentro de la red.

Internet, en su aspecto físico, es la interconexión de millares de redes de ordenadores mediante un protocolo de comunicaciones común, que permite el intercambio de ficheros entre dos ordenadores situados en diferentes sitios en cualquier lugar de la Tierra, sin más restricción que la velocidad de las transmisiones.

Desde un punto de vista social Internet es un medio de comunicación bilateral directa y, hasta el momento libre, entre individuos e instituciones, más ágil que el propio teléfono, porque permite el intercambio de textos y multimedia. También puede ser un tipo de comunicación múltiple: la información que se transmite se puede ofrecer a un solo individuo determinado por medio del correo electrónico o dejarla a disposición de todos en la red.

Lo que debe estar claro es que Internet como entidad es algo abstracto que no pertenece a nadie.

La difusión de Internet y su crecimiento, de carácter exponencial, han hecho de ésta un lugar idóneo para los negocios y poco a poco se está convirtiendo en un gran zoco virtual global.

Es el vehículo ideal para diseminar ideas, imágenes, propaganda e informaciones de todo tipo de forma tan interactiva como se desee.

Sus características: virtual y global, le confieren una especificidad que va a tener gran importancia para el derecho.

El cambio que se produce en nuestra sociedad debido a este nuevo, mejor dicho a la extensión de este nuevo, medio de relación es de tal importancia y relevancia que prácticamente queda implicado el derecho en su conjunto y con la precaridad de tener que aplicar derechos nacionales a problemas supranacionales y aún debiéramos decir de trascendencia mundial.

Así vemos que en el cambio social que se origina están implicados: el derecho mercantil debido a la proliferación de nuevos tipos de contratos mercantiles con la aparición del comercio electrónico; el derecho fiscal incapaz muchas veces de hacer frente a la imposición en paraísos que ya podemos considerar virtuales, por ejemplo, en los casinos electrónicos; el derecho civil con los continuos ataques a la propiedad intelectual, cuya propia existencia se cuestiona; el derecho penal con la aparición del terrorismo a través de la red y la pornografía infantil entre otros delitos; el derecho financiero con el nacimiento del ciberdinero; el derecho constitucional con los ataques a la intimidad de las personas en las múltiples transmisiones transnacionales; el derecho internacional en su conjunto dadas las colisiones de derechos nacionales que se producen y el protagonismo que adquiere el principio de territorialidad; el derecho político con la utilización de la red con fines electorales y la publicidad que pueden hacer pequeños grupos minoritarios; el derecho procesal ante los nuevos tipos de prueba que aparecen debido a las tecnologías que emergen, en fin, como vemos, cualquier rama del derecho queda alterada ante esta nueva situación.

En definitiva, Internet está empezando a ser un fenómeno social que tiende a modificar en parte muchos de los conceptos que afectan a la sociedad, no sólo en materia de comunicación, sino también en las relaciones entre individuos, comunidades, empresas, etc. y esto, como sabemos, afecta profundamente al derecho.

DAVARA RODRÍGUEZ, en una obra reciente[8] dice: "Son las telecomunicaciones avanzadas, con el apoyo en el desarrollo tecnológico, las que tienen que proporcionar la herramienta para dar respuesta acertada al caos social que se está viviendo. Ahora bien, es necesario que esto sea comprendido por

[8] MIGUEL ÁNGEL DAVARA RODRÍGUEZ. De las autopistas de la información a la sociedad virtual. Aranzadi. Pamplona. 1996. pág. 189.

aquellos que tienen en sus manos mayores posibilidades de actuación en la orientación y desarrollo del marco en el que se moverán estas telecomunicaciones.

La necesidad de salir de la angustiosa situación social y económica que se nos avecina tiene el caldo de cultivo adecuado para lograr esta transformación social sin traumas mediante la adaptación de una nueva cultura en todos los ámbitos sociales y económicos que permita, aprovechando la coincidencia con el avance de las Tecnologías de la Información y las Comunicaciones, activar los impulsos en beneficio de un desarrollo social más justo y digno."

PÉREZ LUÑO dice[9]: Los juristas debemos realizar un esfuerzo para superar la tendencia congénita a escanciar el vino nuevo de las cuestiones que emergen del cambio social y tecnológico en los odres viejos conceptuales y metódicos de la dogmática jurídica tradicional. De no actuar así se corre el riesgo de operar desde las coordenadas metodológicas condenadas ab initio a la obsolescencia."

En resumen, vemos que nos encontramos ante una herramienta muy poderosa, reciente en su implantación generalizada, que es barata, accesible desde cualquier punto de conexión a la red telefónica, incluida la móvil, y prácticamente independiente de las distancias. Estas características la configuran como un marco ideal para conseguir la generalización del comercio y evitar en alto grado la intermediación entre otros posibles beneficios.

12. Responsabilidades de los auditores informáticos

La responsabilidad viene originada por la existencia de un daño y la idea de que ese daño tiene que ser reparado.

Si los actos no están penados por la Ley, la reparación al perjudicado da lugar a la responsabilidad civil; si el quebrantamiento es del orden

[9] ANTONIO ENRIQUE PÉREZ LUÑO. Manual de Informática y Derecho. Ariel Derecho. Barcelona 1996. pág. 21.

jurídico establecido, la reparación procede de la sociedad y da lugar a la responsabilidad penal.

Los auditores informáticos en el ejercicio de su trabajo pueden incurrir en tres clases de responsabilidades: civil, penal y profesional.

Responsabilidad civil

Para ALBALADEJO[10] "los denominados hechos ilícitos son aquellos que causando un daño, hacen nacer la obligación de repararlo" y añade "siendo una persona culpable del daño que otra recibe, queda - como regla - obligada a reparárselo e incluso aun sin serlo lo queda también, excepcionalmente, en ciertos casos."

En la primera hipótesis, en cuanto que la responsabilidad se basa en la culpa del autor del acto, se habla de responsabilidad por culpa; en la segunda de responsabilidad objetiva, en cuanto que se responde no por ser culpable, sino por ser (en cierto sentido más o menos directo) causante (aun sin culpa) del daño.

Existen tres tipos de responsabilidad civil:

a)la contractual definida en el artículo 1101 del Código civil consecuencia del incumplimiento de una obligación previamente constituida

b)la extracontractual regulada por los artículos 1902 y siguientes del Código civil y

c)la responsabilidad civil delictual o derivada del delito originada por un acto delictivo tipificado en el Código Penal y regido por los artículos 1902 del Código civil y 109 a 126 del Código Penal.

■[10] MANUEL ALBALADEJO. Derecho civil II. Derecho de Obligaciones. Parte especial. Librería Bosch. Barcelona 1972. págs. 345 y ss.

La jurisprudencia de los Tribunales ha venido dando un giro espectacular en este tema. Para DÍEZ PICAZO[11]: "Tal vez esté latiendo una intuitiva preocupación, que es, a mi juicio, la raíz última del mero derecho de daños, la necesidad social de defender y de amparar a la persona frente a un maquinismo social desencadenado en beneficio de determinadas partes de la sociedad y sólo indirectamente de la totalidad de ella."

YZQUIERDO TOLSADA[12] matiza lo anterior diciendo que: "De este modo la indemnización cobra el aspecto de un imperativo social ineludible. Si el aforismo del sistema codificado era no hay responsabilidad sin culpa, la nueva realidad con sus exigencias de defensa vigorosa de la persona reclama una respuesta que tienda no ya a castigar los comportamientos negligentes o reprobables, sino a que las víctimas encuentren a toda costa un patrimonio responsable: que todo daño quede reparado."

En resumen lo que ha sucedido es que hemos pasado de la consideración de que no hay responsabilidad sin culpa a que todo daño quede reparado.

El auditor informático que ejerce la profesión sin depender de una empresa, como cualquier otro profesional en esas circunstancias, si es prudente, debe tomar un seguro de responsabilidad civil profesional.

Lo que puede suceder es que esto no sea fácil, toda vez que las aseguradoras carecen de "datos históricos" en esta profesión para en base a los mismos calcular la prima correspondiente.

En cualquier caso si se encuentra una aseguradora dispuesta a contratar el seguro, es importante tener presente la importancia de las Condiciones particulares del mismo.

■[11] DÍEZ PICAZO. Estudios sobre la jurisprudencia civil I. Madrid 1966. págs. 27 y ss.

■[12] MARIANO YZQUIERDO TOLSADA. La responsabilidad civil del profesional liberal. Teoría General. Reus Madrid 1989. pág. 4.

A continuación figuran algunas de las condiciones que es conveniente incluir en una póliza de este tipo:

a) Riesgos cubiertos. Se garantiza al Asegurado, dentro de los límites estipulados, el pago de las indemnizaciones de que pueda resultar civilmente responsable por daños patrimoniales ocasionados a terceros, debidos a errores, faltas o negligencias cometidos por sí mismo o personas de las que legalmente deba responder durante el ejercicio de su actividad profesional como informático.

b) También serán objeto de garantía las reclamaciones por daños materiales y corporales que se deriven de la utilización de inmuebles para el desarrollo de la función profesional, como propietarios o usuarios.

c) Serán igualmente objeto de garantía las reclamaciones por los daños, pérdidas y extravíos sufridos por los expedientes y documentos que se encuentren en poder del asegurado para el desarrollo de las gestiones que le sean encomendadas.

Es importante verificar qué tipo de riesgos excluye y asimismo las garantías que cubre.

La garantía por siniestro representa el límite máximo de indemnización por parte de la Compañía aseguradora en caso de siniestro, tanto por lo que respecta a un daño único que proceda de varios errores profesionales, como respecto a todas las consecuencias de un mismo error. Por ello, todos los pagos que deba realizar la Compañía aseguradora, sea cual sea el concepto que los motive, no podrán sobrepasar la cantidad máxima asegurada.

Es importante también tener en cuenta el límite temporal al que nos referimos en el siguiente epígrafe.

Responsabilidad penal

A diferencia de lo que ocurre con la responsabilidad civil en este caso es necesaria la voluntariedad del informático, por lo que vemos difícil que por el simple trabajo del auditor informático se pueda cometer un delito.

Responsabilidad profesional

De la responsabilidad puramente profesional se suele responder ante el colectivo legalmente constituido al que se pertenezca, ejemplo: Colegio de Abogados, Colegio de Médicos, etc. y responde al cumplimiento de un Código Deontológico que ha sido aceptado.

En el caso de los auditores informáticos el tema es más complicado al no existir un Colegio Profesional informático. Existe una Asociación profesional: la Organización de Auditoría Informática.

13. Los seguros informáticos

URÍA[13] define el contrato de seguro como aquél "contrato por el que una persona (asegurador) se obliga a cambio de una prestación pecuniaria (prima), a indemnizar a otra (asegurado), dentro de límites convenidos, los daños sufridos por la realización de un evento incierto."

Los seguros informáticos son aquellos que cubren los riesgos que se produzcan relacionados con los medios informáticos.

Los seguros informáticos pueden facilitar cobertura a estos tres grandes grupos de riesgos:

1)"hardware"
2)"software"
3)responsabilidad civil.

Los seguros informáticos del "hardware" se pueden referir entre otros a los siguientes posibles riesgos: fuego, agua, explosión, robo, electricidad, manipulación fraudulenta y suspensión del servicio de mantenimiento.

Respecto al "software" podemos encontrar los siguientes: errores de los consultores, errores de la instalación, errores de programación, errores de interoperabilidad, fraudes del personal, y suspensión del servicio de mantenimiento.

■[13] RODRIGO URÍA. Derecho Mercantil. Madrid 1974. pág. 557.

A los seguros de responsabilidad civil nos hemos referido en el epígrafe anterior.

Cuando se plantea la conveniencia de contratar un seguro es importante seguir una metodología parecida a la que enunciamos a continuación, no debemos olvidar que nos encontramos ante un caso más de resolución de problemas:

1°Identificar y analizar los riesgos que en el área informática puede sufrir la empresa
2°Evaluar los riesgos
3°Evaluar los costes de los seguros
4°En función de los puntos 2° y 3° preparar un Plan de Actuación.

La actuación puede ser:

a)Aumentar las medidas preventivas y de seguridad
b)Asumir el riesgo
c)Contratar el seguro
d)Combinar b) y c).

Póliza de seguro

Es importante hacer figurar en la póliza una serie de condiciones así como examinar detenidamente otras. Entre ellas: riesgos cubiertos, riesgos excluidos, límite máximo de indemnización, ámbito geográfico y límite temporal.

Respecto al límite temporal es conveniente comprobar la fórmula que se emplea:

a)"claims made": atiende las reclamaciones que se hagan dentro de la vigencia de la póliza con independencia de cuando ocurrió el hecho.

b)"loss ocurrence": atiende las reclamaciones de hechos que hayan ocurrido durante la vigencia de la póliza.

Puede ocurrir que exista un vacío asegurador en el que creyendo estar cubiertos frente a unos posibles riesgos, en realidad no estemos cubiertos.

El auditor informático deberá examinar las pólizas de los seguros informáticos suscritos y comprobar qué es lo que cubren.

14. Los dictámenes y peritajes informáticos

Los cambios tecnológicos que se están produciendo a gran velocidad con las consiguientes consecuencias jurídicas obligan a la existencia de personas peritas en estas materias que colaboren con la Justicia y la sociedad en la solución de los contenciosos que se produzcan.[14]

Indudablemente entre esas personas peritas en estas materias se encuentran los auditores informáticos.

Estos peritos deberán exponer sus conclusiones logradas a través de los oportunos peritajes en los correspondientes dictámenes e informes periciales.

Un dictamen es un informe escrito sobre una determinada materia que, debidamente motivado y razonado, es emitido por un profesional versado en la misma.

El dictamen ha de reunir las siguientes características: claridad, concisión, fundamentación y justificación.

En los dictámenes judiciales el perito no prueba en sí nada, no acredita ningún hecho, simplemente suministra al juez una base científica, técnica, artística o práctica para juzgar sobre aquello a lo que se refiere el dictamen.

■[14] Para más información sobre este epígrafe ver: EMILIO DEL PESO NAVARRO, MIGUEL ÁNGEL RAMOS GONZÁLEZ, CARLOS MANUEL FERNÁNDEZ SÁNCHEZ Y MARÍA JOSÉ IGNOTO AZAUSTRE. Manual de Dictámenes y Peritajes informáticos. Díaz de Santos. Madrid 1995.

La prueba pericial es apreciada por los jueces o tribunales según las reglas de la sana crítica (art. 632 Lec) y, por ello, es de libre ponderación por el tribunal.

Cada día es más importante la actuación de los peritos informáticos y no sólo ante los Tribunales de Justicia, sino ante las Cortes de Arbitraje o simplemente en casos de mediación.

15. Bibliografía

Revista Informática y Derecho 1. Contratos informáticos. Documento electrónico. Derecho a la intimidad. Inteligencia Artificial. Tecnologías de la Información. Terrorismo por computadora. Bases de Datos. Habeas Data. UNED. Centro Regional de Extremadura. Mérida. 1992.

Revista Informática y Derecho 2. El derecho de la prueba informática. Problemática y perspectivas. UNED. Centro Regional de Extremadura. Mérida. 1991.

Revista Informática y Derecho 4. III Congreso Iberoamericano de Informática y Derecho. Actas I volumen. UNED. Aranzadi. Mérida. 1994

Revista Informática y Derecho 5.

Revista Informática y Derecho 6 y 7. La protección de Datos personales. Acta II volumen

Revista Informática y Derecho 8. Tributación e informática. Documento electrónico. Informática y Filosofía del Derecho. Protección jurídica de las Bases de Datos. Informática jurídica documental. Informática y poder legislativo. Contratación informática. Jurimetría. UNED 1995

Revista Informática y Derecho 9, 10 y 11. II Congreso Internacional de Informática y Derecho. Actas volumen I. UNED 1996

Revista Informática y Derecho 12, 13, 14, y 15. II Congreso Internacional de Informática y Derecho (Actas II volumen 1996)

Encuentros sobre Informática y Derecho. 1990 – 1991

Encuentros sobre Informática y Derecho. 1992 – 1993

Encuentros sobre Informática y Derecho. 1994 – 1995

Encuentros sobre Informática y Derecho. 1995 – 1996

Encuentros sobre Informática y Derecho. 1996 – 1997

Facultad de Derecho e Instituto de Informática Jurídica de la Universidad Pontificia de Comillas (ICADE). Aranzadi. Pamplona.

Alvarez Cienfuegos Suárez, José María
La informática en el ámbito de la Administración de Justicia. Actualidad Informática Aranzadi núm. 4. Julio 1992.

Barriuso Ruiz, Carlos
Interacción del Derecho y la Informática
Dykinson, Madrid 1996

Carrascosa López, Valentín
La protección de los datos personales. Regulación nacional e internacional de la seguridad informática. Centre d' Investigacio de la comunicació i Unversitat Pompeu Fabra. Generalitat de Catalunya, 1993

Davara Rodríguez, Miguel Ángel
Derecho Informático. Aranzadi. Pamplona, 1993

De las autopista de la información a la sociedad virtual. Aranzadi. Pamplona, 1996

Heredero Higueras, Manuel
La ley Orgánica 5/1992, de Regulación del Tratamiento Automatizado de los datos de carácter personal. Comentarios y textos. Tecnos. Madrid, 1996

Orozco Pardo Guillermo.
Informática y propiedad intelectual. Actualidad Informática Aranzadi. Núm 19 Abril 1996

Paéz Maña, Jorge.
Bases de Datos Jurídicos. CSIC. Madrid 1994. Comentarios sobre algunas particularidades de las bases de datos jurídicas. Actualidad Informática. Aranzadi nº 16. Julio 1995.

Pérez Luño, Antonio Enrique.
Manual de Informática y Derecho. Ariel. Barcelona 1996.

Peso Navarro, Emilio del y Ramos González, Miguel Ángel.
Confidencialidad y seguridad de la Información: la LORTAD y sus implicaciones socioeconómicas. Díaz de Santos. Madrid, 1994

Peso Navarro, Emilio del y Ramos González, Miguel Ángel
Manual de Dictámenes y Peritajes Informáticos. Díaz de Santos, Madrid,

Piattini Velthuis, Mario y Peso Navarro, Emilio del. Editores (obra colectiva)
Auditoría Informática. Editorial Roma (próxima publicación)

Suñe Llinás, Emilio
Informática práctica para juristas y profesionales del mundo de las leyes. Seminario de Publicaciones Facultad de Derecho, Madrid, 1994

Trejo Delarbre, Raúl
La nueva alfombra mágica. Usos y mitos de Internet, la red de redes. Fundesco. Madrid, 1996.

Yzquierdo Tolsada, Mariano
La responsabilidad civil del profesional liberal. Teoría General. Reus. Madrid, 1989.

Auditoría Informática

MIGUEL ANGEL RAMOS GONZÁLEZ*

Doctor en Informática.
Socio-Director de Informáticos Europeos Extertos (IEE)

Sed quis custodiet ipsos custodes (Juvenal)

1. Introducción

Aunque habitualmente hablamos de Auditoría Informática, sería preferible hablar de Auditoría **en** Informática, como dicen muchos de nuestros colegas de Hispanoamérica. Al mismo tiempo hemos de ir adaptando la denominación a la realidad: **Auditoría de Sistemas de Información**; a algunos les faltará espacio en las tarjetas si quieren precisar más y dicen Auditor en Sistemas de Información (SI) y en Tecnología(s) de la Información (TI), pero ¿cuántos sistemas de información empresariales hoy día no están basados en TI?

* Miguel A. Ramos, Doctor en Informática (tesis sobre A.I.), CISA (Certified Information Systems Auditor por ISACF), del Comité Directivo de OAI - ISACA; profesor de A.I. en la Universidad Carlos III de Madrid. Coautor de libros técnicos. Socio Director de IEE - Informáticos Europeos Expertos. E-mail: mramos@iee.es.

Hace algunos años se hablaba en inglés de *EDP Auditor*: auditor en proceso electrónico de datos, pero también hablábamos de mecanización antes de eso. No se trata ahora de una modernización de términos sino de una **nueva orientación** de este tipo de auditoría, que puede abarcar globalmente los sistemas de información: la planificación, el grado de alineamiento con las estrategias de las entidades, cómo los SI y el aprovechamiento de las TI aportan ventajas competitivas a la entidad, la gestión de los recursos, y la medida de la rentabilidad de todo ello, que es quizá el único punto que personalmente temo cuando se nos sugiere por parte de los clientes a la hora de establecer objetivos de la auditoría: algunas entidades tienen detallados sus costes (contabilidad analítica), pero ¿cómo cuantificar los auditores en algunas semanas las ventajas y los beneficios si la propia entidad no ha podido hacerlo en toda su existencia?

2. Justificación

La Auditoría en Sistemas de Información como **función interna** está plenamente justificada en las entidades de cierto volumen o criticidad de sus operaciones, o simplemente más avanzadas en cuanto a planteamientos, y en esos mismos casos y en otros puede estar igualmente justificada la Auditoría en Sistemas de Información **externa**: ambas pueden complementarse, lejos de ser excluyentes.

Tanto la normativa como la auditoría son necesarias: una auditoría sin estándares y normas sería subjetiva y hasta peligrosa (aunque en SI es una situación habitual, que no normal); la existencia de normativa sin auditoría podría equivaler a la no existencia de la Guardia Civil de Tráfico, lo que incrementaría los accidentes, e iría convirtiendo la circulación en caótica y peligrosa.

Otros supuesto tan peligroso o más sería tratar de **impartir justicia sin leyes.**

Por tanto, los auditores estamos habituados a tener que auditar sistemas de información en entidades sin políticas, con un marco legal incompleto, y usando estándares internacionales, que a menudo los auditados ponen en tela de juicio porque no están obligados a cumplirlos.

En el panorama tecnológico cambiante que nos ha tocado vivir los **riesgos** varían a gran velocidad según aparecen nuevas modalidades de proceso, pero

también surgen **nuevos controles, técnicas y herramientas,** si bien es aún largo el camino que queda en la protección.

A modo de reflexión ¿cuántas entidades disponen de políticas y procedimientos adecuados, así como de mecanismos para revisar su cumplimiento? ¿cuántas de clasificación de la información? ¿de separación de entornos en cuanto a programas y datos? ¿cuántas han asignado "propietarios" de ficheros, tienen plan de continuidad a diferentes niveles, realizan auditorías de los S.I...?

Vendrían bien algunas estadísticas, que por ahora no se tienen.

En definitiva, como decía un cliente: "No pasan más cosas porque Dios es bueno", y no conocemos la mayor parte de las que pasan, porque ya se ocupan las entidades de que no se difundan.

3. Control, Auditoría, e Inspección

Podemos considerar, en este contexto, que un **control** aislado es una acción o actividad, o un conjunto de ellas, realizadas por uno o varios elementos: humanos, dispositivos... para prevenir, detectar o corregir errores o irregularidades que afecten al funcionamiento de algo.

Cuantos mejores controles tengamos -no es por tanto cuestión de número- mayor **fiabilidad** alcanzaremos, si bien debemos considerar también factores como **coste y productividad.**

Los grandes grupos de controles son los siguientes, además de poderlos dividir en manuales y automáticos, o en generales y de aplicación:

·Controles **directivos**, que son los que establecen las bases, como las propias políticas, o la creación de funciones: de administración de seguridad o auditoría de S.I. interna.
·Controles **preventivos**: antes del hecho, como la identificación de visitas o las contraseñas.

·Controles **de detección**, como determinadas revisiones de accesos producidos, o la detección de incendios.

·Controles **correctivos**, para rectificar errores o acciones intencionadas, como la recuperación de un archivo dañado desde una copia.

·Controles **de recuperación**, que facilitan la vuelta a la normalidad después de accidentes o interrupciones, como puede ser un plan de continuidad adecuado.

Debemos hablar también de **Objetivos de Control**, como declaraciones sobre el resultado final deseado o propósito a ser alcanzado mediante los procedimientos de control, como los recogidos en las publicaciones COBIT *(Control Objectives for Information and Related Technologies)* de ISACA *(Information System Audit and Control Association / Foundation)*.

Cada entidad ha de definir sus propios objetivos de control, y crear y mantener un **Sistema de Control Interno** (funciones, procesos, actividades, dispositivos...) que puedan garantizar que se alcanzan y se cumplen los objetivos de control.

La auditoría puede considerarse el "control del control", como una línea de defensa más.

Además de quienes ejercen funciones de control o de auditoría de S.I. podemos encontrar otros órganos o grupos relacionados como: Auditores financieros u operativos, Inspección de Hacienda, Inspección del Banco de España (para entidades financieras), Inspección de la Agencia de Protección de Datos (para los de carácter personal), auditores informáticos venidos de otros países en el caso de multinacionales, auditores de calidad, o administradores de la seguridad.

Los auditores somos los **"ojos y oídos" de la Dirección**, que a menudo no puede, o no debe, o no sabe, cómo realizar las verificaciones o evaluaciones.

En los informes se recomendará la implantación o refuerzo de controles, y en ocasiones incluso que se considere la supresión de controles, si son redundantes o ya no son necesarios.

Se debe valorar qué cuesta implantar -y mantener- un control, frente al coste de no implantarlo.

El **sistema de control interno** se basa en las políticas, y en parte se puede implantar con apoyo de herramientas, si bien encontramos a menudo que lo que existe es más bien la implantación basada en el criterio de los técnicos, pero no sustentada en normativa, o habiendo partido ésta de los propios técnicos, sin aprobaciones de otro nivel.

El control interno no está aún generalizado en España fuera de los procesos que implican pagos, pero existen otros riesgos tan importantes o más que las pérdidas monetarias directas, relacionados con la gestión adecuada de los recursos informáticos o con la protección de la información, que en este último caso podrían suponer responsabilidades y pérdidas muy importantes para la entidad.

Si existe un sistema de control interno adecuado los procesos de auditoría, especialmente si son periódicos, son revisiones que requieren menos esfuerzo, con informes más breves; si el sistema de control interno es débil, la auditoría llevará más tiempo, su coste será mayor, y las garantías de que se pongan en marcha las recomendaciones son mucho menores; en ocasiones la situación dista tanto de lo aceptable como la del paciente que se somete a un chequeo después de varios años sin control.

Más difícil que entre control y auditoría puede resultar matizar las diferencias entre **auditoría e inspección**, y no bastaría con decir que inspección es el concepto clásico y auditoría es un concepto anglosajón y de orientación moderna, aunque el término auditoría provenga del latín y los antiguos ya llevaran a cabo auditorías, al parecer principalmente escuchando las declaraciones de los auditados.

Hoy día es más común hablar de auditoría en las entidades privadas, y de inspección en las Administraciones Públicas, no habiendo calado aún el enfoque de auditoría, con alguna excepción como el grupo existente en el Ministerio de Economía y Hacienda, integrado por Inspectores de la Hacienda Pública.

También podemos preguntarnos las afinidades entre consultoría y auditoría de S.I.

4. Áreas que puede abarcar la Auditoría

En realidad el concepto que tienen muchos respecto a la auditoría de S.I. no es exacto, y a menudo la confunden con **la auditoría de cuentas con ayuda del ordenador**, si bien es claro que el objeto a examinar en ese caso son los estados contables, balances y otros documentos y aun ficheros de ordenador (incluso con ayuda de paquetes) pero no deja de ser el ordenador el medio o la herramienta, no el objeto.

Simplificando podríamos decir que la auditoría de S.I. es la revisión de éstos y de su entorno, y ello no implica que haya que usar el ordenador: puede tratarse por ejemplo de una auditoría de funciones, de desarrollo de aplicaciones, de gestión de proyectos, etc.

Aunque a veces se asocia auditoría de S.I. con auditoría de la seguridad, y ésta es la función inicial de muchas áreas de auditoría de S.I. interna, la auditoría puede abarcar muchas otras áreas cómo hemos señalado, y de hecho es difícil determinar qué áreas no podría abarcar, sobre todo si se entra en la auditoría de la gestión de los propios S.I.

Una vez centrado el tema, a modo de descripción más que de definición formal se propone:

La auditoría de sistemas de información puede comprender:

la revisión, análisis y evaluación independiente y objetiva, por parte de personas independientes y técnicamente competentes de:

el entorno informático de una entidad, abarcando todas o algunas de sus áreas, como (sin que sea con carácter excluyente):

equipos,
sistemas operativos y paquetes,
aplicaciones y el proceso de su desarrollo,
organización y funciones,
las comunicaciones,
la propia gestión de los recursos informáticos,
la calidad de procesos y productos
las políticas, estándares y procedimientos en vigor en la entidad, su idoneidad así como el cumplimiento de:

dichas políticas, estándares y procedimientos,
los objetivos fijados,
los planes,
los presupuestos,
los contratos y las normas legales aplicables,

el grado de satisfacción de usuarios y directivos,
los controles existentes,
un análisis de los posibles riesgos relacionados con la Informática.

Como consecuencia de la revisión y examen ha de emitirse un **informe escrito** que resuma la situación desde un punto de vista independiente y objetivo y, en su caso, dicho informe ha de incluir deficiencias e indicación de mejoras.

Una de las utilidades indirectas de la auditoría de sistemas de información es el apoyo a la auditoría de cuentas, ya que hoy día la mayoría de los entornos cuentan con equipos informáticos para su gestión.

Es evidente que en general **no puede considerarse totalmente fiable** una auditoría de cuentas de un entorno informatizado que no vaya acompañada de una auditoría informática, que asegure que todo el proceso de los datos así como los propios programas están razonablemente exentos de error y de fraude. Para el auditor sin conocimientos técnicos es como encontrarse con una "caja negra".

5. El auditor en S.I.

El **perfil** que se requiere para llevar a cabo auditorías de sistemas de información no está regulado, pero es evidente que es necesaria una formación y sobre todo una experiencia acordes con la función, e incluso con las áreas a auditar: seguridad, desarrollo de aplicaciones, gestión... además de ser imprescindibles en el perfil otras características o circunstancias como independencia respecto a los auditados, madurez, capacidad de análisis y síntesis, e interés no meramente económico.

En el seno de la citada ISACA existe un certificado relacionado: **CISA** *(Certified Information Systems Auditor).*

Otro punto a considerar al crear la función interna es si se forma a técnicos en

auditoría general o se forma a auditores en otras áreas en auditoría en S.I. La independencia se consigue en parte ubicando la función en el lugar adecuado del organigrama, fuera en todo caso del área de S.I., circunstancia que no se cumple en gran número de entidades en España.

6. Auditoría de la Seguridad

Como decíamos, en algunos casos se llega a confundir auditoría con seguridad, e incluso hemos encontrado a personas que ostentaban ambas funciones a la vez, lo que es ilógico e incompatible.

La seguridad es una de las áreas objeto de la auditoría de S.I. pero en absoluto la única ni en todos los casos la más importante: podrían estar los datos y los sistemas muy seguros, y sin embargo por ejemplo estar sin cubrir las necesidades de la entidad, porque las aplicaciones y las inversiones en SI y TI se hubieran realizado sin alineamiento con las estrategias de negocio o de servicio de la entidad.

Desde la perspectiva de la auditoría de la seguridad es necesario revisar si se han considerado las **amenazas**, o bien evaluarlas si es el objeto, y de todo tipo: errores y negligencias en general, desastres naturales, fallos de instalaciones, o bien fraudes o delitos, y que pueden traducirse en daños a personas, datos, programas, redes, instalaciones, u otros, y llegarse a traducir en un peor servicio, imagen degradada, e incluso pérdida irreversible de datos.

Debemos pensar que las medidas deben considerarse como **INVERSIONES en seguridad**, aunque en algunos casos se nos diría que no es fácil reflejarlas como activos contables y que cual es su rentabilidad; podemos estar de acuerdo, pero ¿cuál es la rentabilidad de blindar la puerta de acceso a nuestro domicilio, o la de instalar un antirrobo sofisticado en nuestro coche? Esa rentabilidad la podemos determinar si los dispositivos o controles han servido para evitar la agresión, y a veces habrá constituido una medida disuasoria y no llegaremos a enterarnos de su efecto positivo.

En todo caso la seguridad tiene un impacto favorable en la **imagen** de las entidades, aunque ello sólo no suela justificar sus costes, y tanto para clientes y posibles clientes como para los empleados. Unos y otros pueden sentirse más protegidos, así como considerar más protegidos sus activos.

Y la protección no ha de basarse sólo en dispositivos y medios físicos, sino en **formación e información** adecuada al personal, empezando por la **mentalización** a los directivos para que, en "cascada", afecte a todos los niveles de la pirámide organizativa.

Algunos autores se refieren a los accidentes no humanos como *actos de Dios*; cuando ha habido intervención humana en muchos casos ha participado alguien de la propia entidad afectada, al menos facilitando información sobre controles existentes y sus debilidades. Cuando los sistemas informáticos son el fin más que el medio se suele distinguir entre el ***cracker***: alguien que quiere entrar en los sistemas para hacer daño, y el ***hacker***: quien intenta acceder a los sistemas más para demostrar (a veces sobre todo para demostrarse a sí mismo/a) de qué es capaz, y que puede superar las barreras de protección que se hayan establecido, más que por hacer daño, aunque finalmente todos lo hagan de una forma más o menos directa.

Frente a ello en la auditoría se recomiendan controles, que debieran poder fundamentarse en la **seguridad jurídica**, si bien todavía hay muchos aspectos que nuestras leyes no recogen: no se exige hacer copias de seguridad, por ejemplo, aunque son evidentes los riesgos de no hacerlo, y de forma especial cuando las amenazas se han traducido en incidencias.

Debieran también apoyarse los controles, en segundo término, en lo que podemos denominar **seguridad organizativo - administrativa**, consistente en políticas, normas y procedimientos, separación de funciones, funciones específicas como administración de seguridad o la propia de auditoría interna, designación de propietarios, clasificación de la información, y otras.

En relación con la **separación de tareas**: es peligroso que una misma persona realice una transacción, la autorice, y revise después los resultados (un diario de operaciones, por ejemplo), porque podría planificar un fraude o encubrir cualquier anomalía, y sobre todo equivocarse y no detectarse; por ello deben intervenir funciones / personas diferentes y existir controles suficientes.

Después ya podemos llegar a otros controles más extendidos **de seguridad física y lógica.**

En un proceso de auditoría, por tanto, se evaluarán estos aspectos, y otros como si la seguridad es realmente una preocupación corporativa: que exista

presupuesto para ello no es suficiente, si las personas a diferentes niveles están mentalizadas; que exista una ***cultura* de la seguridad**, si hay un comité que fije o apruebe los objetivos correspondientes y en qué medida se alcanzan, qué modelo de seguridad se quiere implantar o se ha implantado, qué políticas y procedimientos existen: su idoneidad y grado de cumplimiento, así como la forma en que se realiza el desarrollo: en un entorno seguro y con inclusión de controles en las aplicaciones, si el proceso se lleva a cabo igualmente en un entorno seguro: separación de programas y separación en cuanto a datos, si los seguros cubren los riesgos, pero sin que sea ésta la única medida de protección, y si está prevista la continuidad de las operaciones en el caso de incidencias.

En ocasiones la entidad está en medio de un proceso de implantación de la seguridad, y la evaluación normalmente abarcará qué proyectos hay en curso, y un contraste de los objetivos y los medios usados o previstos.

Aunque no es posible en esta ocasión profundizar en todos los puntos sí queremos incluir algunos comentarios sobre algunos de ellos: en cuanto a **evaluación de riesgos** en general, se trata de evaluar la probabilidad de que algo ocurra y el impacto o pérdida que puede suponer; para ello disponemos de listas, que podemos incluir en hojas de cálculo, o bien usamos paquetes, y tal vez en el futuro sistemas expertos. El problema sigue siendo la adaptación de los puntos a cada caso: tales como actividad, dimensión, tipo de datos, y plataformas, y asignar el peso que puede tener cada uno de los puntos.

En el informe se explican los diferentes puntos, e incluso se clasifican por importancia, y la entidad decide qué acciones tomar y con qué prioridad, a veces en función de sus disponibilidades de recursos, o bien según qué planes tenga que puedan afectar, como puede ser la sustitución de equipos o de aplicaciones.

Lo mejor sería poder **eliminar los riesgos** en todos los casos, pero normalmente lo más que conseguimos es disminuir o la probabilidad de que algo se produzca o bien su impacto: con sistemas de detección, de extinción, mediante revisiones, o bien copiando ficheros críticos, exigiendo una contraseña, u otros controles según los casos.

Los manuales hablan de ***transferir*** los riesgos, por ejemplo contratando un seguro, pero debemos recordar que si se nos pierden los datos la entidad aseguradora nos dará el importe estipulado -si no puede agarrarse a alguna cláusula en letra pequeña- pero seguiremos sin recuperar los datos.

Finalmente otra posibilidad es **asumir los riesgos**, pero debe hacerse a un nivel adecuado en la entidad, y considerando si puede ser mayor el coste de la inseguridad que el de la seguridad, lo que a veces sólo se sabe cuando ha ocurrido algo. ¿Cuál es el máximo admisible de riesgo que puede permitirse una entidad? Depende de lo crítica que sea para ella la información y disponer de ella, e incluso puede depender del momento: es un tema tan grave que no puede generalizarse la respuesta ni decidirla un administrador de seguridad.

Volviendo a los **aspectos físicos**, que son una de las barreras más visibles, hay puntos a considerar en la auditoría, desde el emplazamiento del centro de procesos o de los servidores y terminales, el control de accesos, el uso de llaves, protecciones frente al fuego, agua, vandalismo, robo, y hasta la continuidad de la energía; respecto a la continuidad en general es fundamental disponer de copias actualizadas en un lugar adecuado.

Además de la identificación física, y como paso siguiente, existe la identificación y autenticación que denominamos lógica, generalmente mediante contraseña, si bien si se sigue produciendo un abaratamiento progresivo se puede empezar a utilizar la **biométrica**.

Podemos decir que una **contraseña** es un conjunto de caracteres que sólo debe conocer el propio usuario, y que sirve para dar acceso a recursos tales como todo un sistema, ficheros o bases de datos concretos, programas, transacciones, o incluso el acceso físico.

Puntos a considerar en relación con las contraseñas:

·La contraseña debe ser **fácil de recordar** por el verdadero usuario, para evitar que la tenga que escribir, y **difícil de imaginar por otros**.

·Si fuera necesario anotar la contraseña debe hacerse en lugares protegidos y preferiblemente disimulada entre otras anotaciones.

·En la mayoría de casos y entornos (no en todos) es preferible que **la asigne el propio usuario**, si bien siguiendo criterios adecuados.

·Para **evitar situaciones de bloqueo** el administrador ha de poder crear, con el debido control, usuarios con un perfil determinado en caso de emergencia, o bien existir éstos, y sus datos estar debidamente protegidos, incluida la propia

contraseña.

·Se debe **limitar el número de intentos** cuando el usuario marca la contraseña, previendo suplantaciones.

·En todo caso es necesario **investigar los intentos de acceso fallidos** para verificar si se trata de errores del usuario o intentos de suplantación.

·Las contraseñas han de tener una **vigencia limitada**, por ejemplo treinta días; incluso las puede haber de un sólo uso.

·En algunos sistemas se trata de hacer al usuario preguntas que otros no deberían conocer.

·Puede haber también otros **modelos pregunta / respuesta**, basados en una función matemática que se ha comunicado al usuario.

·Existen algunos sistemas o aplicaciones que incluyen usuarios y contraseñas "de fábrica", incluso con perfil de administradores, que deben variarse o protegerse, sobre todo cuando aparecen en los propios manuales.

·No deben aparecer en claro en las pantallas, ni en listados ni ficheros, en los que deben estar **cifradas**.

Criterios de asignación:

·En todo caso debe fijarse una **longitud mínima** según la criticidad de lo que se quiere proteger: el código que usamos para los cajeros de entidades financieras tiene 10.000 posibilidades (10^4), pero si ampliamos la longitud a seis, y utilizamos además de cifras las letras (unas 26 si el sistema no admite diferenciar mayúsculas y minúsculas) y algunos símbolos como *, $... (pensemos que hasta cinco símbolos) tenemos 41^6 posibilidades.

La realidad demuestra que a menudo se asignan palabras que están en un procesador de textos, con lo que alguien que conozca algunos de sus caracteres puede llegar a averiguar los restantes.

·Otra restricción aconsejable es **no admitir las "x" últimas asignadas**, para evitar que el usuario asigne de forma alternativa dos o tres contraseñas, lo que

disminuye la seguridad.

·Se puede elegir una letra (por ejemplo la primera) de cada palabra de una frase: refrán, título de una película...

·O bien tomar una palabra de un libro (incluso siempre del mismo) y del que anotamos página, línea y número de palabra, en vez de anotar la contraseña.

·Es evidente que ha de conocerla sólo el usuario y hay que evitar contraseñas de grupo o departamentales, para poder saber quién hizo qué (además de cuándo y desde dónde) y poder exigir responsabilidades.

Y una posibilidad ciertamente rebuscada pero que se da en forma de **"caballo de Troya"**, y especialmente peligrosa en un "PC" que emule un terminal: que alguien haya introducido un programa que simule el contenido de la pantalla de identificación al sistema, con los mismos mensajes, grabe la contraseña, haga creer al usuario que ha habido algún tipo de error y le haga repetir el proceso ya dentro del procedimiento normal, con lo que habrá recogido la contraseña (incluso de un administrador), sin que nadie haya sospechado.

Cuando las contraseñas formen parte de mensajes de comunicaciones pueden ir camufladas: partidas, en posición variable, y lo mejor de todo: cifradas mediante algoritmos criptográficos.

El **cifrado** es una de las medidas más eficaces si se usa bien y se eligen adecuadamente los sistemas, la longitud de las claves, y su distribución; puede usarse no sólo en las comunicaciones sino también para proteger los soportes magnéticos que haya que trasladar -incluso por seguridad- y especialmente si lo hacemos por canales menos fiables: para evitar la copia no autorizada o interceptación del soporte.

Los métodos de los romanos: **sustitución** de caracteres de un alfabeto (en todo el mensaje la A por la L, la M por la S...) o **transposición** (por ejemplo la primera letra pasa al lugar de la quinta, la cuarta al segundo lugar del texto...) resultarían hoy pueriles, sobre todo usando los propios ordenadores para el criptoanálisis.

Los métodos modernos son mucho más complejos y sus algoritmos más sofisticados, aunque en muchos casos basados en la sustitución y transposición,

pero a nivel de "bits" y con todos los caracteres ASCII o EBCDIC.

El más extendido en aplicaciones comerciales, aunque muy discutido en los últimos años, es el DES (**"Data Encryption Standard"**) que IBM desarrolló con el nombre interno de "Lucifer". Es de clave privada y simétrico, es decir la clave para descifrar es la misma que para cifrar.

Entre los sistemas asimétricos de clave pública destaca **RSA** (de sus autores "Rivest, Shamir, Adleman"), basado en las propiedades de los números primos relativos y los residuos cuadráticos.

Puede cifrarse por "hardware" y por "software".

Las interceptaciones en las comunicaciones ("pinchados") pueden ser pasivas: sólo lectura, o activas: variación de contenido.

Deben limitarse los intentos de acceso para evitar que accedan suplantadores por intentos sucesivos, y en algunos casos es preferible establecer una **llamada de retorno**: el sistema identifica al usuario que quiere acceder y le obliga a "colgar" para ser el propio sistema el que llama a la dirección registrada como válida.

En el caso de las **redes locales**, son aplicables muchos de los controles de las grandes redes, además de establecer controles específicos de prevención y detección de virus y proteger la configuración de manera que los usuarios sólo puedan realizar las funciones autorizadas, en cuanto a cambios, carga de programas, transferencia de ficheros, y otras, para evitar fugas de datos, introducción de virus y carga o copias "pirata" de programas.

Al hablar de seguridad siempre se habla de sus tres dimensiones: confidencialidad, integridad y disponibilidad de la información, y algunos controles van más dirigidos a tratar de garantizar una (o dos) de estas características.

- La **confidencialidad**: se cumple cuando sólo las personas autorizadas (en un sentido amplio podríamos referirnos también a sistemas) pueden conocer los datos o la información correspondiente.

Podemos preguntarnos ¿qué ocurriría si un soporte magnético con los datos de los empleados o clientes o pacientes de una entidad fuera cedido a terceros? ¿cuál podría ser su uso final? ¿habría una cadena de cesiones o ventas

incontroladas de esos datos?

La **LORTAD** (Ley Orgánica de Regulación del Tratamiento Automatizado de Datos de carácter personal) ha influido positivamente en concienciarnos respecto a la confidencialidad.

- La **integridad**: consiste en que sólo las personas autorizadas puedan variar (modificar o borrar) los datos. Además deben quedar pistas para control posterior y para auditoría.

Pensemos que alguien variara datos de forma que perdiéramos la información de determinadas deudas a cobrar (o que sin perderla tuviéramos que recurrir a la información en papel), o que modificara de forma aleatoria la última parte de los domicilios de algunos clientes.

Algunas de estas acciones se podrían tardar en detectar, y tal vez las diferentes copias de seguridad hechas a lo largo del tiempo estarían "viciadas" (corruptas se dice a veces), lo que haría difícil la reconstrucción.

- La **disponibilidad**: se alcanza si las personas autorizadas pueden acceder a tiempo a la información a la que estén autorizadas.

El disponer de la información después del momento necesario puede equivaler a la falta de disponibilidad. Otro tema es disponer de la información a tiempo pero que ésta no sea correcta, e incluso que no se sepa, lo que puede originar la toma de decisiones erróneas.

Otro caso grave es la ausencia de disponibilidad absoluta, por haberse producido algún desastre. En ese caso, a medida que pasa el tiempo el impacto será mayor, hasta llegar a suponer la falta de continuidad de la entidad, como ha pasado en muchos de los casos producidos (más de un 80% según las estadísticas).

Por tanto, **los datos son uno de los activos** que más y mejor debemos proteger, hasta el punto de que en muchas multinacionales la función que conocemos como administración de seguridad se llama *data security:* es necesaria la designación de propietarios, clasificación de los datos, restricción de su uso para pruebas, inclusión de ***muescas*** para poder detectar usos no autorizados, así como aprovechar las posibilidades del Sistema de Gestión de Bases de Datos que se esté

utilizando.

Uno de los primeros pasos que deben dar las entidades es la clasificación de la información: definición de unos cuantos niveles y asignación de categorías, como pueden ser: Pública (no clasificada), Confidencial o Restringida, Secreta, e incluso de Alto Secreto ("TOP SECRET"), además de pendiente de clasificar.

De este modo se podrá definir qué pueden conocer los empleados de tal departamento, o restringir la variación de determinados datos a tal función.

Decíamos que la **LORTAD** ha supuesto un impulso a la protección de datos en España, sobre todo en algunos sectores, a pesar de que aún está pendiente el Reglamento de Seguridad.

Deben establecerse controles en la entrada, proceso y salida de los datos, e incluso después respecto al tiempo que hay que conservarlos y si es necesario finalmente destruirlos, y tanto en soporte magnético, como papel u otros.

En los casos de transacciones más críticas se puede exigir la revisión por un supervisor independiente antes del proceso.

En cuanto a las **bases de datos** existen unos criterios generales, además de recomendaciones específicas según sean bases de datos documentales, orientadas a objetos, distribuidas, con datos críticos, muy volátiles...

Cuando se trata de bases de datos con diferentes niveles de confidencialidad e integridad se pueden usar bases de datos multinivel, que permiten etiquetar los elementos de datos, y que usuarios o grupos de usuarios con distintos niveles de acceso tengan vistas diferentes de la misma base de datos.

Como sobre todo en las entidades grandes y medias los sistemas se basan en redes de redes, con conexiones internas y externas, es necesario proteger y controlar los sistemas frente a posibles **transferencias de ficheros**, ya que los datos que pueden estar perfectamente protegidos en equipos centrales, una vez que son transferidos a redes con menor protección pueden a su vez transferirse a equipos de uso personal e incluso portátiles.

En relación con ello se va imponiendo la identificación y autenticación únicas ***(single sign-on)***, y el intento de que los datos viajen por diferentes plataformas

con la misma *etiqueta* de seguridad que hayan podido tener inicialmente según su clasificación.

Otro aspecto es la **protección de los programas**, al menos desde dos perspectivas: de los programas que sean propiedad de la entidad, realizados por el personal propio o contratados a terceros, y el uso adecuado de aquellos programas de los que se tenga licencia de uso, pero este tema se tratará en otra ponencia expresamente y por un verdadero especialista.

Es necesario hablar de **virus**, que hace años era un problema que se relacionaba con el uso de programas *no legales*, y cuya incidencia ha disminuido aunque nunca hay que bajar la guardia: la disminución en buena medida se debe al uso progresivo de programas *legales*, aunque aún estemos lejos de los niveles de otros países, a las medidas preventivas generales, y al uso de herramientas de prevención y detección, lo que supone en las redes un gran esfuerzo de administración y actualización, además del coste que suponen los propios paquetes, hasta el punto de que en muchos casos se protege sólo el servidor, y a nuestro juicio se debe completar la situación con la existencia de normas adecuadas y la posibilidad de responsabilizar al usuario.

Existe un riesgo constante porque de forma continua aparecen nuevas modalidades de virus (a menudo en países distantes) que no son detectadas por los programas antivirus hasta que las nuevas versiones los contemplan. Y un riesgo adicional es que los virus pudieran llegar a impactar los grandes sistemas, sobre todo a través de las redes, pero esto es realmente difícil -no nos atrevemos a decir que imposible- por las características y complejidad de los grandes equipos y de sus sistemas operativos.

Un último aspecto a considerar en la auditoría de la seguridad, ya citado, es la **continuidad:** que en el caso de incidencias de diferente impacto las operaciones de la entidad puedan reanudarse -incluso no interrumpirse- en un plazo inferior al fijado, según la criticidad de las aplicaciones. En relación con ello es necesario revisar en la auditoría si se han determinado los registros vitales -y la información es uno de ellos- y las aplicaciones que la procesan, y los sistemas de proceso y redes son necesarios también. A la vez se suele revisar el denominado plan de evacuación, que afecta más directamente a las personas, y que puede existir con independencia del anterior, y con carácter general en la entidad o edificio.

Los activos se deben proteger pensando en los intereses de los accionistas, de

los clientes, y también pensando en los empleados y en los proveedores.

7. Auditoría de la Gestión

Es una de las áreas más novedosas para los auditores, hasta el punto de que a veces en los cursos nos preguntan, incluso profesionales con experiencia, si realmente tendrían que abordar también estas áreas.

Entre los **objetivos** pueden estar:

·Alineamiento y sincronización de las inversiones y uso de los sistemas de información con las estrategias generales de "negocio" o de servicio.

·Aportación de los S.I. y del aprovechamiento de las tecnologías de la información para conseguir ventajas competitivas.

·Cobertura de necesidades de cada área usuaria y nivel de servicio, frente al riesgo de que se vaya a la tecnología por la tecnología.

·Organigrama adecuado.

·Contratos.

·Calidad: de procesos y de productos.

·La llamada informática de usuario final, así como la existencia del gran almacén de datos *(Data Warehouse)* y su aprovechamiento, llegando a la minería de datos o *Data Mining.*

·Políticas, estándares y procedimientos relacionados con la gestión.

·Existencia y aportación de Comités.

·Gestión económica: costes, posible repercusión, rentabilidad.

Es necesario revisar lo que podemos llamar ***arquitecturas***: de datos, de aplicaciones, de equipos, y topología de comunicaciones.

8. Auditoría del Desarrollo de Aplicaciones

Algunos aspectos a revisar pueden ser: metodología seguida, normativa, grado de participación de los usuarios, entornos de desarrollo, lenguajes, herramientas, pruebas, calidad, productividad, costes, e incluso comparación con otros o con niveles medios o destacados *(benchmarking)*; y no sólo en el caso de desarrollos propios, sino desarrollos contratados o con equipos mixtos, e incluso los términos del contrato, o en el caso del uso de paquetes de aplicación.

El diseño y las pruebas tienen mucho que ver con la **calidad**, relacionada en muchos aspectos con la seguridad; así, deben probarse los módulos, rutinas y programas, realizar pruebas en cadena, de volumen o de "estrés", de aceptación (por parte de los usuarios, por la unidad de producción o explotación, y por el área de mantenimiento de aplicaciones), además de considerar la posibilidad de lanzar versiones alfa y beta, y realizar paralelos.

El uso o no de **datos reales** vendrá determinado por la clasificación de la información, y en el caso de usar datos reales debería "mimetizarse" su contenido.

El pase al entorno de explotación real debe estar controlado, no descartándose la **revisión de programas** por parte de técnicos independientes del proyecto, para determinar, además de la calidad, la ausencia de "Caballos de Troya", bombas lógicas y similares.

9. Auditoría de la Producción

Algunos aspectos a revisar son: el nivel de servicio frente a las necesidades de los usuarios, la capacidad de proceso, la planificación y control de la explotación, la posible repercusión de costes, la gestión de problemas y cambios, y la atención a usuarios.

10. Técnicas y métodos

En cada proceso de auditoría se fijan los objetivos, ámbito y profundidad, lo que sirve para la planificación, y para la consideración de las fuentes, según los objetivos. El factor sorpresa puede llegar a ser necesario en las revisiones, según

lo que se quiera verificar.

Como métodos y técnicas podemos considerar los cuestionarios, las entrevistas, la observación, los muestreos, las **CAAT** ***(Computer Aided Auditing Techniques)***, las utilidades y programas, los paquetes específicos, las pruebas, la simulación en paralelo con datos reales y programas de auditor, o la revisión de programas.

11. El informe

El informe debe ser escrito en todos los casos, y debe ir firmado.

En él deben constar los antecedentes, el objetivo del proceso de auditoría, los agradecimientos (si proceden), las posibles limitaciones, y un resumen para la Dirección, en términos no técnicos.

En cada punto que se incluya debe explicarse, siempre que sea posible, por qué es un incumplimiento o una debilidad, y alguna recomendación, a veces abarcando varios puntos.

El informe ha de discutirse con los auditados antes de emitir el definitivo.

En algunos casos, bien en el propio informe o en otro documento, se recogen las respuestas de los auditados.

La entidad decide qué acciones tomar, y en el caso de los internos suelen hacer también un seguimiento de las implantaciones.

Los auditados siempre buscan un informe lo más benigno posible, mientras que los auditores nos proponemos llegar a un informe veraz y útil; estos diferentes puntos de vista a veces crean conflictos en la discusión del informe.

12. Conclusión

La auditoría en S.I. no está suficientemente implantada en la mayoría de las entidades españolas, si bien supondría una mayor garantía de que las cosas se hacen bien y como la entidad quiere: en general hay coincidencia entre ambos

puntos. Puede ser también una profesión con futuro cuando la auditoría despegue.

Como función aporta al auditor un conocimiento privilegiado del área de S.I., con una perspectiva muy amplia.

El auditor, como cualquiera que esté relacionado con las tecnologías de la información, ha de mantener sus conocimientos al día.

La forma de realizar el trabajo va variando y se está llegando a aplicar el control por excepción y la teleauditoría.

En cuanto a nuevas áreas, surgen las relaciones con el **comercio electrónico** y el uso de SET *(Secure Electronic Transaction)*, e incluso en cuanto a las **páginas WEB**, y por algunos casos que se han producido, la revisión de quien autoriza, varía y controla los contenidos; cada vez es más necesaria la separación de dominios: en las entidades por seguridad y productividad, y en los hogares, aunque esto se sale de la auditoría y queda en el control, para evitar que los menores accedan a contenidos con violencia o pornografía.

Volviendo a las entidades, se están dando muchos casos de uso indebido de acceso a redes: en varias empresas de Estados Unidos muy conocidas se registraron más de cuatro mil accesos en 1996 sólo a la revista *Penthouse.*

Por último, dos aspectos que hay que tener muy en cuenta: la revisión de los sistemas en cuanto a su **adaptación al euro**, y la previsión del tratamiento adecuado al **año 2000**, que podría impedirnos entrar en el nuevo milenio con "buen pie"; ya se están produciendo errores: uno de los más leves el de un paciente de un centro sanitario de Madrid para el que el ordenador emitió un volante de pediatría ¡el paciente tiene 101 años! pero este problema se ha dado a menudo en diferentes sectores y mucho antes de que afecte el cambio de siglo y de milenio: debemos llegar al 2000 entusiastas, preparados y prevenidos.

13. ANEXOS

ORGANISMOS Y ENTIDADES RELACIONADOS

ANSEI (Asociación Nacional de Seguridad en Entornos Informáticos)
Tfno: (91) 722 50 40

ASIS (Sociedad americana para la Seguridad Industrial)
Génova, 3
28004 MADRID

AESPI (Asociación Española de Sociedades de Protección contra Incendios)
Tfno: (91) 411 27 56

Instituto de Auditores Internos
Montera, 24 - 4° A
28013 MADRID

OAI (Organización de Auditoría Informática), Capítulo Español de ISACA
Claudio Coello, 18
28001 MADRID

Secretariado de ISO **American National Standards Institute**
1430 Broadway
New York, NY 10018 Estados Unidos
Tel: 1-212-642-4900

Commission of the European Communities
Senior Officials Group - Information Systems Security Secretariat
DG X111F, TR61, 2/30
Rue de la Loi 200, B-1049 Bruselas BÉLGICA
Fax: +322-235-0654

Information Systems Audit and Control Association (ISACA)
(Antes Electronic Data Processing Auditors Association, Inc.)
3701 Algonquin Rd., Suite 1010

Rolling Meadows, IL 60008 Estados Unidos
Fax: 07-1-708-253-1443

Information Systems Security Association (ISSA)
4350 Dipaolo Ctr.
Glenview, IL 60025
Tel.: 1-708-699-6441
Fax: 1-708-699-6369

SIC (Seguridad en Informática y Comunicaciones)
Jorge Juan, 96 - Bajo 1
28009 MADRID

Cuadernos de Seguridad
Avda. de la Industria, 32, nave 2
28100 ALCOBENDAS (Madrid)

Selecciones Security Management (en español)
Edf. EULEN
Ctra. de La Coruña Km. 17,900
28230 LAS ROZAS (Madrid)
Tfno: (91) 631 08 00
Fax: (91) 631 08 51

Computer Fraud & Security Bulletin
Elsevier Advanced Technology, Mayfield House
256 Banbury Rd.
Oxford OX2 7DH Inglaterra
Tel +44-71-239-7764
Fax +44 (0) 865-310981

Computers & Security
Elsevier Advanced Technology, Mayfield House
256 Banbury Rd.
Oxford OX2 7DH Ingla

Computers Security Journal
Computer Security Institute
600 Harrison St.,
San Francisco, CA 94107 Estados Unidos
Tel: 415-905-2626
Fax: 415-905-2218

Auditor Journal
ISACA,
3701 Algonquin Rd., Suite 1010,
Rolling Meadows, IL 60008 USA
Phone 1-708-253-1545
Fax 1-708-682-4010

EDPACS -- The EDP Audit, Control, and Security Newsletter
Auerbach Publications, Warren Gorham Lamont,
210 South St.,
Boston, MA 02111-2797 Estados Unidos
Tel 1-617-423-2020

Information Systems Security
Auerbach Publications,
One Penn Plaza,
New York, NY 10119 Estados Unidos
Tel: 1-212-971-5005

ISSA Journal
Dain Gary, Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15212 Estados Unidos
Tel: 1-412-268-5724
Fax 1-412-268-6989

Security Management
American Society for Industrial Security,
1655 North Fort Myer Drive, Suite 1200,
Arlington, VA 22209 USA
Tel: 1-703-522-5800
Fax 1-703-243-4954

BIBLIOGRAFÍA

Abrams, M. D., Jajodia, S. and Podell, S. J. *Information Security.* IEEE Computer Security Press. 1995.

Acha Iturmendi. *Auditoría Informática.* Paraninfo. Madrid 1993/1994.

Alonso Rivas, Gonzalo. *Auditoría Informática.* (Editorial Díaz de Santos).

Baker, Richard H. *The Computer Security Handbook.* TAB Professional and Reference Books.

British Standards Institution. *A Code of Practice for Information Security Management.* Department of Trade and Industry, British Government. Londres, 1993

Bruce, Glen y Dempsey, Rob. *Security In Distributed Computing: Did You Lock the Door?.* Prentice Hall. 1996.

Caballero, P. *Introducción a la Criptografía.* RA-MA, Textos Universitarios, 1996.

Calle Guglieri, J.A. *Reingeniería y Seguridad en el Ciberespacio.* Ed. Díaz de Santos. Madrid, 1997.

Castano, S., Fugini, M., Maetella, G., Samarati, P. *Database Security.* Addison Wesley, 1994.

Chapman, D. B., Zwicky, E. D. *Building Internet Firewalls.* O´Relly & Associates, 1995.

Coelli, William, Longley, Dennis and Shain, Michael. *Information Security. Handbook.* Macmillan Publishers, Ltd.

Data Security Management. Auerbach.

Datapro Reports on Information Security. DATAPRO. McGraw - Hill.

Davara, Miguel Ángel. *De las Autopistas de la Información a la Sociedad Virtual.* Editorial Aranzadi. Pamplona, 1996.

Davies, D. W. and Price, W. L. *Security for Computer Networks.* John Wiley & Sons.

Del Peso, Emilio y Ramos, Miguel A. *Confidencialidad y Seguridad de la Información: la LORTAD y sus Implicaciones Socioeconómicas.* Editorial Díaz de Santos, Setiembre 1994. Madrid.

Del Peso, Emilio, Miguel A. Ramos et al. *Manual de Dictámenes y Peritajes.* Editorial Díaz de Santos, Noviembre 1995. Madrid.

Dupont, Daniel G, and Richard Lardner. *The Culture of Secrecy.* Government Executive, vol. 27, nº 6. Junio, 1995.

EDP Auditing, AUERBACH

Eloff, J. H. P. and Von Sloms, S. H. *Information Security - the Next Decade.* Chapman & Hall. May, 1995.

Ford, Warwick. *Computer Communications Security: Principles, Standard Protocols and Techniques.* Prentice Hall. 1994.

Geyelin, Milo. *Why Many Businesses Can't Keep Their Secrets.* The Wall Street Journal, 20 Noviembre, 1995.

Ginn, Ron. *Continuity Planning.* Elsevier Advanced Technology.

Henry. M. *Practical Computer - Network Security.* Artech House, 1995.

Hughes, L. J. *Internet Security Techniques.* New Riders Publishing, 1995.

Hutt, Arthur E., Douglas B. Hoyt, y Seymour Bosworth. *Computer Security Handbook.* 3ª edición, 1995. John Wiley & Sons. Nueva York, 1995.

ISACA (Information Systems Audit and Control Association / Foundation). Varios libros editados.

----- *COBIT: Control Objectives for Information and Related Technology.* Abril, 1996.

IT security: the need for international cooperation. *Proceedings of the IFIP TCII International Conference on Information Security.* Singapur. Mayo, 1992

Kaufman, Charles, Perlman, Radia y Speciner, Michael. *Network Security: Private Communication in a Public World.* Prentice Hall. 1995

Longley, Dennis and Shain, Michael. *Data & Computer Security.* Macmillan Publishers, Ltd.

Morant, J.L., Ribagorda, A. T y Sancho, J. *Seguridad y Protección de la Información.* Editorial Centro de Estudios Ramón Areces. Madrid, 1994.

Murphy Michael A. y Parker Xenia L. *Handbook of EDP Auditing,* Warren, Gorham & Lamont

O'Shea, G. *Security in computer operating systems.* NCC Blackwell. Oxford, 1991.

Palmer, I.C. and Potter, G.A. *Computer Security - Risk Management.* Jessica Kingsley Publishers.

Perry, William E. and Kuong, Javier F. *EDP Risk Analysis and Control Justification.*

Pfleeger, Charles P. *Security in Computing, 2/E* . Prentice-Hall, 1996.

Piattini, M.G. *Control interno y auditoría en un entorno de bases de datos relacionales. Parte I y II.* Revista Base nº 21, noviembre 1992 y nº 22, abril 1993.

Prooceedings of the Sixth IFIP. International Conference on Computer Security and Information Intergrity. Helsinki - Mayo 1990.

RACF. Auditor's Guide. IBM.

Ramos González, MA. La seguridad y confidencialidad de la información y la LORTAD. *Actas XXII Curso de Informática y Derecho: Ley de Protección de Datos Personales.* UNED. Mérida, 1993.

----- La Auditoría de la seguridad informática. *Revista CHIP.* Marzo, 1992.

----- Contribución a la mejora de las técnicas de Auditoría Informática mediante la aplicación de métodos y herramientas de Ingeniería del Conocimiento. *Tesis Doctoral.* Facultad de Informática. Universidad Politécnica de Madrid.

----- La importancia de la seguridad informática en el ámbito empresarial. *Ponencias II Conferencia de Seguridad Informática.* Madrid, 1989.

----- Auditoría de la Seguridad: charlas en dos ediciones de Securmática
----- Auditoría (en) informática. *Seguridad informática.* Núm. 17. Noviembre, 1995.

----- La información como activo estratégico: seguridad y protección. *Selecciones de Security Management.* Núm. 75. Madrid, 1995.

----- La Auditoría Informática y el Reglamento de Seguridad de la LORTAD. Revista Seguridad Informática y Comunicaciones. Septiembre 1997 (en prensa).

----- Auditoría de la Seguridad. Capítulo en la obra Auditoría Informática coordinada por Del Peso, Emilio, y Piattini, Mario. Ed. RA - MA, Octubre 1997 (en preparación).

----- (Coautor de otras obras; vid. Del Peso...).

Ribagorda Garnacho, A. *Seguridad y Protección de la Información.* De este autor y de JL Morant y J. Sancho. Editorial Centro de Estudios Ramón Areces. Madrid, 1994.

----- *Glosario de Términos de Seguridad de las T.I.* Ediciones CODA. Madrid, Abril 1997.

R. Posch. *Communications and Multimedia Security.* Graz University of Technology, Austria. August 1995.

Sánchez, JI. e Ignoto, MJ. *La Seguridad Informática.* Manuales IMPI. Madrid, 1991.

SEDISI. *Guía de Seguridad Informática.* (Asociación Española de Empresas de Tecnologías de la Información). Abril, 1997.

Security. Module 9. Systems Auditability and Control. *The Institute Internal Auditors Research Foundation.* Altamonte Springs, 1991.

Simpson, Glenn R. *A '90s Espionage Tale Stars Software Rivals, E-Mail Spy.* The Wall Street Journal, 25 Octubre, 1995.

Siyan, K., Hare, Ch. *Internet Firewalls and Network Security.* New Riders publishing, 1995.

Stalling, William. *Network and Internetwork Security: Principles and Practice.* Prentice Hall. 1995

Tantam, Mark. *Computer Abuse Investigator.* Elsevier, 1991 (Gran Bretaña)

The EDP Audit, Control, and Security Newsletter. EDPACS. Auerbach Publications.

The Journal, revista de la ISACA.

Vallabhaneni, Rao. *Auditing computer security. A manual with case studies.* John Wiley & Sons, 1989.

Wong, Ken y Watt, Steve. *Managing Information Security.* Elsevier, 1990 (Gran Bretaña).

Wood, Charles Cresson. *A Policy for an Information Security Management Committee.* Computer Security Alert, nº 115. Octubre, 1992. Publisher: Computer Security Institute, San Francisco, CA, USA.

ALGUNAS DIRECCIONES "WEB"

//www.acl.com	Herramientas para auditoría
//www.aenor.es	Asociación Española de Normalización
//www.amazon.com	Libros
//www.ansi.org	American National Standards Institute
//www.auditserve.com	Artículos, noticias
//www.bibliomania.com	Libros
//www.booksatoz.com	Libros
//www.bookshop.com	Libros
//www.bookwire.com	Libros
//www.compubooks.com/books.html	Localización de libros de informática
//www.datapro.com	Datapro
//www.echo.lu	Comisión Europea
//www.elservier.com	Libros, revistas, congresos
//www.etsi.fr	European Telecomunications Standards Institute
//www.fundesco.es	Consulta catálogos de bibliotecas
//www.hp.com //www.hp.es	Hewlett Packard mundial / española
//www.ibm.com //www.ibm.es	IBM Mundial / española
//www.iee.es	IEE - Informáticos Europeos Expertos
//www.ifip.or.at	IFIP
//www.iso.ch	International Standards Organization
//www.it-ch.com	Chapman & Hall (Libros sobre TI)
//www.mec.es	Educación y Ciencia (+ información tesis: teseo)
//www.microsoft.com	
//www.ovum.com	Informes Técnicos
//www.rsa.com	Algoritmo de cifrado
//www.uned.es	Universidad Nacional de Educación a Distancia
//www.wiley.com	Libros técnicos

Medios eficaces en la lucha contra la Piratería

CARLOS MANUEL FERNÁNDEZ SÁNCHEZ*

Director de Programas Antipiratería de Microsoft

Estas breves reflexiones pretenden ser un mero apunte esquemático en el quede plasmado el planteamiento de la problemática que presenta la piratería informática y las consecuencias antisociales de la misma.

Introducción

Las Tecnologías de la Información (Hardware & Software) pertenecen al sector industrial que mayores índices de crecimiento han experimentado en las dos últimas décadas.

* Carlos Manuel Fernández Sánchez. Vicepresidente de la Organización de Auditoría Informática (OAI-ISACA). Delegado del comité Directivo de la BSA. (Business Software Alliance)

En los años 80 surge una revolución en el sector de la Informática con la llegada de los ordenadores personales y el software que se puede ejecutar en estos. Donde los paquetes de ofimática son los más representativos.

El éxito del denominado Software estándar (la Ofimática), se debe principalmente a la facilidad de uso y su bajo coste, esto implica una gran difusión de este tipo de Software. Las empresas fabricantes han dedicado grandes recursos humanos y económicos, a fin de crear herramientas de fácil manejo que permitan el uso del ordenador al mayor número de personas posible, facilitando el acceso a las tecnologías de la información, y por ende a la información misma destinada a un número de personas insospechado hasta entonces.

Detrás de cada programa de ordenador hay muchos años de investigación y desarrollo (I+D),que además repercute en la creación de nuevos empleos en este sector y/o reconversión de puestos de trabajo a otros de mayor cualificación.

Los avances de la informática supondrán una nueva era para todos los habitantes de nuestro globo como pronostican grandes Gurús de nuestro tiempo como Nicholas Negroponte en el "Mundo Digital" o el famosísimo multimillonario de la informática Bill Gates en sus recientes conferencias y encuentros que ha realizado por todo el mundo, por no citar a otros como Alvin Tofler, en sus recientes reflexiones sobre la red de redes "Internet"., vamos hacia un nuevo tipo de sociedad la "Sociedad de la Información", cualquier persona sobre este planeta tendrá toda la información que desee o necesite, la información llegará a todos los niveles de la sociedad. En este nuevo camino nos estamos encontrando con uno de los mayores obstáculos a los que se enfrenta el desarrollo del sector informático: la copia ilegal de programas de ordenador, lo que conocemos con el termino generalizado de Piratería Informática.

La práctica de utilizar o comercializar programas de ordenador de manera ilegal por parte de usuarios, revendedores y falsificadores tiene graves consecuencias para el sector informático y para la industria en general y por ende para la sociedad. Concretamente podemos citar las siguientes consecuencias negativas que inciden directamente en aspectos sociales y económicos.

Consecuencias negativas de la Piratería Informática.

Tomando como baremo el índice orientativo de piratería registrado para el año 1996 que es del 65% , es decir sólo el 35% del software utilizado en nuestro país es legal, (el índice medio de piratería en Europa occidental es del 43%), desde un punto de vista socio-económico se pueden citar como más significativas las siguientes consecuencias negativas de la piratería informática:

1.- Paralización de la inversión: no se generan nuevas inversiones (I + D) en el desarrollo y adaptación de programas futuros de ordenadores, especialmente con respecto a nuestro país, por desconfianza del sector informático al ser pirateados. Agravándose el problema en el mercado español, según estudio publicado por SEDISI y MINER , donde se detecta una baja tasa de penetración de las tecnologías de la Información en nuestro país. Así lo indica el ratio entre Gastos en T.I. y el Producto Interior Bruto, cuya media europea es de 2,08 mientras en España fue en 1995 de 1,18.

2.- No se crean empleos en el sector del software al ritmo que demanda la sociedad en comparación con el resto de países europeos: la copia ilegal de programas de ordenador estándar supone que cada año dejen de crearse miles de empleos.

Si el índice de piratería en España alcanzara la media europea occidental, se crearían 25.000 nuevos puestos de trabajo en este sector en 4 años. (Fuente: Informe sobre: "El Impacto de la Industria del Software en las Economías Europeas" . Elaborado por Price Waterhouse para la BSA (Business Software Alliance Septiembre, 1995)

3.-Perdidas económicas en el sector de la informática en España que se evalúan en torno a los 22.000 millones de ptas. (1996); con el gran impacto que supone para la Hacienda Pública, que deja de ingresar miles de millones en concepto de impuestos directos e indirectos, en detrimento de la sociedad española.

4.- Competencia Desleal, la comercialización de los programas de ordenador de forma fraudulenta tiene como consecuencia directa la competencia desleal y perjudicial para todo ese tejido de establecimientos de venta de productos de informática "PYMES de Informática" que ven como desaprensivos

no respetan las mínimas reglas del juego empresarial, poniendo a sus negocios al borde de la quiebra.

5.- Incumplimiento repetitivo de la Ley de Propiedad Intelectual (Ley de Protección de Programas de Ordenador), con unos efectos nocivos para la sociedad, como pueden ser respeto a los derechos de autor y como consecuencia respeto los demás.

6.- Carencia o degradación de valores ético profesionales en diferentes ámbitos o sectores de nuestra sociedad tales como el Universitario, Empresarial, etc. al no considerar la piratería informática como un robo.

7.- Proyección Internacional negativa: La imagen internacional de España con respecto a nuestro alto índice de piratería, supone que seamos considerados como un país tercermundista en el mundo de la informática.. La International Intellectual Property Association (IIPA) ha recomendado al gobierno de los Estados Unidos de América (U.S.A) que nos incluya en la Lista 301 (Watch List-Marzo 1997), donde aparecen recogidos todos aquellos países que transgreden la Propiedad Intelectual. Esto lleva aparejado gravísimas consecuencias para nuestras exportaciones al coloso Norteamericano y con ello para nuestro Comercio Exterior.

8.- Perjuicios para el consumidor: El comprador de buena fe se siente frustado y engañado al comprobar que el software que ha adquirido era pirateado y en consecuencia no tiene derecho a acceder al servicio y asistencia técnica de los productos ni a las posteriores versiones actualizadas de los mismos.

Todos estos factores negativos repercuten de manera nefasta en nuestra sociedad creando una desconfianza a la inversión y una falta de proyección del sector informático en nuestro país, que ve como las prácticas de piratería informática se multiplican alarmantemente; siendo las más usuales las que a continuación detallamos.

Prácticas más usuales de Piratería Informática

Las prácticas ilegales incorporan con increíble rapidez las novedades que aportan los avances tecnológicos, apareciendo hoy nuevos frentes en los que combatir la piratería informática.

El Hard Disk Loading (Carga de Software pirateado en el disco duro de los ordenadores nuevos, es decir software pirateado preinstalado), la copia de software pirateado en soporte de Diskette , la copia en soporte CD Rom y la piratería a través de Internet son los ejemplos más significativos del momento.

Las redes de comunicaciones por ordenador y la navegación por el ciberespacio se están introduciendo en las dinámicas de trabajo, en el entorno familiar e incluso, entre las alternativas para los momentos de ocio. No hay ninguna duda acerca de que la red multiplica enormemente las posibilidades de interrelación de los seres humanos pero es un hecho, que Internet abre un nuevo escenario para desarrollar nuevas formas de delincuencia informática.

Medidas de Protección Legal contra la Piratería Informática

Motivados e impulsados por las empresas fabricantes de software, los distintos ordenamientos jurídicos han intentado frenar las consecuencias negativas de este extendido fenómeno así, de forma paulatina los diferentes países han ido incorporando a sus sistemas jurídicos las medidas legislativas de protección que equiparan los programas de ordenador a las creaciones literarias.

Asimismo, en su articulado se expresan medidas especiales de protección, señalando que los Estados miembros deberán adoptar medidas adecuadas contra las personas que pongan en circulación una copia de programa de ordenador conociendo o pudiendo conocer su naturaleza ilegítima o que tengan con fines comerciales una copia de programa de ordenador, presumiendo igualmente ilícito.

Ocho gobiernos europeos han llevado a cabo la transposición de esta norma comunitaria a sus correspondientes legislaciones. Los gobiernos de Alemania, Dinamarca, España, Francia, Grecia, Irlanda, Italia y Reino Unido han adaptado nuevas leyes nacionales sobre la Propiedad Intelectual que refuerzan la protección jurídica de los programas.

En España, la protección jurídica de los programas de ordenador está regulada en dos ámbitos, el civil y el penal. El primero de ellos queda regulado por el Real Decreto Legislativo 1/1996, de 12 de Abril, por el que se aprueba el texto refundido de la Ley de Propiedad Intelectual, regulando, aclarando y armonizando las disposiciones legales vigentes sobre la materia.

Por otra parte, en los artículos 270 y siguientes del código penal de 1995 se recogen los delitos relativos a la propiedad intelectual, denotando el espíritu progresista de esta norma con la inclusión de un supuesto que sanciona, la circulación y tenencia de cualquier medio destinado a la supresión o neutralización de dispositivos utilizados para proteger los programas de ordenador.

La normativa sobre esta materia se completa aludiendo a la posibilidad de enérgicas actuaciones judiciales, pudiendo autorizar registros sorpresa, acordar medidas cautelares tales como el secuestro de medios técnicos y la clausura del centro de actividad del infractor, así como las sanciones e indemnizaciones que en cada caso correspondan de acuerdo con los daños patrimoniales y morales causados. [1]

Campaña de la BSA y SEDISI contra la Piratería Informática

La Business Software Alliance (BSA) es una asociación que actúa legalmente contra la piratería informática en más de 65 países de Europa, Asia, Norteamérica y Latinoamérica. BSA aglutina a las principales compañías internacionales que ofrecen programas de ordenador y servicios en el sector informático. La Asociación Española de Empresas de Tecnología de la Información (SEDISI) es representante y portavoz de los intereses profesionales de las empresas españolas del sector. Ambas asociaciones representan el 80 % del sector empresarial informático español.

Entre las actividades de las dos asociaciones en defensa de los intereses del sector informático, está el desarrollo de la campaña contra la Piratería Informática Aunque dicha campaña afecta tanto a instituciones públicas como privadas, se ha diseñado por ambas asociaciones basándose sobre cinco líneas muy definidas de actuación:

Promoción y apoyo del cumplimiento de las leyes que regulan la protección jurídica de programas de ordenador en cada país.

■ [1] Esta información ha sido extraída de artículos y ponencias del prestigioso abogado en Derecho Informático D. Javier Ribas (asesor legal de la BSA & SEDISI).

Difusión de las consecuencias que conlleva infringir la ley.

Sensibilizar a la conciencia pública sobre los beneficios del uso de programas originales frente las copias piratas.

Apoyar al sector informático en la lucha contra la piratería potenciando la creación de frentes comunes que unifiquen esfuerzos.

Emprender acciones legales contra las organizaciones que comercializan o producen copias ilegales de programas, así como contra los que los compran o utilizan.

Conclusiones

La piratería informática es un fenómeno antisocial que perjudica a todos los niveles de la sociedad:

Al individuo: al comprador estafado; al individuo como persona portadora de valores a transmitir de honradez, legalidad, respeto, etc. A la correcta formación del individuo; al individuo como trabajador por la negativa repercusión laboral de este fenómeno que implica la destrucción de puestos de trabajo

A la empresa de Tecnologías de Información: que ve mermados sus beneficios por la invasión ilegítima de la piratería en lo que sería su legítimo mercado.

Al sector empresarial en su conjunto que ve dificultado el acceso a las tecnologías de Información por un encarecimiento de los productos y servicios informáticos.

Al Estado: en su propia economía interior puesto que supone una perdida de sus ingresos recaudatorios; en su organización ya que le obliga a efectuar un despliegue de medios para combatir la piratería; en su proyección internacional puesto que supone un desincentivo al comercio exterior y a la inversión extranjera en nuestro país.

La piratería es una práctica de competencia desleal.

La piratería es una transgresión jurídica a la norma = es un delito.

La piratería es un ataque a la más elemental ética: es un disvalor que hay que erradicar de nuestra sociedad.

Bibliografía

1.- "El Mundo Digital".1995.Nicholas Negroponte.Editorial:Ediciones B.

2.- "La Tercer Ola". 1980. Alvin Toffler. Editorial: Plaza & Janes.

3.-"Teoría Z". William Ouchi. 1982 .Editorial: Ediciones Orbis.

4.- "Deontología Informática". 1993. Vázquez y Barroso. Editorial : Instituto de Sociología Aplicada.

5.-"I Jornadas Tecnologias de la Información y Eficiencia Empresarial". 1996. Editorial: Grupo Nuevo Lunes.

6.-" Informe sobre el Impacto de la Industria del Software en las Economías Europeas". 1995. Editorial: Price Waterhouse & BSA.

7.-"Informe sobre "Prácticas Ilegales en las Empresas Españolas". 1995. Editorial: BSA.

8.- "Ponencia de D. Xavier Ribas sobre Protección Jurídica del Software: Legislación Española". 1997. Editorial: I Congreso Internacional de La Policía contra el delito Informático.

9.- "Interacción del Derecho y la Informática". 1996. Barriuso Ruiz. Editorial: Dyckinson.

10.-"Manual de Dictámenes y Peritajes Informáticos". 1995. Emilio del Peso, Carlos Manuel Fernández Sánchez y otros. Editorial: Díaz de Santos.

11.- "Tratamiento de Datos Personales Informatizados". 1996. Editorial: La Agencia de Protección de Datos.

12.-"Informática y Derecho 6 & 7" . 1994. Editorial: UNED.

13.- "Confidencialidad y Seguridad de la Información : La Lortad y su implicaciones socioeconómicas". 1994. Emilio del Peso. Editorial: Díaz de Santos.

14.-"El Humanismo en la Empresa". 1992. Varios. Editorial: Rialp.

15.- "El Fraude y otros Delitos Informáticos". 1990. Sneyers. Editorial: Tecnologías de Gerencia y Producción.

16.- "El Delito Informático". 1987. Camacho. Editorial: Camacho.

17.- Papeles de Avila: Expertos en Auditoría Informática". 1986. Marina Touriño , Carlos Manuel Fernández Sánchez y otros. Editorial: CREI.

18.- "Seguridad en los Sistemas de Información".1984. Fisher y Traducido por : Carlos Manuel Fdez. Sánchez. Editorial: Díaz de Santos.

19.- "Control Objectives for Information and Related Technology". 1996. Editorial: Information Systems Audit and Control Foundation.

20.- "Guía de Seguridad Informática" . 1997. Varios. Editorial: SEDISI (Asociación Española de Empresas de Tecnologías de la Información).

Marco Legal de la Automatización de la Actividad Administrativa

El "expediente electrónico" en Uruguay

CARLOS E. DELPIAZZO *

Universidad Mayor de la República Oriental de Uruguay

I) INTRODUCCION

En el marco de la reforma del Estado que se viene procesando en nuestro país, la ley Nº 16.736 de 5 de enero de 1996 contiene un conjunto de disposiciones tendentes a facilitar la automatización de la actividad administrativa cuya trascendencia jurídica es destacable.

* Doctor en Derecho y Ciencias Sociales. Profesor de Derecho Público y de Informática Jurídica en la Facultad de Derecho de la Universidad Mayor de la República Oriental del Uruguay. Profesor de Informática Jurídica en la Facultad de Derecho de la Universidad Católica del Uruguay "Dámaso Antonio Larrañaga". Profesor de Derecho Administrativo Económico y de Derecho Informático en el Instituto de Estudios Empresariales de Montevideo. Miembro del Instituto Uruguayo de Derecho Administrativo. Secretario General del Instituto Rioplatense de Derecho Administrativo.

Bajo el título "Normas de Desregulación y Reforma Administrativa", se incluyen cinco disposiciones (arts. 694 a 697), cuya reglamentación se comete al Poder Ejecutivo (art. 698). De las mismas resulta que:

a) se promueve la aplicación de medios informáticos y telemáticos por las Administraciones públicas, garantizando a los administrados el pleno acceso a las informaciones que les conciernan o sean de su interés;

b) se reconoce a las actuaciones que se realicen por medios informáticos idéntica validez y valor probatorio que a las que se tramiten por medios convencionales;

c) se asigna plena validez a las notificaciones personales realizadas por correo electrónico u otros medios informáticos o telemáticos; y

d) se regulan aspectos de la documentación electrónica.

Dichas normas vienen a complementar las existentes hasta el momento y su incidencia sobre la normativa vigente en materia de actuación administrativa -sustentada en el expediente sobre soporte papel- posibilita el pleno desarrollo del llamado "expediente electrónico", entendiendo por tal la acumulación en soporte magnético (y ya no en legajo escrito) de toda la información relativa a un asunto.

II) ANTECEDENTES

Sabido es que la Administración pública ha sido uno de los principales clientes del mercado informático y uno de los mayores consumidores de bienes y servicios vinculados a las nuevas tecnologías de la información[2].

Por eso, no es de extrañar que el desarrollo del Derecho Informático positivo en el Uruguay[3] haya estado signado por la regulación de temas tales

■[2] Carlos E. DELPIAZZO - "Contratación administrativa en materia informática", en Rev. de Derecho Público (Montevideo, 1992), N° 2, pág. 59 y sigtes.

■[3] Carlos E. DELPIAZZO - "Derecho Informático Uruguayo" (Idea, Montevideo, 1995), págs. 39 y sigtes., y 175 y sigtes.

como la documentación electrónica, las bases de datos públicas, el intercambio de información entre dependencias oficiales, y la adopción de soluciones acordes al avance tecnológico en el procedimiento administrativo.

Así, la primera norma legal en la materia la constituye el art. 129 de la ley N° 16.002 de 25 de noviembre de 1988, a cuyo tenor "la documentación emergente de la transmisión a distancia, por medios electrónicos, entre dependencias oficiales, constituirá, de por sí, documentación auténtica y hará plena fe a todos sus efectos en cuanto a la existencia del original trasmitido". A renglón seguido, el art. 130 de la misma ley prevé que "el que voluntariamente transmitiere a distancia entre dependencias oficiales un texto del que resulte un documento infiel, incurrirá en los delitos previstos por los arts. 236 a 239 del Código Penal, según corresponda", los que refieren a la falsificación documentaria material o ideológica[4].

Con la posterior aprobación del nuevo reglamento de procedimiento administrativo (Decreto N° 500/991 de 27 de septiembre de 1991), se establecen un conjunto de soluciones de principio y de carácter instrumental tendentes a la aplicación de las nuevas tecnologías de la información en ese ámbito[5].

Entre ellas, merece destacarse en primer lugar el art. 14, cuyo inc. 1° establece que "es de interés público, para el mejor cumplimiento de los servicios, el intercambio permanente y directo de datos e información entre todas las unidades y reparticiones de la Administración pública" (con excepción de los calificados como secretos, confidenciales o reservados, de acuerdo con las normas legales o reglamentarias vigentes). Agrega el inc. 2° que, "a efectos de implantar sistemas de libre flujo de información, se propenderá a la interconexión de los equipos de procesamiento electrónico u otros medios similares". Asimismo - finaliza diciendo el inc. 3°- podrá la Administración brindar el servicio de acceso

■[4] Carlos E. DELPIAZZO - "La prueba de las transferencias electrónicas de fondos en el Derecho uruguayo", en Rev. Derecho y Tecnología Informática (Bogotá, 1989), N° 2, pág. 114; y Pedro J. MONTANO - "Los delitos informáticos", en La Justicia Uruguaya, tomo 94, sección Doctrina, pág. 57 y sigtes.

■[5] Carlos E. DELPIAZZO - "El procedimiento administrativo y las nuevas tecnologías de la información", en Rev. Uruguaya de Derecho Constitucional y Político (Montevideo, 1992), tomo VIII, N° 48, pág. 417 y sigtes.

electrónico a sus bases de datos a las personas físicas o jurídicas, estatales, paraestatales o privadas que así lo solicitaren".

En segundo término, prevé el art. 33 que "en aplicación de lo dispuesto por el art. 14, la Administración propiciará el uso de soportes de información electrónicos, magnéticos, audiovisuales, etc., que faciliten la gestión pública".

En tercer lugar, el art. 19 admite "la presentación de los particulares por fax u otros medios similares de transmisión a distancia", en tanto que el art. 91 habilita practicar las notificaciones a domicilio "por telegrama colacionado certificado con aviso de entrega, por carta certificada con aviso de retorno, telex, fax o cualquier otro medio idóneo que proporcione certeza en cuanto a la efectiva realización de la diligencia y a su fecha, así como en cuanto a la persona a la que se ha practicado". Similares posibilidades de presentación se reconocen en materia de interposición de recursos administrativos (arts. 154, 157 y 158).

Cabe agregar que, al amparo de la normativa reseñada, se han desarrollado interesantes experiencias de automatización de la actuación administrativa, como es el caso de la llamada "licitación electrónica"[6].

Por otra parte, la ley N° 16.616 de 20 de octubre de 1994, relativa al Sistema Estadístico Nacional, ha consagrado y definido en su art. 3 D una serie de principios relativos al manejo de la información respectiva, entre los que se destacan los de pertinencia, transparencia, rigurosidad, legalidad objetiva y motivación.

De la rápida reseña precedente se desprende que la normativa que precedió al dictado de la ley N° 16.736 tenía alcance limitado o jerarquía sublegal, constatándose la ausencia de disposiciones de carácter general y rango de ley aplicables a la actuación de todas las Administraciones públicas.

■[6] Carlos E. DELPIAZZO - "La licitación electrónica", en Rev. Derecho y Tecnología Informática (Bogotá, 1995), N° ó, pág. 49 y sigtes.

III) AMPLIA RECEPCION DE LAS N.T.I.

1 - Aspectos a considerar

Conforme al art. 694 de la ley N° 16.736, "las Administraciones públicas impulsarán el empleo y aplicación de medios informáticos y telemáticos para el desarrollo de sus actividades y el ejercicio de sus competencias, garantizando a los administrados el pleno acceso a las informaciones que les conciernen o sean de su interés".

De la sola lectura de dicha disposición se desprende que la misma implica un amplio reconocimiento de las nuevas tecnologías de la información (N.T.I.) en un doble sentido: desde el punto de vista de la actuación de las Administraciones públicas (que promoverán el uso de medios informáticos y telemáticos) y desde el punto de vista de la protección de los administrados (a quienes se garantiza el pleno acceso a la información administrativa pertinente).

Ambas perspectivas plantean aspectos jurídicos de interés que vale la pena comentar por separado.

2 - **Automatización de la actividad administrativa**

La primera parte de la norma transcripta contiene un claro mandato para que las Administraciones públicas impulsen el empleo no sólo de medios informáticos sino también telemáticos, lo que supone el reconocimiento del papel que la Informática y las Comunicaciones juegan en el proceso de reforma del Estado[7].

A1 respecto, corresponde observar que junto al empleo del tratamiento automatizado de la información -que es objeto de la Informática[8]- se promueve

■[7] Luis MARTINEZ MIGUEL - "E1 papel de la Informática y las Comunicaciones en la modernización de la Administración del Estado", en Informática y Derecho (Mérida, 1996), N° 9-11, pág. 167 y sigtes.

■[8] Carlos E. DELPIAZZO y otros - "Introducción a la Informática Jurídica y al Derecho Informático" (A.M.F., Montevideo, 1984), pág. 15.

también su transmisión a distancia mediante la Telemática, que nace de la combinación de las técnicas informáticas y de las telecomunicaciones para posibilitar la comunicación a distancia de la información automatizada[9].

Ello es lógico en el marco de la emergente "sociedad global de la información" en la que nos encontramos inmersos, surcada por las "autopistas de la información" que atraviesan el planeta sin reconocer fronteras nacionales, con implicaciones regionales y mundiales que convocan hoy a la reflexión jurídica[10] y a la definición de nuevas políticas[11]. Ejemplo de ello es INTERNET, constituida por una red de redes de computadores unidos por líneas telefónicas, fibras ópticas, cables submarinos y enlaces por satélite que vinculan Universidades, Gobiernos, empresas y millones de individuos en casi todo el mundo. Esta expansión del mercado de la información[12] desborda la normativa nacional e internacional existente[13] y nos enfrenta al progresivo surgimiento de categorías nuevas tales como la noción del servicio universal (y ya no servicio público) en el campo de las telecomunicaciones[14].

■[9] Carlos E. DELPIAZZO - "Información, Informática y Derecho" (A.M.F., Montevideo, 1989), pág. 95 y sigtes.

■[10] André BERTRAND - "Las autopistas de la información y el Derecho", en Rev. Derecho de la Alta Tecnología (Buenos Aires, 1995), Año VII, Ns 82-83, pág. 11 y sigtes.

■[11] Ver: Informe BANGEMANN - "Europa y la sociedad de la información planetaria" (Recomendaciones al Consejo Europeo, 1994, según traducción publicada en DAT, Año VII, NQ 84-85, pág. 20 y sigtes.; e Informe LEHMAN "Intellectual Property and the National Information Infrastructure" (Washington, 1995), especialmente pág. 177 y sigtes.

■[12] Pierre CATALA - "E1 mercado de la información. Aspectos jurídicos", en Rev. Derecho de la Alta Tecnología (Buenos Aires, 1996), Año VIII, N° 93, pág. ó y sigtes.

■[13] Antonio MILLE - "La problemática jurídica de las autopistas de la información en los trabajos hemisféricos y en los documentos oficiales estadounidense y europeo", en Rev. Derecho de la Alta Tecnología (Buenos Aires, 1995), Año VII, Ns 84-85, pág. 1 y sigtes.

■[14] Ives POULLET y otros - "Servicio universal público en la política europea de telecomunicaciones", en Informática y Derecho (Mérida, 1996), NQ 12-15, pág. 827 y sigtes.

A partir de esa realidad, a la que no puede sustraerse ningún Estado, bien puede decirse que la mayor riqueza de que disponen las Administraciones públicas es la información[15]. Ella constituye una necesidad ineludible para el desenvolvimiento diario de los cometidos asignados; sea para resolver un recurso, para verificar un cómputo jubilatorio o para conceder una marca, los funcionarios públicos actuantes han de apoyarse en información convenientemente dispuesta. Pero además, para poder planificar y adoptar decisiones, no hay más remedio que manejar una información adecuada a cada caso. Cuando esa información está estructurada, nos encontraremos en presencia de verdaderas bases de datos[16].

Por eso, las Administraciones públicas son titulares de una gran diversidad de bases de datos, entre las que predominan las relacionales, sin perjuicio de una previsible tendencia hacia un desarrollo de bases de datos distribuidas, con estructura relacional, y de bases de datos orientadas a objetos[17].

Siendo así, puede ocurrir que la información contenida en esas bases de datos sea usada internamente por la propia Administración que la colectó, sea transferida a otras Administraciones, o sea facilitada al público. De dichas tres hipótesis, la primera no plantea dificultades (siempre que el uso sea acorde al fin debido) y la tercera será examinada más adelante; en cambio, la segunda obliga reflexionar sobre el alcance y los límites de lo que el art. 14 del Decreto N° 500/991 llama "sistemas de libre flujo de información" entre dependencias estatales.

Al respecto, se han señalado los riesgos y aún los daños para la seguridad individual que puede comportar ese libre flujo de información[18], en particular

■[15] Jorge GUIMET PERENA "Transferencias de datos entre Administraciones públicas", en Encuentro sobre Bases de Datos en la Administración Pública (M.A.P., Madrid, 1992), pág. 49.

■[16] Julio DELICADO MONTERO-RIOS - "Bases de datos para el servicio público", en Encuentro... cit., pág. 20 y sigtes.

■[17] Carmen COSTILLA RODRIGUEZ - "Avances recientes y tendencias previsibles de las bases de datos", en Encuentro... cit., pág. 119 y sigtes.

■[18] Mariano R. BRITO - "Principios del procedimiento administrativo común", en Procedimiento Administrativo (UCUDAL, Montevideo, 1991), pág. 16 y sigtes.

cuando refiere a datos personales. Es que la vinculación entre Informática y telecomunicaciones posibilita no sólo el procesamiento de enormes volúmenes de información sino también su rápida difusión y consiguiente conocimiento por multiplicidad de sujetos, lo que plantea un potencial conflicto entre el poder informático como nueva forma de dominio social y la libertad informática como manifestación moderna del derecho a la intimidad [19].

Para prevenir dicho conflicto, el Derecho comparado exhibe el dictado de multiplicidad de leyes[20] que la doctrina ha clasificado de diversa manera, en atención a sus fines y alcance. Así, se ha hablado de leyes de protección de datos de "primera generación" y de "segunda generación"[21] en consideración al cambio aparejado por el tránsito de la concentración de la información almacenada en unos pocos grandes sistemas, a su dispersión mediante pequeños sistemas interconectados entre los que circula fácil y rápidamente sin que el interesado pueda siquiera sospechar dónde hay datos personales suyos, qué uso se hace de ellos, qué elementos o juicios valorativos se les añaden y qué consecuencias puede aparejarle ese uso. Asimismo, se ha distinguido entre "leyes sectoriales" y "leyes ómnibus"[22] según apunten a la protección en áreas específicas y concretas o procuren una cobertura general.

En todas ellas, la protección de datos no ha sido imaginada para proteger a los datos "per se" sino en consideración a que ellos refieren a la información individual como parte del nuevo rostro del derecho a la intimidad, que ya no

■ [19] Carlos E. DELPIAZZO - "Poder y libertad informáticos", en Primeras Jornadas Nacionales de Derecho Informático (Montevideo, 1987), pág. 147 y sigtes.; y "Posibles medios de protección frente a las responsabilidades derivadas de la gestión de bases de datos en el Derecho uruguayo", en Congreso Internacional de Informática y Derecho (Buenos Aires, 1990), pág. 382 y sigtes.

■ [20] Antonio MILLE - "Informaciones de carácter personal. Derecho comparado y prospectiva", en Informática y Derecho (Mérida, 1996), N° 12-15, pág. 1359 y sigtes.

■ [21] Manuel HEREDERO HIGUERAS - "Nota preliminar", en Informática. Leyes de Protección de Datos (Madrid, 1988), vol. III, pág. 18 y sigtes.

■ [22] Miguel A. EKMEKDJIAN y Calogero PIZZOLO (h) - "Habeas data. El derecho a la intimidad frente a la revolución informática" (Depalma, Buenos Aires, 1996), pág. 27 y sigtes.

consiste sólo en el derecho a ser dejado en paz[23] sino que se configura como un derecho de tercera generación[24], cual es la libertad informática, entendida como derecho de autotutela de los datos personales[25].

En cuanto a la noción de datos de carácter personal, se ha entendido que se trata de "cualquier información concerniente a personas físicas identificadas o identificables" -como reza el art. 3°, lit a) de la ley española N° 5/992 de 29 de octubre de 1992- tales como las de carácter existencial: nacimiento, muerte, matrimonio, divorcio, domicilio, actos objeto de decisión judicial, la actividad profesional, los medios de subsistencia, el patrimonio, la afiliación política o sindical, la pertenencia a una confesión religiosa, la asistencia a eventos públicos o privados, los desplazamientos y las enfermedades. Caben también dentro del concepto datos que no expresan información existencial sino sobre cosas o bienes, como lo aclara la ley alemana de 27 de febrero de 1977, cuyo art. 39 incluye las informaciones sobre "condiciones personales o materiales". Asimismo, se consideran incluidas las opiniones o apreciaciones acerca de la persona interesada, según lo explícita la ley del Reino Unido de 12 de julio de 1984[26].

Entre nosotros, ya hemos tenido oportunidad de señalar reiteradamente[27] que, aún a falta de regulación legislativa expresa sobre la protección de los datos personales, la libertad informática se encuentra reconocida en el art. 72 de la Constitución, a cuyo tenor quedan amparados los derechos y garantías "que son inherentes a la personalidad humana o se derivan de la forma republicana de

■[23] Vittorio FROSINI - "Banche dei datti e tutela della persona" en Quaderni di Documentazioni N° 4 (Camera dei Deputati, Roma 1981), págs. 5 a 7.

■[24] Miguel A. EKMEKDJIAN y Calogero PIZZOLO (h) - "Habeas data" cit., pág. 25.

■[25] Vittorio FROSINI - "La p otezione della riservatezza nella societá informática", en Informática e Diritto (Roma, 1981), vol. VIII, pág. 5 y sigtes.

■

■[26] Manuel HEREDERO HIGUERAS - "La ley orgánica 5/1992 de regulación del tratamiento automatizado de los datos de carácter personal" (Tecnos, Madrid, 1996), pág. 71.

■[27] Carlos E. DELPIAZZO - "Derecho Informático Bancario" (I.E.E.M., Montevideo, 1990), pág. 39 y sigtes.; "Introducción a la Informática Jurídica y al Derecho Informático" cit., pág. 105; y "Derecho Informático Uruguayo" cit., pág. 91 y sigtes.

gobierno". Dicha disposición incorpora al ordenamiento jurídico positivo nacional la esencia ideológica del jusnaturalismo y, por ende, tutela efectivamente los derechos del hombre inherentes a su personalidad[28], garantizándolos tanto en vía administrativa como jurisdiccional.

En consecuencia, cabe concluir que la aplicación de medios informáticos y telemáticos para el desarrollo de la actividad administrativa, en tanto posibilita la implantación de sistemas de libre flujo de información, no significa que todo dato pueda ser libremente circulado entre las distintas dependencias públicas. Por el contrario, sólo podrá transmitirse aquella información que, por su naturaleza o por disposición legal, no revista carácter personal o no sea secreta o reservada.

3 - **Libre acceso a la información administrativa**

En virtud de la parte final del art. 694 de la ley N° 16.736, se garantiza a los administrados "el pleno acceso a las informaciones que les conciernan o sean de su interés". Significa que se asegura el más amplio acceso de cualquier persona a dos tipos de informaciones: las que les conciernan y las que sean de su interés.

Respecto al primer bloque de informaciones, es decir, aquéllas "que le conciernen" al administrado o que refieren a su persona, puede decirse que la norma recibe una de las manifestaciones de la libertad informática, cual es el derecho de acceder o averiguar el contenido de la información que a uno se refiere registrada en una base de datos[29]. Es que el derecho a la protección de los datos personales es un derecho genérico constituido por tres derechos específicos[30] que la legislación comparada suele distinguir[31], a saber:

■[28] Alberto Ramón REAL - "Estado de Derecho y Humanismo Personalista" (F.C.U., Montevideo, 1974), pág. 15 y sigtes., y "Algunas perspectivas humanistas y democráticas del Derecho administrativo contemporáneo", en La Justicia Uruguaya, tomo 84, sección Doctrina, pág. 47 y sigtes.

■[29] Jorge PAEZ MANA y Pilar DEL POZO - "E1 derecho al acceso y distribución de información por vía telemática como derecho fundamental", en Informática y Derecho (Mérida, 1996), Ni 12-15, pág. 1393 y sigtes.

■[30] Miguel A. EKMEKDJIAN y Calogero PIZZOLO (h) - "Habeas data" cit., pág. 63 y sigtes.

a) el derecho a conocer las bases de datos que contengan información a su respecto;

b) el derecho a acceder al contenido de esa información; y

c) el derecho a rectificar dicha información cuando sea inexacta, falsa o errónea.

En cuanto al segundo grupo de informaciones, o sea, aquéllas que "sean de su interés" (del administrado) aunque no le conciernan, la disposición consagra el derecho de acceso a las bases de datos de la Administración, como manifestación actual del viejo derecho de acceso de los ciudadanos a los archivos y registros administrativos[32].

El fundamento de este derecho radica en los principios de publicidad[33] y transparencia[34] de las actuaciones administrativas, sin perjuicio de los límites que puedan resultar de las leyes que establezcan la obligación de reserva (secreto militar, estadístico, etc.) o de la naturaleza de la información (tal como la relativa a la intimidad de las personas).

Además, la referencia al "interés" permite inferir que la garantía proclamada genéricamente a favor del administrado, resultará calificada en cada

■[31] Carlos E. DELPIAZZO - "El procedimiento administrativo y las nuevas tecnologías de la información" cit., pág. 427; y "Derecho Informático Uruguayo" cit., pág. 90.

■[32] Luis Alberto POMED SANCHEZ - "El derecho de acceso de los ciudadanos a los archivos y registros administrativos" (M.A.P., Madrid, 1989), pág. 25 y sigtes.

■[33] Horacio CASSINELLI MUNOZ - "El principio de publicidad en la gestión administrativa", en Rev. de Derecho, Jurisprudencia y Administración, tomo 58, pág. 163 y sigtes.; y Enrique GOMEZ-REINO - "El principio de publicidad de la acción del Estado y la técnica de los secretos oficiales", en Rev. Española de Derecho Administrativo, N° 8, pág. 120 y sigtes.

■[34] Jean AUBY - "Hacia la transparencia de la Administración en Francia", en Rev. de Administración Pública, N° 95, pág. 315 y sigtes.

caso por la acreditación de ser interesado, que circunscribe la esfera activa del derecho de acceso bajo examen.

De lo dicho se desprende que el derecho de acceso a las bases de datos de la Administración, no obstante su amplitud de principio, no es absoluto ya que puede estar acotado según la índole de la información, conforme a la ley.

IV) AUTOMATIZACION DE LOS ACTOS Y PROCEDIMIENTOS ADMINISTRATIVOS

1 - **Cuestiones contempladas**

Conforme al inc. 1° del art. 695 de la ley N° 16.736, "los trámites y actuaciones que conforman el procedimiento administrativo así como los actos administrativos podrán realizarse por medios informáticos".

Agrega el inc. 2° que "su validez jurídica y valor probatorio serán idénticos a los de las actuaciones administrativas que se tramiten por medios convencionales".

Finalmente, el inc. 3° prevé que "la firma autógrafa podrá ser sustituida por contraseñas o signos informáticos adecuados".

De la sola lectura de la disposición, se puede extraer que la misma reconoce ampliamente la viabilidad genérica de la informatización de la actividad administrativa (actos y procedimientos), a la vez que regula tres aspectos específicos de gran importancia: la validez jurídica, el valor probatorio, y la autenticación de las actuaciones cumplidas por medios informáticos.

2 - **Informatización de la voluntad administrativa**

Sabido es que el procedimiento administrativo es la sucesión o secuencia de actos y tareas materiales o técnicas, cumplidos por una entidad estatal o ante ella, instrumentalmente destinados al dictado o a la ejecución de un acto final de naturaleza administrativa; generalizando la definición del art. 168 del Decreto N° 500/991, se trata del conjunto de trámites y formalidades que debe observar la

Administración en el ejercicio de sus poderes, para dictar un acto administrativo o ejecutarlo[35].

A su vez, el acto administrativo ha sido definido por nuestra más prestigiosa doctrina como toda declaración unilateral de voluntad de la Administración que produce efectos subjetivos[36].

Mientras que la automatización de los trámites y formalidades que constituyen el procedimiento aparece a primera vista como una sencilla aplicación de la Informática jurídica de gestión[37], no ocurre lo mismo con los actos administrativos en tanto éstos importan manifestaciones de voluntad. En efecto, la materia del acto administrativo es una determinación de la voluntad jurídica del órgano actuante.

Al respecto, las reglas de Derecho establecen cómo se determina la voluntad jurídica del órgano, mediante acontecimientos del mundo exterior ubicados en el espacio y en el tiempo que consisten generalmente en comportamientos voluntarios de los titulares de los órganos, manifestándose con la firma (en el caso de los órganos unipersonales), a través de la votación tratándose de órganos pluripersonales), o de otros modos. Hasta hace pocos años, sólo el ser humano era capaz de constatar el acaecimiento de los supuestos del acto y de querer las consecuencias jurídicas correspondientes. Pero actualmente, la voluntad humana puede ser sustituida a tales efectos por el computador, siempre que el acto sea la consecuencia de ciertos supuestos objetivamente constatables y cuando esté excluida toda posibilidad de valoración[38].

■[35] Juan Pablo CAJARVILLE PELUFFO - "Procedimiento Administrativo" (Idea, Montevideo, 1992), pág. 12; y "Procedimiento administrativo común", en Procedimiento Administrativo (UCUDAL, Montevideo, 1991), pág. 21.

■[36] Enrique SAYAGUES LASO - "Tratado de Derecho Administrativo" (Montevideo, 1959), tomo I, pág. 388.

■[37] Mario BARRETO y otros - "Informática, Control y Gestión" (A.M.F., Montevideo, 1990), pág. 95 y sigtes.

■[38] Juan Pablo CAJARVILLE PELUFFO - "Invalidez de los actos administrativos" (Universidad, Montevideo, 1984), pág. 21.

Tal realidad es la que viene a reconocer el inc. 1° de la norma bajo examen. No obstante, ya antes de su dictado, habíamos sostenido la viabilidad jurídica de automatizar todas aquellas manifestaciones unilaterales de voluntad de la Administración productoras de efectos jurídicos (actos administrativos) correspondientes a actividades integralmente regladas o aún discrecionales[39], en este último caso mediante la implementación de sistemas expertos capaces de anular la conducta de un experto humano dentro de un dominio limitado[40] a partir del llamado "razonamiento cibernético" que, no obstante sus radicales diferencias con el razonamiento jurídico, constituye una herramienta útil para la adopción de decisiones[41].

En el campo de la Informática jurídica decisional[42], un sistema experto puede caracterizarse en base a tres elementos principales[43]:

a) una base de conocimientos, que es un verdadero banco de datos en base a cuya información se trabaja;

b) un motor de inferencias, a través del cual se aplica el conocimiento acumulado al caso concreto; y

c) una interfase apropiada.

■[39] Carlos E. DELPIAZZO - "Derecho Informático Uruguayo" cit., pág. 148 y sigtes.

■[40] Antonio A. MARTINO - "Sistemas expertos legales", en Informática y Derecho (Depalma, Buenos Aires, 1987), vol. 1, pág. 136 y sigtes.; y Antonio Enrique PEREZ LUÑO - "Sistemas expertos jurídicos: premisas para un balance", en Informática y Derecho (Depalma, Buenos Aires, 1996), vol. 5, pág. 97 y sigtes.

■[41] Enrique SANCHEZ JIMENEZ - "El razonamiento cibernético como sistema de ayuda a la decisión jurídica", en Informática y Derecho (Mérida, 1996), Ni 12-15, pág. 1671 y sigtes.

■[42] Ricardo A. GUIBOURG - "Informática jurídica decisoria" (Astrea, Buenos Aires, 1993), pág. 215 y sigtes.

■[43] María Fernanda GUERRERO - "Los sistemas jurídicos expertos: la inteligencia artificial aplicada al Derecho", en III Encuentro sobre la Informática en las Facultades de Derecho (Madrid, 1989), pág. 193 y sigtes.

Quiere decir que es perfectamente posible que determinados tipos de actos administrativos puedan ser dictados sin intervención de voluntad humana, en la medida en que la información contenida en la base de conocimientos de un sistema experto contenga la previsión de los supuestos necesarios para su aplicación en el caso concreto. En tales situaciones, adquirirán especial relevancia las previsiones relativas a la validez jurídica, el valor probatorio y la sustitución de la firma autógrafa contenidas en el mismo art. 695 de la ley N° 16.736.

3 - **Validez jurídica**

Al tenor de la norma bajo análisis, tanto los trámites y actuaciones que conforman el procedimiento administrativo como los actos administrativos que se realicen por medios informáticos tendrán idéntica validez jurídica a los que se tramitan por medios convencionales, es decir, conformando expedientes sustentados en soporte papel.

Si bien la disposición legal sólo se refiere a la igual validez, es preciso concluir que actos y procedimientos realizados por medios informáticos tendrán también idéntica eficacia. En efecto, configurados los presupuestos (circunstancias extrínsecas) y los elementos (circunstancias intrínsecas) del acto, éste se reputará válido y adquirirá existencia jurídica[44], estando en condiciones de desplegar los efectos correspondientes[45].

Quiere decir que no existirán diferencias de validez y eficacia -la ley habla de identidad- entre las actuaciones y los actos administrativos que se realicen por medios convencionales o por medios informáticos.

■[44] Juan Pablo CAJARVILLE PELUFFO - "Invalidez de los actos administrativos" cit., págs. 12 y 13.

■[45]Horacio CASSINELLI MUNOZ - "Oposición superviniente: ¿ derogación o inconstitucionalidad ?", en Rev. de Derecho, Jurisprudencia y Administración, tomo 55, pág. 160.

4 - Valor probatorio

Sin perjuicio de lo que se dirá al examinar el tratamiento de la documentación electrónica en la nueva ley (infra: capitulo VI), cabe observar que el art. 695 refiere al valor probatorio de los procedimientos y actos administrativos sustanciados por medios informáticos conjuntamente con la cuestión de su validez jurídica y calificándolo del mismo modo: será idéntico a las actuaciones que se tramitan por los medios clásicos.

Es de observar que la disposición legal no refiere a la cuestión de la admisibilidad como medios probatorios[46] de los actos y trámites que conforman el "expediente electrónico" sino que la da por supuesta, abordando exclusivamente la cuestión de su valoración.

Al respecto, nuestro Derecho ha optado por un sistema mixto[47], aplicable no sólo en el ámbito jurisdiccional sino también en el ámbito administrativo[48]: de prueba legal para determinados medios probatorios, como los instrumentos públicos o privados auténticos (art. 170 del Código General del Proceso), que hacen plena prueba, y de apreciación judicial conforme a las reglas de la sana crítica (art. 140 y concordantes del mismo Código) para las probanzas no reguladas específicamente. No obstante, en materia informática, el ya citado art. 129 de la ley N° 16.002, ampliado por el art. 697 de la ley N° 16.736, nos ubica ante un supuesto de prueba tasada: dice que "hará plena fe a todos sus efectos", y agrega que "constituirá de por si documentación auténtica"[49].

Por lo tanto, resulta de los dicho que las alteraciones que en la forma de los actos administrativos derivan de su procesamiento automatizado no proyectan

[46] Carlos E. DELPIAZZO - "Derecho Informático Uruguayo" cit., pág. 48 y sigtes.

[47] Luis Alberto VIERA - "La prueba", en Curso de Derecho Procesal (Facultad de Derecho, Montevideo, 1974), tomo II, pág. 117 y sigtes.

[48] Juan Pablo CAJARVILLE PELUFFO - "Procedimiento administrativo común" cit., pág. 32.

[49] Graciela BELLO y Luis Alberto VIERA - "Valor probatorio de la información por computadora", en Rev. Uruguaya de Derecho Procesal, Año 1987, N° 3, pág. 244 y sigtes .

consecuencias en su valor probatorio, el que será idéntico al de aquéllos producidos por medios convencionales.

5 - **Autenticación**

Un aspecto vinculado al del valor probatorio, aunque distinto, es el de la autenticación de los trámites y actos que se realicen por vía informática.

De acuerdo a las normas generales de actuación administrativa, la forma más común de autenticación es la firma, es decir, la escritura a mano de su nombre por parte del funcionario competente. Sin embargo, el tránsito del expediente tradicional al expediente electrónico nos introduce en un ambiente en el que la firma no sólo se hace prácticamente imposible sino que conspira contra la automatización de las actuaciones[50].

Por eso, debe aplaudirse la previsión del párrafo final del art. 695, según el cual "la firma autógrafa podrá ser sustituida por contraseñas o signos informáticos adecuados". Dichas contraseñas o signos informáticos constituyen técnicas de autenticación que pueden ser más confiables aún que la firma manuscrita[51]. Entre ellas, se destacan los códigos secretos y la criptografía.

Mientras que los códigos secretos consisten en simples combinaciones de cifras, de letras o de ambas que sólo el interesado conoce, la criptografía implica la utilización de técnicas que permiten el ocultamiento de la información a personas no autorizadas[52], posibilitando la implementación de "firmas

■[50] Héctor ALEGRIA - "Nuevas fronteras de la documentación, la forma y la prueba de las relaciones comerciales", en Rev. La Ley (Buenos Aires, 1987), vol. 1, pág. 94 y sigtes.

■[51] Sergio FARAUDO - "Aspectos legales de la prueba y la firma en la transferencia electrónica de datos (E.D.I.)", en Intercambio electrónico de datos. Aspectos técnicos y jurídicos (Buenos Aires, 1991), pág. 77 y sigtes.

■[52] José María MOLINA MATEOS - "Libertad informática y Criptología", en Informática y Derecho (Mérida, 1996), N° 12-15, pág. 976.

electrónicas"[53] acordes a la realidad de un procedimiento administrativo no sustentado en soporte papel[54].

En consecuencia, debe interpretarse que la referencia legal a "contraseñas o signos informáticos adecuados" es de una amplitud suficiente para amparar la adopción de distintas técnicas de autenticación, con proyección en la seguridad o confiabilidad de la información contenida en los actos o procedimientos de que se trate.

V) NOTIFICACION ELECTRONICA

Si bien la notificación -en tanto actividad a través de la cual se lleva a conocimiento de alguien un acto o hecho constituye un aspecto del procedimiento administrativo, su análisis por separado está justificado por la circunstancia de que el legislador lo ha regulado en una disposición específica.

Conforme al art. 696 de la ley N° 16.736, "la notificación personal de los trámites y actos administrativos podrá realizarse válidamente por correo electrónico u otros medios informáticos o telemáticos, los cuales tendrán plena validez a todos los efectos siempre que proporcionen seguridad en cuanto a la efectiva realización de la diligencia y su fecha".

Según el régimen general previsto en los arts. 91 y sigtes. del Decreto N° 500/991 ya citado, la notificación personal se practicará en la oficina, en el domicilio o por circular[55].

Mientras que la primera de las tres modalidades indicadas -que supone en principio la concurrencia del interesado a la oficina de la Administración correspondiente podrá en adelante practicarse por medios informáticos, la

■[53] Miguel Angel GALLARDO ORTIZ - "Firmas electrónicas mediante criptología asimétrica", en Rev. de Informática y Derecho (U.N.E.D., Mérida, 1995), N° 1, pág. 19 y sigtes.

■[54] J. Andrés HALL - "El rol del encriptado de datos en la despapelización", en Rev. Derecho de la Alta Tecnología (Buenos Aires, 1996), Año VIII, N° 91, pág. 14 y sigtes.

■[55] Juan Pablo CAJARVILLE PELUFFO - "Procedimiento Administrativo" cit., pág. 115 y sigtes.

referencia a medios telemáticos (que implican la comunicación a distancia) en general, y al correo electrónico en particular[56], hace pensar en la notificación personal a domicilio, de computador a computador.

Cabe recordar que el inciso final del aludido art. 91 del Decreto N° 500/991 establecía que "también podrá practicarse la notificación a domicilio por telegrama colacionado certificado con aviso de entrega, por carta certificada con aviso de retorno, telex, fax o cualquier otro medio idóneo que proporcione certeza en cuanto a la persona a la que se ha practicado". Asimismo, el art. 477 de la ley N° 16.226 de 29 de octubre de 1991 también posibilitaba realizar las comunicaciones y notificaciones administrativas por fax.

Evidentemente, la referencia del texto reglamentario transcripto a "cualquier otro medio idóneo" podía interpretarse como abarcativa de las nuevas tecnologías informáticas y telemáticas. Sin embargo, su explicitación por una norma de rango legal debe reputarse trascendente. Además, la redacción del art. 696 es más precisa en cuanto reconoce la "plena validez" de la notificación electrónica, condicionada a que "proporcione seguridad en cuanto a la efectiva realización de la diligencia y a su fecha".

La introducción del concepto de seguridad vinculado a la efectiva realización de la diligencia y su oportunidad debe considerarse de principio. Consecuentemente, la falta de certeza o cualquier defecto trascendente afectará la validez de la notificación electrónica.

Obvio resulta añadir que la notificación electrónica supone la previa identificación por el interesado de su correo electrónico o similar, exigencia que puede considerarse encartada en la previsión del art. 119 del Decreto N° 500/991, cuando establece que las peticiones deberán contener "indicación del lugar donde deben realizarse las notificaciones".

■ [56] Fausto SERVELLO - "¿ Qué es la telemática ?" (Anaya, Madrid, 1985), pág. 137 y sigtes.

VI) DOCUMENTACION ELECTRONICA

1 - Amplio reconocimiento

De acuerdo al párrafo primero del art. 697 de la ley N° 16.736, "la documentación emergente de la transmisión por medios informáticos o telemáticos constituirá de por sí documentación auténtica y hará plena fe, a todos sus efectos, en cuanto a la existencia del original transmitido".

Se trata de una norma que amplia el antecedente del art. 129 de la citada ley N° 16.002 en dos aspectos sustanciales, a saber:

a) sustituye la referencia a "medios electrónicos" por la más precisa y abarcativa de "medios informáticos o telemáticos"; y

b) elimina la frase "entre dependencias oficiales", lo que apareja la universalización de la solución legal.

En orden a la caracterización del documento electrónico, siguiendo a la más calificada doctrina[57], antes de ahora nos hemos ocupado de determinar cómo la expresión "electrónico" califica al concepto de "documento"[58].

En tal sentido, hemos dicho que por documento electrónico cabe entender tanto el documento formado por el computador como aquel formado por medio del computador. En el primer caso, el computador no se limita a materializar una voluntad externa sino que determina el contenido de esa voluntad, decidiendo en el caso concreto según se vio (supra: capitulo IV, numeral 2). En el segundo caso, en cambio, el computador simplemente manifiesta una voluntad ya expresada.

■[57] Ettore GIANNANTONIO - "El valor jurídico del documento electrónico", en Informática y Derecho Depalma, Buenos Aires, 1987), vol. 1, pág. 94 y sigtes.

■[58] Carlos E. DELPIAZZO - "Transferencias electrónicas de fondos. Los medios de prueba", en Rev. FELABAN (Bogotá, 1989), N° 74, pág. 73 y sigtes., y en Rev. Tributaria, tomo XVI, N° 90, pág. 219 y sigtes.; y "Derecho Informático Uruguayo" cit., pág. 45 y sigtes.

Tal actividad de documentación puede manifestarse de distintos modos: puede estar soportada en la memoria del computador o en medio magnético, en cuyo caso no es legible por el hombre (documento electrónico en sentido estricto), o puede ser producida por el computador y perceptible por el hombre (documento electrónico en sentido amplio, también llamado documento informático).

Significa que muchos de los actos y trámites constitutivos del "expediente electrónico" serán documentos electrónicos en sentido estricto, en tanto que otros serán documentos electrónicos en sentido amplio.

En todos los casos, dicha documentación "constituirá de por sí documentación auténtica y hará plena fe", con lo que el legislador ha reconocido - en forma coherente con las demás disposiciones comentadas- la admisibilidad, el valor probatorio y la validez de la misma.

2 - Extensión de la cobertura penal

La segunda parte del art. 697 dispone que "el que voluntariamente transmitiere un texto del que resulte un documento infiel, adultere o destruya un documento almacenado en soporte magnético, o su respaldo, incurrirá en los delitos previstos por los arts. 236 a 239 del Código Penal, según corresponda".

Aún cuando el examen de esta disposición desde el punto de vista del Derecho Penal excede los limites de este análisis, el simple cotejo de su texto con la norma precedente contenida en el art. 130 de la ley Ni 16.002, permite advertir una significativa ampliación de los comportamientos reprimibles, a saber:

a) se elimina la limitación a la transmisión "entre dependencias oficiales"; y

b) se agrega la previsión de quien "adultere o destruya un documento almacenado en soporte magnético o su respaldo".

Debe reputarse que esta norma es la contracara de la atribución a la documentación electrónica del carácter de "auténtica" en principio, que le asigna la primera parte de la disposición comentada.

VII) CONCLUSION

Después de haber experimentado rápidos progresos, la Informática se ha visto enfrentada en los últimos años a una mutación acelerada como consecuencia de su imbricación con las telecomunicaciones, que ha abierto el nuevo horizonte de la Telemática, fenómeno del que la Administración no ha quedado al margen.

Las profundas transformaciones tecnológicas de nuestros días han suscitado pesimistas enfoques de los riesgos para la sociedad y optimistas perspectivas relativas a un nuevo relacionamiento de la Administración con los administrados, facilitando un diálogo más abierto, una mayor participación, y un mejor control en el ejercicio de los poderes públicos[59].

En ese escenario, el expediente electrónico es hoy una realidad en nuestro país, potenciada por un marco legal como el examinado que, con sobriedad y sencillez, atiende a las principales cuestiones que suscita a una Administración en renovación de la Informática con las telecomunicaciones.

■[59] Simón NORA y Alain MINC - "La informatización de la sociedad" (F.C.E., México, 1980), pág. 24 y sigtes.

Internet y el Derecho

ANTONIO-ENRIQUE PÉREZ LUÑO

Catedrático de Filosofía del Derecho
de la Facultad de Derecho de la Universidad de Sevilla

1. Internet: nueva frontera de la información y la comunicación.

No parece lícito dudar que Internet (*International Network of Computers*)está siendo el fenómeno estelar de las Nuevas Tecnologías de la información y la comunicación en la década de los noventa. En el umbral de un nuevo milenio Internet se presenta como un paso decisivo en el avance de los sistemas de información y comunicación a escala planetaria. Gracias a Internet cada ciudadano, sin moverse de su casa, puede acceder a los centros de documentación más importantes del mundo, puede realizar las más diversas operaciones financieras y comerciales, gozar de una enorme oferta de entretenimientos de la más diversa especie, y se puede comunicar con otros usuarios de la red sin limitaciones de número ni distancia. Si hace algunos años parecía que la "aldea global" era el gran reto del futuro, hoy Internet ha convertido en realidad presente el "hogar global", en la medida en que cada domicilio de los usuarios de la red constituye la terminal de un sistema integrado universal.

Conviene no resbalar, por su importancia, en la extensión presente y perspectivas futuras -se dice que cada dos minutos se incorpora un nuevo usuario a la red- de este amplísimo vehículo de información e intercomunicación. Internet es una red de redes que conecta más de dos millones de ordenadores

pertenecientes a instituciones académicas, entes públicos y empresas privadas. Se calcula que en la actualidad la emplean más de treinta millones de usuarios, cifra que aumenta en un diez por ciento cada mes. La explosión de su crecimiento se ha debido principalmente a la difusión del parque de ordenadores personales equipados con módem y con posibilidades de conectarse a la red telefónica. Con la aparición de herramientas de uso de la red accesibles a todos se ha multiplicado el número de usuarios no especialistas en informática, frente al carácter privativo para los expertos que Internet tuvo en sus inicios.

El ciberespacio es un microcosmos digital en el que no existen fronteras, distancias ni autoridad centralizada. Su conquista se ha convertido en meta obligada para quien desee sentirse miembro de la sociedad informática y es en la actualidad uno de los puntos de encuentro para el ocio y el negocio, que cuenta con mayores perspectivas de futuro.

2. Problemas y riesgos jurídicos de Internet.

No obstante, junto con esas incuestionables ventajas derivadas de las inmensas posibilidades de conocimiento, actuación y comunicación que permite la navegación por el ciberespacio, Internet ha hecho surgir en los últimos tiempos graves motivos de inquietud. El escándalo que meses pasados agitó a la opinión pública española, en relación con el tráfico de imágenes de prostitución infantil a través de Internet, así como la utilización de la red para difundir propaganda de bandas terroristas, ha supuesto la confirmación de un peligro desde hace algún tiempo anticipado. Los miles de ciudadanos españoles, inmediata o potencialmente, agredidos por esas imágenes criminales, abren una brecha en la inconsciencia cívica y política sobre los peligros que entrañan determinadas manipulaciones de las nuevas tecnologías. Ha sido preciso llegar a esta situación para que el conformismo cotidiano de quienes tienen como misión velar por la tutela de las libertades, y quienes tienen como principal tarea cívica el ejercerlas, se viese agitado por la gravedad del riesgo y la urgencia que reviste su respuesta.

No es admisible, al menos para juristas, políticos y tecnólogos, aducir sorpresa o desconocimiento de los eventuales peligros implícitos en el uso de las nuevas tecnologías. Desde hace tres décadas, quienes han evaluado el impacto de la informática en las libertades, han alertado sobre esos peligros, y cualquier especialista mínimamente avisado incurriría en negligencia inexcusable de haberlos desatendido. Es cierto que España, aun siendo una sociedad avanzada,

dista de los países con tecnología punta. De ahí que, entre nosotros, se juzgara mayoritariamente como una amenaza remota las advertencias y experiencias de asalto informático a las libertades, que con el descubrimiento de los abusos perpetrados a través de Internet se han convertido en una siniestra realidad.

Internet ha supuesto un factor de incremento de formas de criminalidad, al potenciar la difusión de sabotajes, virus y abordajes a los sistemas por parte de un número imprevisible e incontrolable de *piratas informáticos*. Las "autopistas de la información" entrañan también un grave riesgo para la protección de los programas. Asimismo, la facilidad de intercambiar informaciones a distancia puede generar importantes peligros para la protección de los datos personales.

Internet implica, por tanto, el riesgo de un efecto multiplicador de los atentados contra derechos, bienes e intereses jurídicos. Su potencialidad en la difusión ilimitada de imágenes e informaciones la hace un vehículo especialmente poderoso para perpetrar atentados criminales contra cuatro tipos de bienes jurídicos básicos:

1)*La intimidad, la imagen, la dignidad y el honor de las personas* (bienes que son tutelados en los artículos 197 ss. y 205 ss. del Código Penal de 1995), al posibilitar la intromisión indebida en datos personales, su transmisión no autorizada, el acoso informático, la propagación universal de difamaciones, calumnias e injurias, la incitación al odio o la discriminación raciales...

2)*La libertad sexual* al permitir la propagación de imágenes o informaciones que entrañen formas de exhibicionismo, provocación sexual o fomenten la pornografía entre menores de edad (actividades penadas en los arts. 185, 186 y 189 del nuevo Código Penal).

3)*La propiedad intelectual e industrial, el mercado y los consumidores* (bienes protegidos en los arts. 270 ss. del Código Penal), ya que Internet puede contribuir a la distribución ilícita de obras registradas como propiedad intelectual o industrial, a la piratería de programas, así como a la difusión de contenidos publicitarios ilegítimos.

4)*La seguridad nacional y el orden público* (garantizados por los arts. 544 ss. del Código Penal), en cuanto que pueden contribuir a facilitar atentados y desórdenes públicos, e incluso actividades terroristas.

El carácter internacional e ilimitado de esas conductas hacen más difícil su descubrimiento, prevención y castigo, ya que incluso en los casos en que puedan ser detectadas pueden plantearse conflictos sobre la jurisdicción sancionadora competente. Existe una evidente dificultad para determinar la responsabilidad jurídica en un medio, como el de Internet, en el que existen diferentes operadores que concurren en la cadena de comunicaciones: el proveedor de la red, el proveedor de acceso, el proveedor de servicio y el proveedor de contenidos. Esta problemática se agudiza cuando los diferentes elementos de la cadena se hallan en países distintos. Internet plantea una preocupante paradoja, que deriva de su eficacia global e ilimitada para atentar contra bienes y derechos, mientras que la capacidad de respuesta jurídica se halla fraccionada por las fronteras nacionales. Por ello, la reglamentación jurídica del flujo interno e internacional de datos es uno de los principales retos que hoy se plantean a los ordenamientos jurídicos nacionales y al orden jurídico internacional.

No huelga tampoco reconocer que la impunidad de determinadas formas de criminalidad informática no siempre constituye una negligencia imputable al legislador. Porque en un sector como el de las relaciones entre la Informática y el Derecho, constantemente, cada Feria tecnológica abre nuevas proyecciones informáticas al Derecho, o innova bienes informáticos que requieren nuevos procedimientos de tutela jurídica, o da a conocer dispositivos que condenan al anacronismo los medios de protección jurídica anteriormente existentes. La criminalidad informática se caracteriza, en suma, por las dificultades que entraña *descubrirla, probarla y perseguirla.* Se ha hecho célebre la imagen de que los sistemas informáticos son como "queso de Gruyer", por las enormes oquedades y lagunas que quedan siempre abiertas a posibles atentados criminales.

3.Sistemas de seguridad en Internet.

Aunque Internet puede haber contribuido a crear nuevos riesgos las técnicas informáticas ofrecen también nuevas medidas de seguridad para oponerse a los atentados contra bienes e intereses jurídicos. Entre las medidas de seguridad más difundidas y eficaces se pueden citar las siguientes:

a)*Programas de encriptación*, que permiten la conversión de mensajes en lenguaje natural en textos que utilizan un lenguaje clave y que aseguran que nadie excepto quien posea la transcripción de esas claves podrá descifrar. Ha adquirido

especial celebridad el programa de encriptación debido a Philip Zimmermann denominado PGP(*Pretty Good Privacy*), que está siendo utilizado por numerosos usuarios de Internet.

Si bien estos programas de seguridad, junto a sus logros para garantizar la confidencialidad de la transmisión de informaciones lícitas, tiene su reverso en haber contribuido a dificultar el descubrimiento de redes informativas ilícitas. La DEA, servicio norteamericano antidrogas, así como otros servicios policiales, han denunciado sus dificultades para perseguir a los narcotraficantes entre los laberintos y las encriptaciones de sus mensajes electrónicos.

b)*Los filtros*, consistentes en programas informáticos selectivos que bloquean el acceso a determinados documentos pero no a otros. La Unión Europea apoya la denominada PICS (*Platform for Internet Content Selection*). Se trata de un servicio para seleccionar contenidos en Internet que lanzó oficialmente el *World Wide Web Consortium*. Estos filtros pueden programarse en un triple sentido: 1) *"Lista blanca"*, dejando pasar solamente aquellos servicios o informaciones que previamente han sido registrados; 2) *"Lista negra"* bloqueando aquellos servicios o programas a los que no se desea tener acceso. Se ha hecho famosa la lista *CyberNot*; que abarca unos siete mil programas clasificados como nocivos por sus contenidos de violencia, obscenidad, racismo, cultos satánicos, drogas... Gracias a este sistema los padres pueden bloquear de forma selectiva el acceso a aquellos servicios que consideran nocivos o peligrosos para sus hijos; 3) *"Etiquetado neutro"* , permitiendo construir un menú de servicios personalizados para cada usuario. Este sistema ofrece un alto grado de flexibilidad y seguridad, al facilitar que cada usuario realice personalmente la criba de aquellos contenidos de Internet que juzgue apropiados a su sensibilidad, cultura y sistema de valores.

c)Los cortafuegos, que operan facilitando o impidiendo la transferencia de imágenes o datos desde Internet a un ordenador o viceversa. Estos sistemas de seguridad permiten el acceso a aquellos servicios previamente establecidos, cortando la entrada o salida a los demás.

d)Los certificados digitales, que permiten identificar o relacionar a todas las partes que intervienen en transacciones comerciales realizadas a través de Internet, dotándolas de la máxima rapidez y seguridad. Así, por ejemplo, el sistema SET (Secure Electronic Transaction).

e)Los Ciberpolicías, se trata de entidades, como por ejemplo FIRST (Forum of Incident Response and Security Teams) y CERT (Computer Emergency Response Team), las cuales ofrecen equipos de expertos en la localización de piratas informáticos, y suministran programas de defensa frente a sabotajes y proporcionan ayuda en caso de siniestros informáticos. Algunas policías de países técnicamente desarrollados han organizado unidades especiales en la investigación de actividades criminales realizadas a través de Internet. En España existe un Grupo de Delitos Informáticos perteneciente a la Unidad Central de Policía Judicial.

Estos sistemas de seguridad representan un principio de esperanza frente a los riesgos y peligros que, sin resquicio a dudas, comportan las actividades abusivas o ilícitas realizadas a través de Internet. Su eficacia es diversa y, todavía, difícilmente evaluable, pero esos sistemas demuestran frente a pesimistas y escépticos que Internet no es un paraíso para el ejercicio de la delincuencia, ni un espacio inexorablemente condenado a la zozobra y la inseguridad.

4.El ciberespacio: ¿anarquía libertaria o libertad garantizada?.

Como la mayoría de las grandes conquistas científicas y tecnológicas que registra la historia, Internet es una realidad ambivalente. Renunciar a sus logros sería hoy una pretensión imposible, porque se trata de un avance irrenunciable y un signo del progreso de nuestro tiempo. Pero ello no debe conducir a aceptar pasivamente o a claudicar ante los riesgos de "abordaje" criminal que amenazan la navegación por el ciberespacio.

Como he indicado, en sus inicios, uno de las mayores alicientes de Internet residía en su carácter ácrata ; se trataba de un espacio absolutamente libre, sin ningún tipo de autoridad o poder que lo regulara o acotara. Como elocuente ejemplo de esa concepción anárquica y libertaria de Internet puede citarse la Declaración de Independencia del Ciberespacio "promulgada" por John Perry Barlow en Davos, Suiza, el 8 de Febrero de 1996. Dicha Declaración ha adquirido notable celebridad en estos meses entre los usuarios de Internet. Consiste en un texto que, en mi opinión, se articula en torno a tres ideas-guía:

1ª) La afirmación de la total autonomía de los cibernautas respecto a cualquier tipo de autoridad estatal: "Gobiernos del Mundo Industrial...No son

bienvenidos entre nosotros. No tienen ninguna supremacía donde nos juntamos...El Ciberespacio está fuera de sus fronteras".

2ª) Negación de los conceptos y categorías jurídicas tradicionales :"Vuestros conceptos legales de propiedad, expresión, identidad, movimiento y contenido no se aplican a nosotros. Aquellos se basan en la materia, pero en nuestro mundo la materia no existe".

3ª) Confianza utópica en un ciberespacio ideal: "Crearemos una civilización de la Mente en el Ciberespacio. Que sea más humana y justa que el mundo creado anteriormente por sus gobiernos".

Como contrapunto a esa visión idílica de Internet señala el profesor de Teoría de la Comunicación en la Universidad París-VII y Director de Le Monde Diplomatique , Ignacio Ramonet, que el ciberespacio está siendo colonizado despiadadamente por todos los gigantes de las telecomunicaciones. Internet está creando nuevas formas de desigualdad entre "inforricos" e "infopobres", al establecer discriminaciones graves en el acceso y utilización de informaciones entre el Norte y el Sur, donde la falta de equipos va a condenar a la marginación a millones de personas. Recuerda, por ejemplo, que hay más líneas telefónicas sólo en la isla de Manhattan (Nueva York), que en toda Africa negra, y sin esas líneas no se puede acceder a Internet. Según Ramonet resulta ingenuo pensar que necesariamente el aumento de comunicación debe traducirse en mayor equilibrio y armonía social. La comunicación, en sí, no es progreso social "y mucho menos cuando la controla, como es el caso de Internet, las grandes firmas comerciales y cuando, por otra parte, contribuye a acrecentar las diferencias y desigualdades entre ciudadanos de un mismo país, y habitantes de un mismo planeta. Internet - concluye Ramonet- era una esperanza; nos la han robado".

Internet ha abierto nuevas y preocupantes posibilidades operativas a los sistemas de control social y político. Se ha hecho célebre una imagen expuesta por Philip Zimmermann en su informe ante el Subcomité de Política Económica, Comercio y Medio Ambiente del Congreso Norteamericano. Indicaba allí Zimmermann que en el pasado cuando el Estado pretendía violar la intimidad de los ciudadanos debía esforzarse en interceptar, abrir al vapor y leer el correo, o escuchar, grabar y transcribir conversaciones telefónicas. Eso era como pescar con caña, de pieza en pieza. Por el contrario, los mensajes del correo electrónico son más fáciles de interceptar y se pueden scanear a gran escala, y ordenar en función

de palabras claves. Esto es como pescar con red; y supone una diferencia orwelliana cuantitativa y cualitativa para la garantía de la democracia.

El utopismo ácrata se opone a cualquier regulación del Ciberespacio por entender que con ello se reprime la libertad de los cibernáutas, a la vez, que se refuerza el poder estatal. Pero la realidad no es tan simple. Paradójicamente los grandes beneficiarios de la anarquía de Internet no son los cibernáutas particulares, sino las grandes multinacionales e, incluso los aparatos de control social de los gobiernos. No huelga advertir que, en los últimos meses, se están transmitiendo por Internet, sin ningún tipo de garantías y con evidente menoscabo del derecho a la intimidad, datos personales (incluso voz e imagen) en investigaciones policiales; a través de un medio que por su naturaleza y características es accesible a millones de usuarios de todo el mundo. Tampoco está de más, recordar que algunos Colegios de Abogados norteamericanos han denunciado las prácticas de determinadas oficinas fiscales tendentes a interceptar las comunicaciones por Internet entre distintos bufetes de sus colegiados, especialmente en casos referentes a narcotráfico.

Los peligros de una utilización abusiva, incontrolada o criminal de ese espacio plantean ahora, de forma apremiante, la necesidad de su ordenación. Han sostenido historiadores muy autorizados que la historia es cíclica y retorna siempre; quizás por ello los actuales debates sobre Internet recuerdan a aquellos mantenidos hace siglos por los filósofos contractualistas en relación con el estado naturaleza. En la tradición contractualista se explica el origen de las instituciones políticas y jurídicas a partir de la exigencia -empírica o racional, utilitaria o ética, a tenor de las diversas interpretaciones del estado de naturaleza y el pacto social- de abandonar una situación (el estado de naturaleza) en la que el hombre posee una ilimitada (aunque insegura) libertad, a otra de libertad limitada pero protegida y garantizada por la autoridad y las leyes.

5.Algunas respuestas jurídicas.

Una vez perdida la inocencia del idílico "estado de naturaleza" de libertad sin restricciones de Internet, las circunstancias aconsejan remediar los peligros del desorden mediante soluciones jurídicas. Esa necesidad de apelar al Derecho para poner coto a los abusos perpetrados desde Internet ha llevado a algunos juristas de nuestros país a invocar el art. 301 del nuevo Código Penal, que pena a quien "convierta o transmita bienes, sabiendo que éstos tienen su origen en un delito grave...". Cabría asimismo aducir que, en la medida en que Internet es hoy, entre

otras muchas cosas, un espacio lúdico utilizado para su esparcimiento de forma habitual por un creciente número de niños, sería posible incriminar, al amparo del art. 186 del Código Penal, a quién "por cualquier medio directo, difundiere, vendiere o exhibiere material pornográfico entre menores de edad o incapaces...".

Pero el recurso a esas normas suscita la inquietud de si se está escanciando el vino nuevo de las más recientes formas de criminalidad informática en los odres viejos de tipos penales pensados para castigar conductas delictivas ajenas al universo tecnológico. Porque a diferencia de los más graves atentados informáticos contra la intimidad, la utilización ilícita de tarjetas electromagnéticas y la estafa o fraude informáticos, que se hallan expresamente previstos en el nuevo Código Penal (en los arts. 197, 239 y 248.2, respectivamente), parece evidente que nuestro legislador penal no pensaba en Internet al tipificar el delito de receptación o de exhibicionismo y provocación sexual. Por ello, la aplicación de estos tipos puede suscitar serias dudas en orden al respeto del principio de legalidad penal, pero no hacerlo puede provocar situaciones de profunda alarma en la sociedad.

En los últimos meses se han producido algunas iniciativas dirigidas a establecer un marco jurídico regulador de los contenidos criminales de Internet. La más importante ha sido la Ley para la Decencia en las Comunicaciones (Communications Decency Act.), aprobada por el Congreso de los Estados Unidos en febrero de 1996. Dicha ley prevé sanciones para quienes almacenen o distribuyan por la red informaciones, imágenes o sonidos que puedan considerase obscenos o indecentes por agredir a la media de los valores morales de la comunidad.

Esta norma ha suscitado una viva polémica entre los juristas y ha sido objeto de diversos recursos. Como resultado de uno de ellos, un Tribunal de Pennsylvania ha declarado la inconstitucionalidad de dicha ley. Se considera que en ella se limita injustificadamente el derecho a la libertad de expresión garantizado en la primera enmienda de la Constitución norteamericana, ya que al no considerar las informaciones transmitidas por Internet como prensa escrita se las somete a la censura previa por parte de la influyente Comisión Federal de Comunicaciones. Se denuncia también, como atentado a la seguridad jurídica, la forma excesivamente vaga e imprecisa con la que se tipifican los supuestos que pueden entrañar atentados contra la decencia. Asimismo se considera que, la legítima protección de los menores, no debiera limitar la libre difusión de

informaciones o imágenes normales para adultos, ya que los suministradores de servicios no pueden determinar la edad de los usuarios.

6.Iniciativas de la Unión Europea.

En el seno de la Unión Europea se ha elaborado, en octubre de 1996, una Comunicación de la Comisión sobre Contenidos ilícitos y nocivos en Internet. Constituye el fin principal de dicho documento el logro de "un correcto equilibrio entre la garantía de la libre circulación de la información y la protección del interés público" entre los Estados miembros de la Unión Europea. Se parte para ello del principio básico de que lo que es ilegal fuera de la red también lo es en ella, por lo que los Estados miembros deben aplicar la legislación existente que pueda sancionar esas conductas ilícitas. No obstante, dada la descentralización y el carácter planetario de Internet, parece necesario establecer medidas en el ámbito de Justicia e Interior para intensificar la cooperación y la respuesta jurídica unitaria frente al reto que representa la criminalidad en Internet. Para ello, la Comisión, en el documento de referencia, insta a incrementar el intercambio de información entre los Estados miembros sobre los suministradores de contenidos delictivos; al tiempo que exhorta a los Estados miembros para que establezcan "criterios europeos mínimos" sobre contenidos criminales en Internet. La comisión reitera su propósito de fomentar los proyectos de autorregulación elaborados por las asociaciones de suministradores de acceso a Internet, por considerar que el papel de las mismas es de primordial eficacia para limitar la distribución de contenidos ilícitos en la red.

Complementaria, en cuanto a su cronología y alcance, de esa iniciativa se puede considerar el Libro Verde sobre la protección de los menores y de la dignidad humana en los nuevos servicios audiovisuales y de información, debida también a la Comisión respondiendo a una petición previa del Parlamento Europeo y del Consejo. Si se coteja el Libro Verde con la Comunicación se advierte que se trata de un documento, paradójicamente, más genérico y más específico. Más genérico en cuanto a su ámbito, ya que no se limita a la regulación de Internet, sino que se ocupa de todos los servicios audiovisuales y de información. Pero, al propio tiempo, se trata de un texto más específico en cuanto a su objeto, ya que se circunscribe a la protección de los menores y de la dignidad humana.

El Libro Verde recuerda que la protección jurídica de los menores y la dignidad en las normas constitucionales y legislativas de los Estados miembros de

la Unión Europea tienen como soporte básico el Convenio Europeo de Derechos Humanos. Dicho Convenio ha sido integrado en el ordenamiento jurídico comunitario por el art. F2 del Tratado de la Unión Europea.

En el Convenio Europeo se reconoce el derecho al respeto de la vida privada y familiar (art.8) y, asimismo, el derecho a la libertad de expresión (art.10). No obstante, ambos derechos no son considerados como absolutos e ilimitados, al estar previsto que pueda condicionarse su ejercicio por medidas necesarias, en una sociedad democrática, para garantizar la seguridad, la salud, la moral o los derechos y libertades de los demás (arts.8.2 y 10.2).

La libertad de expresión a través de los servicios audiovisuales y, en consecuencia, de Internet no es ilimitada en el seno de la Unión Europea, si bien, sus limitaciones deben ser admitidas restrictivamente. No en vano la libertad de prestar servicios, también en la esfera de la información y la comunicación, es una de las libertades básicas reconocidas en el Tratado de la Unión. El Libro Verde se remite a la jurisprudencia del Tribunal Europeo de Derechos Humanos (TEDH) de Estrasburgo para advertir que la libertad de expresión defiende no sólo las ideas e informaciones que no suponen intromisión u ofensa en los valores o derechos ajenos, sino también las susceptibles de ofender, contradecir o perturbar (STEDH, Handyside/Reino Unido, 1976).

El Libro Verde, acogiendo la jurisprudencia del TEDH (SS, Handyside/Reino Unido, 1976; The Sunday Times/Reino Unido, 1979; Autronic, 1990; Groppera Radio, 1990; Informationsverein Lentia, 1993), propugna que las restricciones a la libertad de expresión fundadas en la defensa de derechos ajenos, en concreto de los de los menores y la dignidad, se halle condicionada a tres exigencias acumulativas:

1)Prohibición de arbitrariedad , lo que implica que cada restricción deba estar prevista por la ley;
2)Necesidad social imperiosa de garantizar valores y derechos de las sociedades democráticas;
3)Legitimidad de objetivos, enumerados de forma limitada y entre los que la defensa de la moralidad y la salud públicas se estiman particularmente adecuados para proteger a los menores y la dignidad humana.

Es fácil inferir los problemas que pueden derivarse de la precisión de lo que, en cada caso, deba considerarse como "necesario" para legitimar una medida

legal restrictiva y que persiga un "objetivo legítimo". No basta para ello que tal medida resulte "útil" o "razonable". El carácter legítimo de la medida sólo puede probarse tras un profundo examen de su eficacia en relación con el grado de injerencia que implica. Este análisis constituye una prueba de proporcionalidad de las medidas restrictivas. De ello se desprende que no deben imponerse restricciones a la libertad de expresión audiovisual que no estén justificadas en virtud de dicha prueba de proporcionalidad.

El Libro Verde, en definitiva, auspicia una regulación de las redes audiovisuales que tienda a armonizar la libertad de expresión con la defensa de los menores y de la dignidad. Para ello, aboga por el establecimiento de sistemas (por ejemplo, filtros de clasificación de contenidos) que garanticen que los menores no accedan a programas perjudiciales, permitiendo no obstante el acceso de los adultos. Se trata de soluciones procedentes de la base (bottom up) más que procedentes desde arriba (top down), que permiten obviar la necesidad de censura previa y aumentan la potencial eficacia de la autorregulación

7.Hacia una ética jurídica ciberespacial.

No es este el lugar para una consideración detenida en pormenores sobre las múltiples implicaciones económicas, culturales, sociales y políticas que se derivan de ese ciberespacio cuya navegación y conquista ha hecho posible Internet. Las consecuencias que pueden derivarse de esa forma de comunicación humana en soporte informático son imprevisibles y, a veces, paradójicas. Puede darse la circunstancia de que el máximo desarrollo de la comunicación tecnológica implique simultáneamente un empobrecimiento de las formas de comunicación tradicionales. Suele aducirse, para corroborar esos riesgos, la anécdota de un foro de "cibernautas" que concertaron un encuentro personal para reforzar sus contactos iniciados a través de Internet. La reunión fue un completo fracaso por las dificultades para establecer un diálogo interpersonal; la comunicación sólo se hizo de nuevo fluida cuando cada uno de los cibernautas la reemprendió desde su pantalla de ordenador.

No obstante, esta reflexión pecaría de un exceso de pesimismo si no reconociese las posibilidades de una renovación de los valores cívicos que puede promover Internet. Las redes de telecomunicaciones pueden conducir a una nueva ética "ciberespacial", que genere y estimule actitudes de conciencia colectiva sobre el respeto de las libertades y de los bienes amenazados por una utilización indebida del ciberespacio, y contribuir a la formación de vínculos solidarios para

la prevención de los crímenes informáticos y la ayuda a su descubrimiento. La difusión capilar de las redes comunicativas puede conducir a la producción de reglas jurídicas consuetudinarias sobre su uso, en las que la dimensión coactiva de las normas basada en la autoridad de un poder centralizado, dejè paso a códigos de conducta cuya eficacia se base en la convicción de los usuarios y en su responsabilidad solidaria.

8.Bibliografía.

Barlow, J. P., Declaración de Independencia del Ciberespacio, en "Cibernautas por la Tolerancia", http://www.ctv.es/ USERS/mrb/tolerancia/.

Branscomb, A.W., (1995): Anonimity, Autonomy and Accountability: Challenges to the First Amendment in Cyberspace, en "Yale Law Journal", n.104, pp. 1639 ss.

Bustos, M., Detectives en el Ciberespacio, en "Especial Simo", "El País", 5, noviembre, 1996.

Byassee, W.S., (1995): Jurisdiction of Cyberspace, en "Wake Forest Law Review", n. 30, pp. 197 ss.

Cavazos, E.A. y Morin, G.,(1994): Cyberspace and the Law, MIT Press, Cambridge (Mass.).

Ciampi,C.,Guida all´informazione giuridica nel ciberspazio, http://www.idg.fi.cnr.it/ita/informazione/guida/cs_guide.htm.

Ciampi, C., (1995), Una guida per giuristi nel ciberspazio di Internet: strumenti per la navigazionee prospettive di sviluppo, en Atti del Congresso Annuale AICA, Chia-Cagliari, vol.I, pp. 543-550.

Colom, V. y Van Bolhuis, H. E, (1995): Cyberspace Reflections, European Commission, Brussels.

Contenidos ilícitos y nocivos en Internet, (1996), Comunicación de la Comisión de las Comunidades Europeas, en "Documentos COM (96)" 487 final.

Cutrera, T., (1991): The Constitution in Cyberspace: the Fundamental Rights of Computers Users, en "University of Missouri Law Review", n. 60, pp. 139 ss.

Fernández Calvo, R., El Ciberespacio y sus dilemas en "Especial Simo", "El País", 5, noviembre, 1996.

Forester, T. y Morrison, P. (1990): Computer Ethics. Cautionary Tales and Ethical Dilemmas in Computing, MIT Press, Cambridge (Mass.).

Internet desde la perspectiva jurídica, en Manual práctico de Internet, nº 13, en "Cuadernos de Cinco Días", 19, Febrero, 1997.

La explosión Internet, Dossier de "Muy Especial", 1997, nº 28.

Libro Verde sobre la protección de los menores y de la dignidad humana en los nuevos servicios audiovisuales y de información (1996), Comisión de las Comunidades Europeas, en "Documentos COM (96)" 483 final.

Moreno, M. A, (1995): ¿Es segura la Internet?" en "Base Informática", n. 27, pp.60-65

Pérez Luño, A.E., (1996): Manual de Informática y Derecho, Ariel, Barcelona.

Pérez Luño, A.E., Internet navegaciones y abordajes , en "ABC" (Tribuna Abierta), 28, Octubre, 1996.

Pérez Luño, A.E., (1997), Internet navegaciones y abordajes, en "La Ley" (Revista Jurídica Española de Doctrina, Jurisprudencia y Bibliografía), nº 4258, pp. 1 y 14-15.

Ramonet, I., ¡Nos han robado una esperanza! en Internet, ¿un bien o una maldición? en "El País Digital- Debates", 25/2/97.

Ribas, J., Aspectos legislativos de las autopistas de la información: Delitos en Internet en "Jornadas Profesionales Informat- 96", Barcelona, Octubre 1996.

Rico, I, (1995): Navegar por Internet en, "Ideas-IBM" n. 15.

Impacto de las Nuevas Tecnologías y de la globalización en el Estado Moderno

SILVIA SUSANA TOSCANO

Abogada. Universidad de Buenos Aires (ARGENTINA)

INTRODUCCION

"La historia brinda, supuestamente, un conocimiento del contexto más amplio en el cual se ubica nuestra vida. No es simplemente la evolución de la tecnología; es la evolución del pensamiento." (La Novena Revelación de James Redfield Pag.31)

Ha sido mi deseo comenzar este artículo citando este novedoso libro del cual he extraído la frase precedente porque destaca, en una sociedad que la historia describirá diciendo que su característica más notable es el progreso tecnológico, la importancia del pensamiento que, en definitiva, es destacar nada más y nada menos que la importancia del hombre.

Trataré de abordar en las siguientes páginas distintas cuestiones compartiendo con ustedes las inquietudes que, como abogada perteneciente a la administración pública me han surgido en los últimos años como consecuencia de este proceso de globalización y tecnificación en el cual estamos inmersos y frente al cual sólo podemos reorganizarnos y reordenarnos mas no ignorarlo.

Es el propio contexto jurídico-institucional el que deberá evolucionar para dar respuestas inmediatas y precisas a los planteamientos tecnológicos siendo

el derecho el ámbito del cual se esperan los mayores cambios y sólo es posible su desarrollo futuro si nuestro pensamiento de juristas es capaz de aprehender esta realidad y dar soluciones creativas a los nuevos planteos. He aquí la razón de la cita de la frase de Redfield.

ALCANCES DEL IMPACTO A NIVEL INSTITUCIONAL

El que fuera el paradigma de los estados de la segunda mitad del siglo XIX, o sea, el estado democrático liberal basado en la autonomía y en la capacidad de autogobernarse y de determinar su futuro cede ante la fuerza de la mundialización de la economía que crea mercados únicos, ante la existencia de intereses supranacionales e internacionales reduciéndose la noción de Estado-Nación a efectos meramente territoriales o ancestrales.

No es casual que los avances tecnológicos y la globalización se imbriquen con procesos mundiales de reforma del Estado dejando paso a una noción de estado "liberal" o "subsidiario" producto de la transformación de las estructuras socioeconómicas e institucionales. Este nuevo estado que reemplaza al Estado de bienestar transfiere a los particulares importantes sectores hasta ahora bajo su dominio manteniendo para sí aquellas funciones indelegables como la justicia, la seguridad, el manejo de las relaciones exteriores y la educación, entre otras.

La liberación de la economía de las trabas y limitaciones estatales coloca al Estado como actor y gestor principal de esta transformación social y económica. Para cumplir semejante compromiso debe capacitarse, fortalecerse y modernizarse.

Por otra parte, el rol de la política se desdibuja detrás de factores y fuerzas económicas favoreciendo ese pasaje de una economía nacional controlada por el Estado a una economía de mercado altamente mundializada.

Frente a ello, la globalización supone la crisis de la noción tradicional de estado liberal desdibujando las fronteras especialmente cuando las comunicaciones y la tecnología de la información desbordan la posibilidad de control en áreas donde otrora estos estados ostentaban el monopolio y un dominio indiscutido .

¿Cómo imaginar la famosa "aldea global" sin una red informática pública de fácil acceso como es Internet mediante la cual los ciudadanos puedan

desarrollar su vida social y laboral?. Sin embargo, los estados modernos poco pueden regular acerca del uso y del acceso a esta autopista de la información ya que los intereses y las soberanías nacionales ceden ante acuerdos regionales y supranacionales.

Asimismo, estos estados modernos utilizan las redes de información para sus políticas culturales, educacionales y aún institucionales siendo muy común la existencia de páginas WEB no sólo para espacios publicitarios o de propaganda proselitista sino también con carácter interactivo o bidireccional.

Conjuntamente con este cambio en el rol tradicional del estado, se promueve el surgimiento de una administración pública diferente y un Derecho Administrativo novedoso donde prima la realidad sobre la ideología.

Este estado liberal o subsidiario al que me he referido debe no sólo asumirse como integrante de un mundo jurídica y económicamente globalizado sino también como receptor de todos los progresos tecnológicos que le permitirán desarrollar una modernidad al servicio de los ciudadanos.

Por otra parte, recordemos que el Estado moderno se encuentra en un período de transición entre una etapa de ajuste económico que ha provocado y provoca aún un aumento de la brecha de las desigualdades y una etapa de "deuda social" en la que deberá combinar el cumplimiento de objetivos económicos con los sociales. Este proceso es global en mayor o menor medida y vuelve a colocar a la política y al Estado en primer plano.

Pero esta apertura a las innovaciones tecnológicas obliga al replanteamiento de muy diferentes cuestiones que van desde la implementación de políticas para la adquisición de aquellas hasta la búsqueda de soluciones concretas ante los innumerables planteamiento que se suscitan con la aplicación de las mismas.

En concreto, a continuación analizaré someramente las situaciones que han sido objeto de estudio tales como las particularidades de la adquisición de recursos informáticos y nuevas tecnologías en la administración pública, las implicaciones del documento electrónico administrativo, la seguridad y la protección de datos y la conservación de los actos administrativos en archivo no tradicionales.

PAUTAS DE CONTRATACION DE TECNOLOGIA EN LA ADMINISTRACION PUBLICA.

Cuando se habla de modernización del Estado, generalmente se piensa en una gran inversión en recursos informáticos, principalmente hardware y software la cual no siempre va acompañada de una política y una estrategia global adecuada a las necesidades .

No dudo que el Estado, al ser una gran organización con manejo de grandes volúmenes de información, es una de las áreas más propicias para la aplicación de la informática y de tecnología de punta pero ello no puede llevar a una adquisición indiscriminada de equipamiento que al poco tiempo se transforma en obsoleto con la correspondiente pérdida de agilidad y competencia técnica.

Asimismo, esta inversión debe requerir la correspondiente capacitación de los agentes de la administración para permitir un mejor y más racional aprovechamiento de aquélla. De lo contrario, el objetivo perseguido con la incorporación tecnológica que es la eficiente y rápida gestión de la cosa pública, es neutralizado por una formación no adecuada, indiscriminada e irracional.

El Estado debe prever su política en materia de contrataciones informáticas y de tecnología de punta y arbitrar los mecanismos necesarios para que las mismas estén dotadas de celeridad y eficiencia especialmente en aquellas incorporaciones de tecnología que , por su complejidad u onerosidad requieren una mayor transparencia, racionalización y aprovechamiento de los fondos públicos.

Los procedimientos administrativos actuales no satisfacen los requerimientos de una administración rápida y eficiente como debe ser la del estado moderno inmerso en un intercambio de información. Esto se produce no sólo porque los mecanismos de contratación se demoran en el tiempo y en la burocracia provocando, en más de un caso, que la tecnología de punta se transforme en obsoleta e inoportuna sino también porque no existe o no se quiere que exista una modalidad que asegure la innovación tecnológica oportuna y conveniente y que sea algo más que el cumplimiento del paradigma de la modernidad.

Existen, en mi criterio ciertas pautas que deben ser tenidas en cuenta y que, a título de ejemplo son: la capacidad técnico financiera de la empresa proveedora y su solvencia moral, económica y técnica, características que aseguren la continuidad del asesoramiento, la compatibilidad con otros sistemas, el respeto por la normativa internacional en materia de patentes, licencias y propiedad intelectual, la actualización permanente, etc. Asimismo, es muy relevante los antecedentes de la empresa en el mercado y en especial su comportamiento en otras contrataciones lo que nos permite analizar el cumplimiento de sus obligaciones contractuales, legales, fiscales y/o administrativas.

Se deben adecuar los controles existentes en las sucesivas etapas de una contratación - sea directa o por licitación- y, además, los mismos deben mantenerse una vez puesta en marcha la inversión a los efectos de lograr una eficiente aplicación de la tecnología adecuada al cumplimiento del objetivo previsto en el momento de su incorporación.

No pretendo en este artículo agotar este tema de por sí muy complejo y extenso y al cual me he referido en otros trabajos (ver bibliografía citada). Es mi intención simplemente repensar el hecho de que la globalización y el intercambio de información nos exige el dominio y el conocimiento de tecnología para lo cual el Estado no sólo debe capacitar a sus agentes en la aplicación que de ella se haga sino dotar a sus cuerpos técnicos y consultivos de herramientas que les permitan mantener un cierto equilibrio en la negociación y que, fundamentalmente le proporcione la cuota de transparencia que la sociedad le exige como respuesta al manejo de sus fondos y de sus voluntades políticas. Una dependencia en materia tecnológica puede ocasionarle al Estado graves perjuicios por dejar al libre arbitrio funciones y objetivos que le son indelegables como así también datos que requieren su protección porque en ellos está el destino de la sociedad.

IMPLICACIONES DEL DOCUMENTO ELECTRONICO ADMINISTRATIVO

¿Cómo se manifiesta la actividad administrativa? En actos administrativos de menor o mayor complejidad que hacen a la operatividad, gestión y servicio propio de la actuación del Estado. Dicha complejidad viene generalmente justificada por la garantía de imparcialidad y por la tutela del interés público. El procedimiento administrativo involucra enormes volúmenes de datos, múltiples instancias preparatorias y consultivas, intervención de numerosos agentes, todo

ello con el objetivo de cumplir las funciones específicas del Estado en un marco de eficiencia y transparencia que garantice la seguridad jurídica.

La incorporación de la informática a la actividad administrativa no plantearía, en principio, diferentes cuestiones que aquellas que se suscitan en una gran organización privada a no ser por la función de incontestabilidad que deben cumplir estos actos en cuanto manifestaciones de la voluntad estatal. El reemplazo del papel por el documento electrónico no produce los mismos efectos en el mundo privado que en el ámbito público. Ello así porque si bien toda actividad debe tender a perpetuar su contenido, en el derecho público, el formalismo y la necesidad de materialidad son aún mayores porque hacen a la certeza pública.

La irrupción de la informática en un mundo como el jurídico caracterizado por el uso del papel como soporte documental y basado en un formalismo riguroso pone en crisis la propia noción de documento y si esto se traslada al ámbito estatal la cuestión se complica por la necesidad de protección del valor fe pública e integridad del documento administrativo.

Actualmente es común el uso de la informática en la gestión estatal, a nivel contable, en la formación y administración de bases de datos pero todavía no se utiliza en la formación, emisión, publicidad y conservación del acto administrativo. Estamos en presencia de un nuevo desafío: la elaboración de una teoría del acto administrativo electrónico.

La mayoría de las legislaciones administrativas requieren que el acto se realice en forma escrita donde conste el autor, la fecha, la firma, y otros requisitos formales además de la motivación, la causa, el organismo emisor, etc. Para que el acto administrativo electrónico pueda ser reconocido como documento se debe asegurar la inalterabilidad de los datos y de su procedimiento, la integridad y fidelidad de su contenido, entre otras.

Hasta el momento en Argentina no se ha realizado una reforma legislativa integral que recepte la validez del documento electrónico si bien numerosa jurisprudencia y fundamentalmente la práctica admiten su presentación en juicio.

En el ámbito público, un paso importante se ha dado con la sanción de la Ley de Presupuesto de 1995 (Ley Nro 24624) que, en su artículo 30 prevé la destrucción de los documentos en soporte papel pertenecientes al Archivo

General de la Nación, organismo que testimonia cada uno de los gastos realizados por el Estado Nacional. Este procedimiento sólo se lleva a cabo luego de la digitalización y archivo de los mismos en soportes magnéticos que aseguran la integridad y la inalterabilidad del contenido del documento.

La tecnología digital ha traído aparejada esta posibilidad que pone fin al almacenamiento de millones de legajos en papel siendo el original un documento electrónico en un disco óptico. El procedimiento someramente es el siguiente: el expediente administrativo es escaneado y la imagen digitalizada pasa a una oficina de control pasando el cual, se labra el acta de destrucción del documento y el documento papel desaparece siendo el auténtico aquel incorporado en el disco. Es de esperar que esta práctica se difunda entre los organismos públicos y pueda encararse una reforma integral del procedimiento administrativo que permita el tratamiento electrónico del acto administrativo desde su emisión.

Una cuestión que preocupa a los administrativistas es la relativa a la firma que, entre otras condiciones, otorga al acto administrativo validez. ¿Qué pasaría si un funcionario firmara sobre el teclado de su computador personal convalidando un acto abandonando totalmente el papel?. Aún estamos lejos de admitirlo pero sin lugar a dudas a corto plazo esta es una de las cuestiones que requerirán nuestra consulta. La firma digital o electrónica será otra de las innovaciones tecnológicas que nos obligará a pensar en esta transformación del derecho inevitable y, por otra parte fascinante.

SEGURIDAD Y PROTECCION DE LOS DATOS Y DE LOS PROCEDIMIENTOS ADMINISTRATIVOS

El Estado no se ha mantenido apartado de los cambios que se han suscitado en materia de comunicaciones y prueba de ello es la implementación de redes entre diferentes organismos y como producto de la globalización, la inclusión en Internet de algunos bancos de datos estatales.

Esta apertura y transparencia administrativa conlleva la responsabilidad del Estado por la seguridad de sus sistemas y por la protección de los datos. Con la aparición del tratamiento electrónico de la información y con el crecimiento masivo de las redes de interconexión, la dependencia de las organizaciones respecto de sistemas de seguridad se ha vuelto crítica y más, en el caso del Estado

donde están en juego cuestiones relativas a la seguridad nacional y a los derechos personalísimos de los ciudadanos.

Entonces, ¿cómo garantizar la confidencialidad y la disponibilidad de la información existente en el Estado? Sin lugar a dudas, parece imprescindible recurrir a métodos avanzados de cifrado o encriptado que atiendan al problema de la confidencialidad, o sea, acceso sólo al autorizado, a la autenticación que se refiere a la certeza del origen del mensaje y a la integridad o sea la posibilidad de modificar los datos o que la información transmitida sólo pueda ser modificada por personas autorizadas.

Si a la actividad administrativa no se le aplican las mejores tecnologías en materia de seguridad, si el Estado moderno no invierte en capacitación y auditorías de seguridad, no podrá asumir el nuevo rol que los avances en comunicación y el intercambio de información le deparan.

Asimismo, la apertura de los bancos de datos públicos han conducido al Estado a tomar recaudos para la protección de los mismos asumiendo una responsabilidad refleja por el hecho de sus agentes y receptando en algunos casos constitucionalmente, institutos como el habeas data presente en la mayoría de las legislaciones modernas.

CONCLUSIONES

La globalización, las innovaciones tecnológicas, el intercambio de información nos presenta un nuevo mundo, de cambios vertiginosos en el cual, como pensadores jurídicos debemos poner todo nuestro conocimiento y creatividad para vivir este desafío.

El Estado se ve inmerso en este torbellino de cambios con una estructura rígida, aún sacudida por los ecos de una reforma más aparente que real, con la cual debe enfrentar las funciones que le son indelegables y que hacen a su verdadera esencia.

La eficiencia, la transparencia, y la seguridad jurídica son el marco en el cual debe desarrollar su actividad y el cumplimiento de sus objetivos incorporando todos los avances tecnológicos sin descuidar las características propias de su actuar.

La modernidad que le impone un mundo globalizado y tecnificado le exige combinar un sistema económico liberal, una reforma racional de sus estructuras con una sociedad que le plantea como compromiso un retorno a un sistema político que permita el cumplimiento de objetivos sociales además de los económicos.

Banca Electrónica: Implicaciones Jurídicas de los Sistemas Electrónicos de Comunicación.

JOSÉ MARÍA ÁLVAREZ-CIENFUEGOS SUÁREZ

Magistrado-Jefe del Gabinete Técnico del Tribunal Supremo

La aparición y difusión de las nuevas tecnologías en la convivencia diaria de los ciudadanos hace que, en muchas ocasiones, los conceptos jurídicos tradicionales resulten poco idóneos para interpretar las nuevas realidades. Así, resulta que el jurista tradicional, formado en esquemas conceptuales no informáticos, encuentra verdaderas dificultades para adaptar la Ley y la jurisprudencia a los cambios tecnológicos.

Donde estos problemas son más intensos, como veremos, es en el campo de la prueba. Deberemos acostumbrarnos, como ocurrió en su día en el derecho mercantil, a los nuevos usos informáticos, como principios inspiradores de una nueva forma de concebir la contratación.

Los medios informáticos se nos presentan como instrumentos idóneos para la generación de actos y negocios jurídicos en masa; facilitando el intercambio de documentos mediante sistemas de comunicación electrónica. Sin embargo, existen grandes dificultades para acreditar la validez y autenticidad de un documento elaborado electrónicamente.

En este sentido, pocas épocas de nuestra historia han soportado una disociación más radical entre los avances tecnológicos y su consecuente proyección sobre la convivencia social por una parte, y por otra, los conceptos

jurídicos destinados a regularlos. Los Códigos Civiles y las leyes procesales, por lo que respecta a la prueba, siguen concibiendo sus preceptos pensando en el soporte tradicional, en el papel, la prueba documental, la prueba de peritos, por ejemplo, están pensadas para la escritura y la calificación tradicional.

Pongamos algunos ejemplos; mientras que en la vida diaria de nuestras ciudades un alto porcentaje -cada día mayor- de las transacciones económicas y comerciales se realizan por medios electrónicos, nuestros códigos civiles y nuestras leyes procesales desconocen la figura del negocio jurídico celebrado por medios informáticos y sus consecuencias jurídicas, fundamentalmente en el ámbito de la prueba.

Mientras que la dogmática tradicional ha elaborado durante siglos, el concepto de acto jurídico y las consecuencias que de él se derivan para la persona, los juristas modernos encuentran serias dificultades para delimitar los efectos de una voluntad consciente y libre proyectada sobre un programa informático.

La misma idea de documento, tradicionalmente unida a un soporte físico, como el papel o el cartón, encuentra dificultades para ser aplicada a los discos magnéticos y ópticos en los que, cada día con mayor intensidad, se almacenan los actos y negocios jurídicos.

Todas estas nuevas realidades nos ofrecen un panorama que, con acierto, la doctrina italiana ha calificado de nueva cultura informática.

Los juristas en general, y los jueces, los abogados y los profesores universitarios en particular, tienen que hacer un gran esfuerzo para adaptarse a estas nuevas realidades.

La informática asociada a la persona y a sus derechos, tanto personales como patrimoniales, se nos manifiesta como un fenómeno social de primera magnitud.

Ante el nacimiento de un mercado telemático europeo, acorde con el mercado único, el derecho y particularmente los juristas tendrán que conciliar, en lo que a la circulación de datos se refiere, aspectos tan diversos como el respeto a la vida privada, el acceso a los sistemas de información, los intereses generales de los Estados, los derechos de autor, su fiscalidad, todo lo que, en síntesis,

podríamos denominar estatuto jurídico europeo de los datos informatizados, su libre circulación y transmisión.

Surge así una nueva forma de entender «la circulación jurídica», en el marco del espacio judicial europeo que supera las fronteras nacionales, y que cada día demanda una mayor uniformidad de la documentación judicial, paso imprescindible para hacer efectivo el espacio judicial europeo.

Esta situación viene favorecida por el desarrollo de los programas EDI (Electronic Data Interchange), mediante los cuales se permite la transferencia de ordenador en ordenador de mensajes «estructurados». El EDI ofrece una mayor seguridad, rapidez y eficacia en el intercambio de mensajes, mediante la oportuna codificación de los documentos. Así se ha acreditado en el sistema bancario (Sistema Swift); en la industria automovilística (Proyecto Odette); electrónica (proyecto Edifice); química (proyecto Cefic); del seguro (proyecto Rinet) y transportes (proyecto Cost 306), entre otras. No es suficiente, con ser mucho, que existan redes, autopistas de la información, en el espacio jurídico europeo, es necesario y esto me parece fundamental desde el punto de vista de la seguridad jurídica, estructurar y codificar los mensajes para que el intercambio de información sea efectivo, establecer unas normas generales para estandarizar la información jurídica y ofrecer controles que permitan otorgar fiabilidad a los mensajes. La filosofía de la denominada banca telefónica está, a mi juicio, en ofrecer un alto grado de fiabilidad en los mensajes y, a la vez, en garantizar un adecuado control en el acceso al sistema.

En otro orden de cosas, la Comunidad Económica Europea, a través del programa TEDIS (Trade Electronic Data Interchange System), pretende armonizar las legislaciones de los Estados Miembros para facilitar el intercambio electrónico de documentos comerciales, siendo consciente, por otra parte, de la necesidad de cambiar unos sistemas jurídicos que fundan sus medios de prueba, muy especialmente, sobre la escritura. Por lo que respecta a nuestro país, la reciente Reunión Plenaria de Actividades EDI en Portugal, patrocinada por la CEOE, ha puesto de relieve la necesidad de intensificar la estandarización de los mensajes y la creación de un organismo de Certificación Nacional Electrónica.

Hoy día, puede decirse que ante la carencia de una regulación normativa adecuada, los empresarios europeos han asumido voluntariamente el valor probatorio de las transferencias y los negocios jurídicos concertados por medio del EDI. Ha nacido lo que para muchos podrá llamarse la facturación electrónica.

ALGUNOS EJEMPLOS:

Llama la atención el tremendo contraste entre la masiva aplicación de los sistemas electrónicos en la contratación empresarial y la carencia de normas para regular la prueba de estas operaciones.

Ya anticipo mi opinión, el Derecho y el trabajo de los juristas es, con frecuencia, una vuelta a los principios, en este caso, debemos recordar cómo se generalizó la validez y eficacia de instrumentos de pago como la letra de cambio, los pagarés y los cheques.

A) **Compraventa de títulos valores**.

Donde la innovación tecnológica, representada por los sistemas informáticos, ha encontrado una rápida y eficaz aplicación dentro del sector público ha sido en los mercados modernos de compraventa de títulos valores que hoy día están implantados en todo el mundo.

En España, el Real Decreto 505/1.987, de 3 de abril, creador del sistema de anotaciones en cuenta para la deuda del Estado, puso de relieve como el título valor, tal y como ha venido siendo concebido, supone un obstáculo para el tráfico mercantil, condicionado por la rapidez y la masificación de las operaciones.

Así, la propia exposición de motivos reconoce como la rapidez en el tratamiento de la información, la posibilidad de incorporar mecanismos que eviten o subsanen los errores cometidos, así como las facilidades de interconexión permiten el intercambio, a distancia, de cientos de miles de datos. Hoy día, el tratamiento informático permite la sustitución del viejo soporte documental del título valor tradicional, por simples referencias procesables en los ordenadores.

Por su parte, el nuevo Texto Refundido de la Ley General Presupuestaria, de 23 de Septiembre de 1988, establece, ya con carácter general y con el adecuado rango normativo, que: <<La Deuda Pública podrá estar representada en anotaciones en cuenta, títulos-valores o cualquier otro documento que formalmente la reconozca».

Surge así la Central de Anotaciones en el Banco de España en la que se toma constancia, mediante la oportuna anotación en cuenta, de las transacciones

efectuadas con la deuda del Estado. La Central de Anotaciones, auténtico servicio público del Estado, junto con las Entidades Gestoras, titulares de cuentas, se convierten en protagonistas de un nuevo sistema que ha revolucionado el mercado de la deuda pública, al modificar sustancialmente el concepto de título valor en su dimensión material.

Dicho resguardo, importante cuestión (reflejo de la incidencia tecnológica en el derecho), debe codificarse de manera que se garantice la correspondencia con los registros de la Entidad y con la información comunicada a la Central de Anotaciones.

La Ley reguladora del Mercado de Valores, Ley de 28 de julio de 1988, crea un mercado único e integrado mediante una interconexión informática que permita la inmediata compensación y liquidación de valores.

Su artículo 5, permite que los valores negociables puedan representarse por medio de anotaciones en cuenta o por medio de títulos tradicionales. Se potencia así la rapidez, la fiabilidad y el control de la información, la cual se convierte en un bien jurídico de primer orden en nuestra sociedad.

Los negocios jurídicos sobre valores representados por medio de anotaciones en cuenta tendrán lugar mediante transferencias contables, produciendo la inscripción de la transmisión a favor del adquirente (art. 9), los mismos efectos que la tradición de los títulos, siendo oponible a terceros.

Para la gestión de todo este nuevo mercado la ley prevé la constitución de una red informática, columna vertebral de un sistema de interconexión bursátil de ámbito estatal. Dicho sistema aparece administrado por una sociedad denominada Servicio de Compensación y Liquidación de Valores.

El Real Decreto 291/1992, de 27 de Marzo (R. 1992, 784), sobre emisiones y ofertas públicas de venta de valores, ha asignado a la Comisión Nacional del Mercado de Valores, por su disposición adicional quinta 1, el desempeño de las funciones en materia de codificación de valores negociables, configurándola como única entidad competente en esta materia.

En concreto, mediante la Circular 8 de Octubre de 1.992 se establece que la asignación por la Comisión Nacional del Mercado de Valores de los códigos correspondientes se contrae exclusivamente a los fines identificadores y de

normalización operativa que inspiran la función de codificación, sin que la asignación de esos atributos alfanuméricos por la Comisión Nacional del Mercado de Valores suponga pronunciamiento alguno sobre la regularidad del instrumento codificado, en lo que toca a su naturaleza, mecanismo de circulación, o legalidad de su emisión, en aquellos otros planos de verificación y registro que dicho Organismo tiene encomendados por la Ley 24/1988, de 28 de Julio del Mercado de Valores.

La transformación de los métodos operativos en el sector público y privado es ya irreversible. La reciente circular 13/1992, de 26 de junio, publicada en el B.O.E. de 11 de Julio de 1992, da un paso, a nuestro juicio definitivo, en la consolidación del Sistema Nacional de Compensación Electrónica: la circular 1/1990, de 2 de Febrero, establecía como sistema de comunicación para la liquidación del sistema general de cheques y pagarés de cuenta corriente el telefax y el fax.

Una forma eficaz de facilitar la futura prueba requiere, a mi juicio, intensificar los controles y requisitos en el acceso a la circulación electrónica, ofrecer garantías, dar seguridad inicial a los sistemas. Como ejemplo, estos últimos días la prensa de Madrid anunciaba que la Bolsa, en una sola sesión, había realizado más transacciones que en todo el año 1983. Yo diría que la futura prueba se facilita con la credibilidad de los sistemas.

Pues bien, a partir de esta nueva Circular las comunicaciones entre las Entidades asociadas y el servicio de liquidación del Banco de España, se efectuará, como sistema ordinario, a través de un proceso automatizado que permitirá el diálogo directo entre el Centro de Procesos del Banco de España y los Centros de las Entidades participantes en el Sistema Nacional de Liquidación.

De esta forma, la constatación de las liquidaciones interbancarias se incorpora totalmente a sistemas informatizados. La prueba misma del incumplimiento de una obligación derivada de una relación jurídica mercantil, concertada por los medios tradicionales, se condiciona a la existencia de un diálogo electrónico entre una Entidad Bancaria asociada y el Centro de Procesos del Banco de España, en donde, con plena eficacia solutoria, quedan anotadas informáticamente miles de operaciones cada día.

La creación de centros oficiales y privados que controlen la circulación electrónica, el nacimiento de notarías electrónicas, facilitará la credibilidad de las

condiciones en que se desarrolla el envío de los mensajes. Ante la falta de la percepción material del mensaje mismo, debe reforzarse el control sobre los sistemas de transmisión y recepción.

Este fenómeno que, sin duda, constituye un paso decisivo en la consolidación de los medios electrónicos de prueba, culmina con una declaración impensable hace sólo unos pocos años: A partir de ahora, el fax y los terminales telex, último reducto en el que aparecía el papel como soporte físico de la liquidación de una obligación, solo podrán ser utilizados, con carácter extraordinario, cuando el Centro de Procesos de Datos del Banco de España o de alguna de las Entidades asociadas no puedan utilizar el sistema ordinario que es, ya, desde hoy, la comunicación electrónica.

Como fruto de esta progresión conceptual en el reconocimiento y circulación de los documentos elaborados por medios electrónicos, la circular de 8 de Octubre de 1992 de la Comisión Nacional de Valores, establece un sistema de Codificación de los valores negociables (acciones de Sociedades Anónimas, obligaciones, participación en fondos de inversión, pagarés, etc.), con objeto de normalizar su operatividad en un mercado dominado por las transacciones electrónicas.

Advirtiéndose, sin embargo, por la circular que la asignación de esos atributos alfanuméricos, no supone pronunciamiento alguno sobre la regularidad del instrumento codificado, en lo que toca a su naturaleza, mecanismo de circulación o legalidad de su emisión. En este sentido, la aprobación de nuevas Directivas comunitarias, encaminadas a liberalizar y hacer más flexibles los mercados financieros europeos, va a obligar a nuevas reformas legislativas encaminadas a permitir la intervención en los mercados españoles de agentes financieros de otros países comunitarios. Todo ello conllevará, como no puede ser menos, un nuevo esfuerzo de codificación e identificación electrónica en un mercado de valores cada vez más dependiente de la tecnología.

A mi juicio, un mayor control de los mecanismos de creación e introducción de los mensajes en el sistema electrónico, permitirá una mayor flexibilidad y agilidad de las operaciones. En mi opinión, se puede garantizar, ante todo, el sistema, en sí, más que la transmisión individual, en su pura singularidad.

B) **La modernización de los Registros y del Notariado.**

La documentación y posterior circulación de los actos jurídicos por sistemas informáticos ha penetrado con fuerza en núcleos esenciales del ordenamiento jurídico privado. En concreto, el derecho notarial y los registros de la Propiedad se ven favorecidos por los sistemas informáticos. Así, la Reforma del Reglamento Notarial, operada por el Real Decreto 1368/1992, de 13 de Noviembre de 1992, ha previsto (véase el artículo 4 del Anexo al citado Reglamento), que el Registro General de Actos de Ultima Voluntad se lleve por procedimientos informáticos.

En consecuencia, la información que los Colegios Notariales deben remitir periódicamente al Registro General se enviará en soportes informáticos, para, en su momento, dar paso al sistema de comunicación telemática (Orden del Ministerio de Justicia de 4 de Diciembre de 1992).

En desarrollo de esta normativa, la Dirección General de Registros y Notariado, por resolución -Circular de 31 de Marzo de 1993, ha aprobado las instrucciones necesarias para el envío de los partes testamentarios y los partes de iniciación de las actas notariales de declaración de herederos ab-intestato.

Con ello, al utilizarse el soporte informático, se sustituye el tradicional envío de la información mediante tarjetas escritas.

Se establecen reglas de elaboración de la información para facilitar su tratamiento informático: se configura el número de identificación del Notario o Fedatario autorizante como el elemento básico para el sistema informático y, a la vez, se fijan las características de los soportes magnéticos y del sistema operativo, dándose instrucciones precisas respecto a la forma en que han de estructurarse los datos. Todo ello en garantía de la perfecta compatibilidad y comunicación de los sistemas informáticos.

Siguiendo la línea de informatización progresiva de los Registros y las Notarías, asistimos a una nueva reforma de los Reglamentos Notarial e Hipotecario, originada por el Real Decreto 2.537/1994, de 29 de Diciembre.

El nuevo artículo 175 del Reglamento Notarial impone al notario que antes de autorizar una escritura de adquisición de bienes inmuebles o de

constitución de un derecho real sobre ellos, deberá solicitar al Registro de la Propiedad correspondiente la información adecuada, pudiendo utilizarse para ello el telefax. Se impone, ya con plena vigencia la interconexión electrónica entre los Notarios y el registro de la Propiedad.

Asimismo, el nuevo artículo 249 del citado Reglamento autoriza al Notario para remitir por telefax al Registro de la Propiedad la comunicación relativa a la autorización de escritura susceptible de ser inscrita, que dará lugar al correspondiente asiento de presentación.

Por su parte, el nuevo artículo 354 del Reglamento Hipotecario permite al Registrador remitir su información respecto a la titularidad, cargas, gravámenes y limitaciones de fincas registrales, cuando sean solicitadas por las Notarías, por medio de telefax.

La Disposición Adicional Única del Real Decreto de 29 de diciembre de 1994 impone, a nuestro juicio una obligación de excepcional transcendencia: en el plazo de un año, la obligación de informatizar el Diario de todos los registros de la Propiedad de España.

La reciente instrucción de 29 de octubre de 1996, de la Dirección General de los registros y del Notariado prevé la intercomunicación entre todos los Registros de la Propiedad, permitiendo que la publicidad registral se desarrolle a través de sistemas informáticos, como parece reconocer el art. 12 del nuevo Reglamento del Registro Mercantil, aprobado el 19 de julio de 1996. En el art. 23 del citado Reglamento se establece que los libros del registro de la Propiedad puedan elaborarse por medios informáticos. La Instrucción de 1996 requiere que el 31 de diciembre de 1998 estén incorporados a los índices informatizados de los registradores todos los datos necesarios de las fincas con asientos posteriores a 1950.

El art. 10 reconoce, igualmente, que los registros de la Propiedad puedan comunicarse directamente por vía telemática, utilizando el correo electrónico para recibir información de las fincas registradas.

Por último y por lo que se refiere a los órganos judiciales, éstos podrán enviar por telefax al registro de la Propiedad competente, las resoluciones judiciales que puedan causar asiento registral, el día de su firma o en el siguiente hábil.

Recientemente, como ya hemos visto, se han producido en nuestro ordenamiento jurídico privado reformas de especial significación; nos estamos refiriendo a la modificación operada en la configuración material y organización de los Registros de la Propiedad: el Real Decreto de 30 de Marzo de 1.990 modifica el Reglamento Hipotecario de cara a una informatización integral de los Registros de la Propiedad.

En este sentido, la reforma prevé la creación de un Indice General Informatizado de las fincas y derechos inscritos, para lo cual, el Colegio Nacional de Registradores de la Propiedad remitirá periódicamente al Centro de Gestión Catastral y Cooperación Tributaria, en soportes magnéticos, la información relativa a las transmisiones inscritas (art. 398. c).

Por su parte, el ya citado art. 418.b permite utilizar la telescopia o procedimiento similar para remitir al Registro competente los datos necesarios para efectuar el oportuno asiento de presentación.

C) Cambios en los procedimientos administrativos.

En el campo del derecho público, la Ley de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, Ley 30/92, de 26 de noviembre, ha reconocido plenamente respecto de los actos de la Administración, su posibilidad de manifestarse y documentarse por medios informáticos, teniendo, a todos los efectos, valor probatorio, debe recordarse al respecto el art. 45 de la citada Ley.

Por su parte, el nuevo artículo 230 de la Ley Orgánica del Poder Judicial, además de reconocer la validez de los documentos emitidos por medios electrónicos, informáticos y telemáticos, siempre que se garantice su autenticidad e integridad, permite en su apartado nº 4 que las personas que demanden la tutela judicial de sus derechos e intereses puedan relacionarse con la Administración de Justicia a través de dichos medios técnicos, siempre que éstos sean compatibles con los equipos de que dispongan los Juzgados y Tribunales.

Recientemente el Ministerio de Justicia ha aprobado una Orden Ministerial (30 de noviembre de 1.995, B.O.E. de 21 de diciembre) por la que dispone la informatización del Registro Civil de Murcia.

Y, más recientemente, la Orden de 22 de Marzo de 1996, por la que se desarrolla el artículo 88 de la Ley 37/1992, del Impuesto sobre el Valor Añadido y el artículo 9 bis del Decreto 2.402/1985, de 18 de Diciembre, desarrollan el sistema de facturación telemática en el Impuesto del Valor Añadido. A partir de ahora, las facturas en soporte papel son sustituidos por facturas electrónicas que deberán conservarse en soportes magnéticos u ópticos.

Así se define la factura electrónica: Se entenderá por factura electrónica «un conjunto de registros lógicos, almacenados en soportes susceptibles de ser leídos por equipos electrónicos de procesamiento de datos, que documentan las operaciones empresariales o profesionales, con los requisitos exigidos en el Real Decreto 2. 402/1985, de 18 de Diciembre. En las líneas de las facturas electrónicas, que en todo caso deberán respetar los mencionados requisitos, podrán sustituirse las descripciones de los bienes o servicios que constituyan el objeto de las operaciones facturadas por sus correspondientes códigos estables.

Se entiende por códigos estables aquellos códigos alfanuméricos que identifican de forma única e inequívoca, entre otros, los bienes, servicios, lugares, personas, etcétera, cuya información se transmite a través de un sistema de intercambio de facturación por medios telemáticos y que tienen un carácter de permanencia en su aplicación, y con idéntico significado para cualquier usuario del sistema. Las listas de códigos estables y la descripción de los mismos deberán constar en tablas históricas que puedan ser utilizadas automáticamente por los programas de los usuarios para el tratamiento de los ficheros producidos».

Surge así una nueva metodología en el tratamiento de los fenómenos jurídicos, la transmisión electrónica de declaraciones de voluntad que generan derechos y obligaciones para los partícipes en el «diálogo informático» está provocando un cambio terminológico, a mi juicio inevitable, en los conceptos jurídicos tradicionales. ¿Cómo interpretar, hoy día, nuestro Código Civil cuando impone al vendedor la obligación de «entregar la cosa al comprador».?

Por último la Disposición Adicional de la citada Orden establece que: ..Los empresarios, profesionales o sus agrupaciones que lleven por medios informáticos sus libros, facturación o registros fiscalmente exigibles, deberán conservar en soporte magnético u óptico, durante el período de prescripción, además, los ficheros y documentos siguientes:

a) Ficheros de datos, tanto históricos, como maestros generados por sus aplicaciones informáticas y de los que se deriven los libros a diligenciar.

b) Ficheros de los programas fuentes, con los cuales se procesan los ficheros de datos anteriores.

c) Todos aquellos ficheros, programas y documentación necesarios que permitan la reconstrucción total del camino de auditoría informática del sistema de información del contribuyente u obligado tributario».

Es de resaltar, por lo que afecta a la realidad jurídica de nuestro país, la voluntad decidida de las Instituciones Comunitarias de superar los obstáculos que suponen las lagunas existentes en la normalización de los mensajes, la interoperatividad de las redes telemáticas, la validez jurídica y la seguridad informática de la información transmitida por medios electrónicos.

D) Nacimiento de nuevos contratos: Generalización del uso de los sistemas electrónicos.

Estamos asistiendo, quiérase o no, al ocaso de la civilización del papel, de la firma manuscrita y del monopolio de la escritura sobre la realidad documental. Aparece, cada día con más fuerza, una nueva forma de concertar y garantizar la identidad de la voluntad generadora de los negocios jurídicos, reveladora de una nueva concepción del documento jurídico, asistimos, en muchos casos sin prestarle la necesaria atención, al nacimiento de nuevas formas de documentar los actos y negocios jurídicos.

El análisis de la realidad que acabamos de describir nos permite afirmar que el proceso informático, por el que se crean modifican y extinguen relaciones jurídicas, es un proceso «creíble y probable». El jurista no puede desconocer la realidad social, en palabras del profesor Hernández Gil, el derecho, como el lenguaje, es un producto de la cultura y un sistema de comunicación entre los seres humanos.

La Unión Europea, con exquisita sensibilidad hacia los avances tecnológicos, ha insistido en alguna de las últimas reuniones del Consejo Europeo en la necesidad de abordar la creación de redes transeuropeas de datos comerciales e industriales.

En concreto, desde 1988 se han venido desarrollando programas de Intercambio Electrónico de Datos en sectores tan importantes como: la fabricación de automóviles, la industria química, la industria electrónica e informática, los reaseguros y los transportes, siendo, en estas experiencias, la organización bancaria una de los que, sin duda, han contribuido de una manera decisiva a estos cambios tan profundos en la concertación de negocios jurídicos.

No se nos ocultan los problemas jurídicos que entraña este diálogo «sin papel»; es necesario, por tanto, superar los obstáculos legales que exigen la presentación del soporte escrito para dar por válida una obligación. La desaparición física de documentos básicos para el derecho mercantil, tales como los conocimientos de embarque, las cartas de crédito y el nacimiento de «notarías electrónicas» plantean problemas jurídicos de gran alcance que no se pueden ignorar.

La seguridad e integridad de los mensajes cursados por medios electrónicos ofrecen, no puede ocultarse, dificultades operativas en lo que respecta a la recepción y confidencialidad del mensaje.

Sin embargo, todo este panorama no es sólo un <<futurible>> deseado, se trata más bien de una realidad inminente que se nos aproxima impulsada por la voluntad decidida de la libertad de mercado. La lectura de los documentos y trabajos de las Comisiones comunitarias vaticinan la llegada de un día, no muy lejano, en que, como presupuesto necesario para operar comercialmente en el marco de la comunidad, se nos impongan cambios normativos en nuestro ordenamiento que, hoy por hoy, nos parecen impensables.

Como pone de relieve la doctrina mayoritaria la Comunidad Económica Europea ha potenciado el desarrollo de la transmisión electrónica de datos (programas EDI), facilitando la celebración de contratos tipo entre pequeñas y medianas empresas con el consiguiente logro de una normalización y homogeneización de los documentos a transmitir.

Los usuarios del EDI, a través de acuerdos y convenios particulares, llegan a aceptar el valor probatorio de los mensajes enviados por sistemas electrónicos, dándose al mensaje electrónico normalizado el mismo valor que al documento escrito y firmado.

Nos encontramos, por tanto, ante un auténtico sistema internacional de circulación electrónica de valores que ha sabido salvaguardar las características más esenciales que la legislación mercantil asigna a los títulos valores.

Esta nueva expresión simbólica que permite la circulación electrónica de los valores mercantiles, a la vez que provoca el abandono de la «materialidad» de los títulos valores, paradójicamente, les vuelve a dotar de una nueva forma de significación: la informática. El ordenador y los ficheros que en él se almacenan constituyen hoy día una nueva forma de entender la materialidad de los valores. Para el lenguaje electrónico la «dimensión formal de los valores» es tan evidente, bajo su lectura codificada, como hace cien años para un banquero tradicional lo era el depósito de las acciones.

II.- LA BANCA TELEFÓNICA

Lo primero que deberíamos matizar, a la vista de lo ya expuesto, es una crítica a la expresión «banca telefónica»; para mí conceptual y técnicamente esta expresión resulta hoy día superada por las nuevas realidades.

Por banca telefónica no debemos entender la simple contratación por teléfono, la simple sustitución del papel por la voz enviada a través de la línea telefónica.

¿Qué se esconde detrás de la expresión «banca telefónica» ?, a mi juicio todo un nuevo sistema de contratación que desplazando el soporte papel y la escritura tradicional como únicas realidades documentales y expresiones simbólicas capaces de acreditar una manifestación de voluntad, utiliza los sistemas informáticos y las comunicaciones electrónicas como nuevos vehículos para manifestar y transmitir una declaración de voluntad dirigida a celebrar un determinado negocio jurídico.

En este sentido y con las necesarias matizaciones, podríamos definir la BANCA TELEFONICA como un convenio o acuerdo entre una entidad de crédito y sus clientes, mediante el cual y en base a una especialísima relación de confianza, ambas partes asumen las consecuencias jurídicas de las operaciones celebradas mediante órdenes verbales -a través del teléfono- siempre que se respeten los compromisos de diligencia y confidencialidad previamente pactados.

No se trata, a mi juicio, del único contrato, es, más bien, una nueva forma de operar entre la Entidad de Crédito y el usuario que, como veremos, puede a través de múltiples ..<<productos>> desde la apertura de una cuenta corriente, requisito imprescindible y básico para la banca telefónica, hasta la contratación de una tarjeta de crédito, transferencias bancarias, imposiciones a plazo fijo, contratación de fondos de inversión, planes de pensiones, adquisición de deuda pública, letras del Tesoro, ordenes de compraventa de acciones o de otros títulos admitidos a cotización.

El contrato celebrado entre la entidad de Crédito y el cliente, en el que, es de una especial relevancia el respeto al principio de buena fe pueden, establecerse las siguientes características derivadas de la aplicación de los arts. 1255, 1258 y 1274 del Código Civil.

•La necesaria apertura de una cuenta corriente como base de todas las futuras operaciones, sirve para precisar todos los datos indicativos que individualizan al cliente.

•Reconocimiento del teléfono como vía de comunicación «ordinaria» entre la entidad bancaria y el cliente.

•La confidencialidad como contenido esencial de todas las operaciones. Ello impone en el usuario un deber positivo de sigilo, debiendo asumir las consecuencias jurídicas perjudiciales de su quebrantamiento.

•En cada una de las operaciones, la firma, expresión formal del consentimiento, es sustituida por unos signos y claves de identificación, sólo conocidos por el usuario y cuya utilización vincula su voluntad.

•Importancia de los trámites de identificación antes de iniciar una operación concreta. Las claves secretas correctamente utilizadas vinculan al usuario y al banco que no tendrá que realizar comprobaciones posteriores complementarias.

•La fiabilidad del sistema descansa, como se ha dicho, en un estricto control y seguridad en el proceso de identificación. Existe un compromiso positivo del cliente con la entidad bancaria. Existe un pacto de sigilo y discreción cuyo quebranto perjudicará al infractor, hasta el punto de que el uso de las claves

secretas por personas extrañas para realizar operaciones provocará efectos jurídicos en la persona del cliente.

•Especial deber de diligencia, denunciando la pérdida o sustracción de las claves secretas. No existe, en principio, exoneración de responsabilidad para el cliente. Será necesario, en su día, atender a la jurisprudencia de los Tribunales y a la doctrina del servicio de reclamaciones del Banco de España, respecto de lo que se entiende, en estos casos, por buena práctica bancaria.

•Si bien la voluntad negocial se transmite por el teléfono, manifestando una voluntad concreta, las claves secretas, como nueva forma de expresión simbólica que incorporan indicios suficientes de individualización e identificación, sustituyen y reemplazan, con éxito, a la firma tradicional.

•La entidad de crédito se compromete a conservar durante ó años las conversaciones grabadas, como medio de prueba de las órdenes recibidas del cliente. También se prevé la posibilidad de que éste solicite copia en papel o en cinta de las conversaciones mantenidas con la banca telefónica.

•Para mayor seguridad, las operaciones que implican salidas de fondos de la cuenta del cliente requieren, como garantía añadida, el uso de determinadas posiciones de la clave secreta que, como decíamos, solo es conocida por el cliente.

Esta mayor reflexión, derivada de un uso todavía más singular y específico de las claves secretas, hace que la consciencia de la voluntad sobre la operación realizada quede todavía más de manifiesto.

•La equivocación o el error en el uso de la clave secreta supone una pérdida de las señas de identidad, provocadora, de forma automática, el bloqueo de dichas claves y la paralización de todas las operaciones. Se pretende con ello evitar errores o intentos de suplantar la personalidad de un determinado cliente. Será, necesario, para volver a operar, la entrega de nuevas claves secretas.

•Especial deber de colaboración y diligencia del cliente para con la entidad. Se aprecia en la asunción de su responsabilidad patrimonial por pérdida o acceso indebido de terceros.

•La contratación por medios electrónicos en general, provoca la necesidad en las entidades de crédito de disponer de ficheros informatizados con

numerosos datos sensibles referentes a las señas de identidad de sus clientes. Surge así una delicada e intensa obligación de custodia. La entidad de crédito sólo podrá utilizar esos datos personales, de acuerdo con las previsiones y garantías establecidas en la Ley 5/92, de Protección de Datos, para los fines propios del contrato, no siendo, a mi juicio, ceder esos datos a terceros sin consentimiento expreso del cliente.

•El cliente, como reconoce la Ley 5/92, tiene derecho de acceso, rectificación y cancelación de los datos personales almacenados en ficheros informáticos utilizados en el contrato de " Banca telefónica ".

•Desde el punto de vista operativo el servicio de banca telefónica permite realizar operaciones desde cualquier punto, durante las 24 horas y a lo largo de los 365 días del año, sin necesidad de desplazarse físicamente hasta una sucursal de la entidad de crédito, excepto cuando sea necesario, por razón de la operación, que intervengan un Corredor de Comercio o un Notario.

•Como obligación básica de la entidad de crédito debe resaltarse la "fiabilidad informática", esto es, el compromiso de disponer de los recursos tecnológicos suficientes para hacer efectivas las operaciones del cliente.

Respecto de los posibles problemas interpretativos que plantee el uso de la Banca telefónica, dado que hoy día es un producto de reciente implantación y ofrecido a clientes selectivos, será necesario esperar a las soluciones que ofrecen tanto los Tribunales como el Servicio jurídico del Banco de España.

Las posibles discrepancias entre los usuarios y las entidades de crédito se centrarán, a mi juicio, en las cuestiones referentes a la falta de diligencia, buen uso de la documentación e información, al posible quebranto del secreto y confidencialidad, así como a las consecuencias del eventual uso fraudulento.

Hoy día, en los diversos productos que bajo la denominación genérica de «Banca telefónica» ofrecen las diferentes entidades de crédito, no se establecen sistemas de limitación de responsabilidad como ocurre en los contratos de uso de tarjetas de crédito. Así, tanto el Código de Buena Conducta del Sector Bancario Europeo de 14 de noviembre de 1990, relativo a los sistemas de pago mediante tarjetas de crédito, como la Recomendación de la Comisión Europea (n° 88/590 CEE, de 17de noviembre de 1988), limitan la responsabilidad a 150 ecus, salvo

que el usuario hubiera actuado de forma fraudulenta, a sabiendas o con negligencia grave, quebrantando el secreto, etc.

La Banca Telefónica se nos presenta, hoy día, como un antecedente de una nueva forma de gestionarse los servicios bancarios. Ya asistimos al nacimiento de una auténtica Banca Electrónica y de sistemas multibancos, las empresas, mediante conexiones electrónicas, obtienen productos a medida que les permite optimizar el rendimiento de sus departamentos financieros.

Así la conexión electrónica multibanco les permite controlar la gestión de tesorería, integrar automáticamente los estractos de cuenta y los ficheros de contabilidad. Mediante estas técnicas, las empresas obtienen un gran ahorro de tiempo y mayores garantías de seguridad en la obtención de datos.

De esta forma, el cliente puede realizar, electrónicamente, las mismas consultas y operaciones que realizaría en la sucursal, siendo posible la transmisión y recepción de ficheros, incluyendo el envío electrónico de remesas de efectos, el abono directo de las nóminas, los pagos a proveedores, las transferencias masivas a clientes y los anticipos de créditos a la exportación.

Como producto añadido a todas estas novedades, las empresas logran una mejoría notable en el capítulo de la toma de decisiones. Asistimos, por tanto, a una revolución en el negocio de la prestación de servicios bancarios. Está muy próximo el día en que las entidades de crédito, sobre la filosofía de la banca electrónica, ofrezcan productos «a medida», según las necesidades y características de las empresas.

III.- TRANSFERENCIAS ELECTRÓNICAS Y MEDIOS DE PRUEBA

La incorporación de todas estas realidades al mundo del derecho plantea problemas de especial transcendencia. En este orden de cosas, uno de los puntos críticos pasa por el valor jurídico atribuido a los actos y negocios jurídicos incorporados a soportes informáticos (discos magnéticos y ópticos).

Los medios de prueba tradicionales reconocidos en el derecho español (arts. 1.215 del Código Civil, 47 del Código de Comercio y 578 de la Ley de Enjuiciamiento Civil), y en especial la prueba de documentos -tradicionalmente unida al soporte papel y a la escritura incorporada-, se revelan insuficientes para

explicar las nuevas operaciones y negocios celebrados con la colaboración de soportes informáticos.

Vemos como, hoy día, la informática invade el mundo del derecho, transformando sus pautas de conducta y sus modos operativos.

La llegada del lenguaje electrónico, obtenido por intermediación de una máquina, nos hace arribar a un nuevo concepto del documento; el documento electrónico, el cual se encuentra cada día más cerca del calificativo de documento jurídico.

De ello ya existen múltiples ejemplos en nuestro ordenamiento (véanse los arts. 49 de la Ley del Patrimonio Histórico Artístico de 1985, el art. 1.429 n° 7 de la Ley de Enjuiciamiento Civil y el art. 26 del nuevo Código Penal).

En todo instrumento probatorio hay que distinguir entre la materialidad del soporte (al que se incorpora una manifestación de voluntad o la expresión de un simple hecho) y el contenido del mismo. Por ello, podemos afirmar que el concepto de documento -tanto público como privado- que hoy recogen nuestras leyes se identifica más que con el documento en sí, con las manifestaciones históricas del mismo. En concreto, con el papel y la autografía como única manifestación de la expresión simbólica.

Claro ejemplo de este condicionamiento histórico del concepto de documento son las expresiones utilizadas por el derecho romano clásico: epístula, codex, scriptura y en sentido más genérico tabula e instrumentum.

Nuestro derecho tradicional, por influencia del romano, desconoce, hasta fechas muy recientes, la voz documento. Así, las Partidas utilizan exclusivamente la voz «escritura», definiéndola como toda carta que es hecha por mano de escribano público de Consejo, o sellada con sello del Rey (Partida 3ª, Título XVIII, Ley I). En el mismo texto, al examinar los diversos tipos de escritura los equipara con el término cartas.

Nuestro diccionario de Autoridades, publicado en 1739, desconoce la acepción jurídica de la palabra documento. Por influencia del derecho clásico, recoge la voz «instrumento» que, en una de sus acepciones, se identifica con la escritura u otro papel que sirva para justificar alguna cosa o certificarla.

Para Carnelutti, el medio de la representación documental puede ser, en el estado actual de la técnica, verbal o figurativo; una especie, pero no la única del documento verbal es la escritura, al lado de la cual se coloca hoy el documento fonográfico; una especie, pero no la única del documento figurativo es la fotografía, junto a la cual está el documento figurativo indirecto (el dibujo, la pintura, etc.).

En el informe Nora-Minc, elaborado bajo la iniciativa del Presidente Francés en 1978, ya se indicaba que la telemática supone un cambio profundo en la dimensión y naturaleza de los archivos tradicionales. Para el informe francés, la constitución de bancos de datos informatizados va a originar una rápida reestructuración de los conocimientos humanos, con arreglo a esquemas hoy difíciles de establecer.

Francisco de Santis, recordando la opinión de Carnelutti, según la cual la teoría del documento está dominada por la idea de paternidad del texto escrito, defiende la posible existencia de documentos públicos o privados -según las circunstancias- confeccionados a impulsos de una computadora, siempre que contenga el texto íntegro y éste aparezca autenticado por una firma o contraseña electrónica.

Para Francesco Parisi, en el contrato celebrado mediante un ordenador la firma electrónica vendría a sustituir a la autógrafa con la única diferencia del soporte electrónico en lugar del papel.

Ettore Giannantonio, al pronunciarse sobre el valor jurídico del documento electrónico, advierte que no es difícil prever cómo en un breve período de tiempo, toda la actividad de documentación será desarrollada, salvo casos excepcionales, de forma automatizada, con las consecuencias de que el «documento manual», el documento redactado por formas tradicionales, será sustituido casi completamente por el <<documento electrónico>>.

La fiabilidad del contenido de los documentos generados y enviados por sistemas electrónicos esta condicionada, como en todo caso de discrepancia o controversia jurídica, a lograr el convencimiento psicológico del Juez que ha de valorar las pruebas presentadas bajo las reglas de la sana crítica y de la lógica.

Volviendo a los principios, entiendo que es de excepcional importancia para dotar de «credibilidad ante los Tribunales» a este tipo de mensajes

electrónicos recordar las reglas generales del derecho que han sido el motor de todo el desarrollo normativo en el mundo de las empresas. Principios como el de «contabilidad ordenada», la «buena fe en la contratación», la conducta de un <<comerciante lea>>, unidos a las garantías y controles sobre el funcionamiento y acceso a los sistemas electrónicos de elaboración y transmisión de información, pueden, en un momento concreto, llevar al convencimiento del Juez de la validez y eficacia de una operación comercial celebrada por sistemas electrónicos.

Enzo Meriggiola, haciendo una síntesis del valor probatorio de los documentos electrónicos en los distintos países de la C.E.E., recuerda como ya el Consejo de Europa en 1981 había elaborado una recomendación en la que invitaba a los Estados miembros a revisar el valor privilegiado que se otorgaba a la prueba escrita, en sentido convencional, en detrimento de la prueba no escrita, estableciéndose reglas comunes respecto de los registros informáticos.

Asimismo, la jurisprudencia viene aceptando su admisión en los asuntos sobre negocios, dejando a salvo la facultad del juez de valorar, según su prudente arbitrio la prueba, valiéndose, incluso de la inspección de las fuentes de la información y de la ayuda de un experto.

En líneas generales, aplicables a nuestro ordenamiento, el principio de la libre convicción del Juez en la valoración de la prueba ha de permitir la utilización de documentos electrónicos, ya sea en el proceso civil, penal o contencioso administrativo.

Por lo que respecta a nuestro ordenamiento, habrá que partir, con carácter previo, de la superación de los medios de prueba convencionales; efectivamente, tanto el art. 1215 del Código Civil, como el art. 578 de la Ley de Enjuiciamiento Civil contienen una enumeración de medios de prueba que hoy día, a la vista de los adelantos tecnológicos, no pueden conceptuarse como exhaustivos.

El documento, como objeto corporal que refleja una realidad fáctica con transcendencia jurídica, no puede identificarse ni con el papel, como soporte, ni con la escritura, como unidad de significación.

Para el Magistrado Jaime Rouanet, puede admitirse pacíficamente que la «electrónica» puede ser considerada como escritura, a todos los efectos, y que, por tanto, el documento electrónico pertenece a la categoría de los documentos en

sentido jurídico. La diferencia con el documento escrito tradicional está en el hecho de que la información memorizada sobre soportes informáticos no es inmediatamente comprensible por el hombre y requiere la intermediación y, en cierto modo, la traducción de la máquina.

El profesor de la Universidad de Roma, Luigi Montesano, entiende que el resultado de una operación informática puede ser conceptuado como prueba documental no escrita, pues resulta subsumible en las «representaciones mecánicas» previstas en el art. 2712 del Código Civil italiano.

El documento se nos representa como una materialidad a la que se incorpora una idea, es una cosa, un acontecimiento, un indicio que atestigua, comprueba, ofrece un testimonio de un hecho; más concretamente, es un objeto simbólico, una porción de la realidad material destinada a expresar, a través de signos externos, un significado específico y determinado.

La llegada de operaciones como las aquí descritas, el nacimiento de la «banca electrónica» va a suponer para los juristas un indudable reto en el que, como en todos los momentos de cambio, es aconsejable volver a los principios.

Microsoft



JUNTA DE EXTREMADURA

FEDERACIÓN IBEROAMERICANA
DE ASOCIACIONES DE DERECHO
E INFORMÁTICA