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.