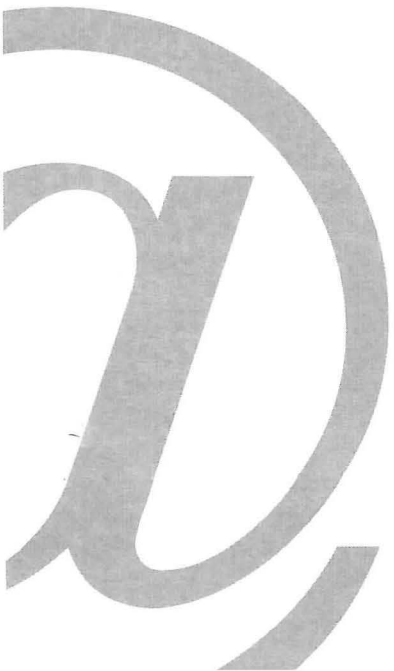

Internet. Responsabilidad civil y penal. Legislación

FRANCISCO JAVIER MONTERO JUANES

INTERNET. RESPONSABILIDAD CIVIL Y PENAL. LEGISLACIÓN.

I. INTRODUCCIÓN

El ministerio fiscal es una institución estatal y constitucional que defiende los intereses de la ley y de la sociedad ante los tribunales de justicia, es el representante del Ius Puniendi del Estado, interviene decisivamente en todo tipo de procesos en persecución de la satisfacción de los derechos e intereses sociales y públicos tutelados y amparados por la ley. Puede afirmarse en que el ministerio fiscal debe ser y es el cordón umbilical entre la sociedad que intenta y debe representar y los tribunales de justicia. Por ello la presencia continua del fiscal en foros de debate propiciados por acontecimientos sociales de actualidad, debe ser puesto en conexión con esa vocación del fiscal de servicio público. Me produce una íntima satisfacción el hecho de que en estas jornadas hayan participado dos fiscales, lo que pone de manifiesto a importancia que el ministerio fiscal como institución, y todo ello con independencia de las personas físicas que lo encarnamos, da a cualquier fenómeno social que se produzca en nuestros días. El ministerio fiscal no es un órgano muerto y ajeno a las transformaciones sociales, muy por el contrario, es un órgano vivo y sensible a las demandas sociales y a la propia evolución de la sociedad. Nadie puede vivir ajeno a la realidad, al entorno que le rodea. Las transformaciones sociales deben de llevar aparejada necesariamente la transformación de sus instituciones más representativas, y por ello, la del propio Ministerio Fiscal.

La ponencia que hoy me corresponde desarrollar se refiere a las responsabilidades penales y civiles que se pueden derivar del uso de las nuevas tecnologías, y particularmente de internet, así como la legislación aplicable al respecto. Sin duda es una materia apasionante, poco elaborada en la actualidad y que tiene un indudable interés, pues esta actividad, está produciendo constantemente innumerables polémicas jurídicas que causan una honda preocupación en todos los

estamentos implicados: sociedad, internautas, informáticos, legisladores, politicos, juristas, empresas informáticas, titulares de derechos de autor o industriales, etc. sin que en la mayor parte de los casos haya ni siquiera principios de acuerdo en torno a las soluciones o criterios a adoptar.

La informática en general, e Internet en particular, además de fenómenos con facetas políticas, jurídicas, económicas, informativas, industriales, son hoy por hoy verdaderos fenómenos sociales, que están suponiendo a nivel global (sobre todo en los países civilizados) una verdadera transformación de usos y costumbres, de conductas y actitudes, de tal entidad, que muy probablemente hará que en pocos años se produzca– si es que no se ha producido ya -lo que se viene denominando desde hace tiempo como una verdadera revolución tecnológica, de comunicación e información, comparable a lo que en su día significaron la revolución industrial en el siglo XIX o la televisión y el telefóno en el siglo XX.

Para hacernos una idea aproximada de lo que ha significado la revolución de la informática y de Internet en el final del siglo XX,y de que esa evolución estaba fuera de todo cálculo racional, recordaremos diversas frases emanadas de genios de la informática, que ponen de manifiesto el como la evolución de la informática ha superado la propia imaginación del hombre. Así, Bill Gates señalaba en 1981 que 640.000 bites de memoria eran suficientes para todo el mundo, Tomas Watson, presidente de IBM auguraba en 1943 que en el mundo existía mercado para 5 ordenadores, o Ken Olson, afamado informático, afirmaba tajantemente en 1983 que no había ninguna razón de peso para que todo el mundo tuviera un ordenador en casa. Estas consideraciones, hechas por personajes célebres y vanguardistas en el mundo de la informática, hoy causan estupor, pero acreditan ese imparable avance de las telecomunicaciones y de la informática que caracteriza este tiempo que vivimos.

Desde los prefistóricos tiempos del inicio de la infórmatica, existe una estracha relación entre esta ciencia y el Derecho. No fue hasta 1973 cuando un juez norteamericano dictaminó que el padre del ordenador moderno era el ruso Anatasoff, quien en 1937 comenzó a construir una máquina que le ayudara a recordar todos los cálculos que empleaba en sus operaciones matemáticas.

Fijado judicialmente ese momento de inicio del mundo de los ordenadores, entre ese año y 1970 se produce una lenta evolución, hasta que surge el mini ordenador, que con un espacio físico reducido ofrece la misma potencia que los grandes ordenadores utilizados hasta entonces con un coste económico notoriamente inferior. De ahí a la masificación de la informática sólo existe un paso que todos conocemos: la importantísima evolución tecnológica trae como consecuencia inmediata el coste reducido y asequible de estas máquinas, y por tanto hace que muchas personas del mundo civilizado posean un ordenador personal, que se convierta en un electrodoméstico más de la casa.

Pero, cada vez más, se hace evidente la necesidad de comunicación e información, de la misma forma que se manifiesta la gran capacidad de procesar información por parte de los ordenadores. De ahí que inmediatamente surgió la conveniencia de la búsqueda de nueva información a procesar, lo que unido a la existencia de fuentes dispersas y diversas de información en diversas organizaciones e Instituciones, hizo buscar la forma de encontrar medios de distribuir esa información a través del ordenador de forma rápida, fiable, automática y económica. Se inició entonces en las instalaciones Xerox de Palo Alto lo que se ha venido en considerar la primera red, precursora de Internet, logrando que los ordenadores se comunicaran entre sí y facilitaran los recursos propios a otros ordenadores dentro de la red. De este ya rudimentario origen surgieron las redes de área local (Lan), las redes de área extensa (Wan), y por fin Internet.

Hoy, es una realidad que Internet es el principal fenómeno de las nuevas tecnologías de la información y la comunicación del final de siglo. Es un paso decisivo en la comunicación humana. Cada ciudadano, desde su ordenador, y muy pronto desde otros aparatos electrodomésticos, puede acceder a millones de páginas web, docenas de servidores y de centros de comunicación de todo el planeta, puede realizar las más diversas operaciones económicas, de ocio, comerciales, entretenimiento, y se puede comunicar en tiempo real con otros usuarios de la red. La popularización de la red, su innegable utilidad, la facilidad de conexión que se produce por el abaratamiento de costes y el mayor equipamiento informático de los hogares de todo el globo (aunque esto sólo puede predicar se en gran medida respecto de los países civilizados), la simplicidad progresiva de uso de los programas informáticos que hacen acceder a esta inmensa red, ha hecho que en la actualidad sean millones las personas que acceden diariamente al universo de Internet y que el incremento constante de usuarios sea medible solamente en criterios de progresión geométrica.

Tan es así de importante el progreso en la utilización de Internet, que días atrás se ha puesto de manifiesto que la capacidad de Internet para registrar nombres está tan saturada, que obliga a que en el año 2001 sea necesario ampliar los sufijos de los dominios llamados genéricos. La autoridad de registro, la ICANN, adoptó el día 16 de noviembre de 2001 una lista de siete nuevos sufijos, relación que no había sido modificada desde mediados de los años 90. Así surgen el .info para referirse a las páginas de información, .name para las páginas personales, .pro para las páginas profesionales, . museum para las instituciones culturales, etcétera.

En nuestro país las cosas son, probablemente, algo diferentes en cuanto al desarrollo que repecto al resto de las naciones civilizadas. Aunque el empuje y ascensión de Internet es impresionante en España, puede considerarse que aún se halla en una fase inicial de implantación. Se trata todavía de un acceso selectivo que no llega a todas las capas de la sociedad.

Más no faltan iniciativas que pretenden universalizar su uso. Esta misma semana El Congreso de los Diputados ha aprobado la creación de Red.es, la nueva

empresa pública que regulará los dominios españoles. Asimismo, están en curso iniciativas legislativas que intentan acercar el mundo Internet a todos los ciudadanos españoles, basándose en el concepto de servicio universal de telecomunicaciones que instauró la ley 11/98 de 24 de abril, general de telecomunicaciones, y de la propia previsión de la misma ley, que faculta al gobierno de España a revisar y ampliar los servicios que se engloban dentro de las comunicaciones, a virtud de la evolución tecnológica, de la demanda de servicios en el mercado y de otros factores como el de política social y el desarrollo territorial. En este sentido, actualmente se halla en tramitación ante las cortes generales una proposición de ley presentada por el grupo parlamentario catalán, que confiere a Internet la consideración de servicio universal, y por la atribución ese carácter, se quiere garantizar a todos los ciudadanos, empresas e instituciones, la posibilidad de acceder a Internet y a servicios de telecomunicaciones que incluyan la transmisión de datos, voz y fax, en condiciones de calidad y de accesibilidad económica adecuadas.

Sin duda, la consecución de esta concepción de Internet como servicio universal, acercaría definitivamente la red a la sociedad española, sin posibilidad de retorno.

2. INTERNET Y RESPONSABILIDAD PENAL.

Sin embargo, aunque LA IRRUPCIÓN DE LA INFORMÁTICA Y DE Internet en nuestras vidas, ha producido una innegable ventaja a buena parte de la población mundial, no se puede ocultar que en los últimos tiempos están surgiendo grandes esferas de inquietud. Es frecuente, y diariamente en la prensa y otros medios de comunicación social se pone de manifiesto, la ocurrencia de hechos que escandalizan a la opinión pública mundial, muchas veces hechos que están plenamente insertos en una pura y dura actividad delictiva. Pensemos en la prostitución infantil que llena muchas páginas web, las agresiones que cibernautas de todo el planeta reciben en forma de virus en su ordenador personal mediante la difusión indiscriminada de correos electrónicos, en el descubrimiento de claves personales de acceso restringido, en las defraudaciones patrimoniales perpetradas por el acceso a cuentas bancarias de personas físicas y jurídicas que operan en la red, de la agresión a la intimidad de las personas mediante la extracción de datos de carácter estrictamente personal, de la propia violación de los derechos de la propiedad industrial respecto a los titulares de las marcas, modelos y de los programas informáticos, de la vulneración de los derechos de autor de los autores de piezas musicales, etcétera.

Y que hablar de la piratería en Internet, los conocidos "HACKERS". Han sido atacados por estos internautas las páginas del Pentágono, del FBI, de Walt Disney, de Microsoft, en España se han apoderado de numerosas claves de usuarios de Terra, han entrado y modificado grotescamente la pagina de La Moncloa, y así podríamos seguir con numerosos ejemplos.

Un estudio de la empresa de seguridad informática SIMANTEC, revela que casi un 40 % de las sociedades norteamericanas habían sufrido en algun momento un ataque de los piratas informáticos, mientras que sólo un 15% de las mismas tenía sistemas de seguridad anti-hackers. En los seis últimos años han crecido en un 2400% este tipo de ataques informáticos, causando en muchas ocasiones importantes daños y perjuicios en los sistemas informáticos de organismos, empresas y entidades.

Sin duda estas cuestiónes no son desdeñables, y partiendo de la idea de que todo acto humano debe estar sujeto a las normas legales imperantes, el hecho de que Internet pueda ser una especie de desierto o isla sin regulación positiva, sin control ni intervención de los poderes públicos, es algo que preocupa a todos, (aunque dependiendo del sector afectado las preocupaciones y sensibilidades pueden ser, y de hecho son, bien distintas), y que debe también preocupar a los internautas, los cuales desde una perspectiva inicialmente ácrata o libertaria del ciberespacio, quizás defiendan, o defendieran en su tiempo, arduamente la independencia de la red respecto a los poderes públicos, pero también a estos les debe interesar evitar la presencia de áreas de impunidad en la que en se desdeñan las normativas básicas de la convivencia humana, que perjudican a todos, que afectan a la seguridad y a los intereses de todos los seres humanos.

La actividad delictiva en Internet preocupa y ocupa a las instituciones europeas, que en el seno del consejo de Europa ha creado un comité de expertos con el fin de perseguir los ciberdelitos. La oposición de diversas asociaciones de internet, (iris), que ven en esa actitud de prevención y represión delictiva un atentado a los principios de la declaración de derechos humanos, en cuanto afecta a la libertad humana y a sus manifestaciones más concretas como las libertades de expresión, difusión de ideas y de opinión, e incluso divergencias entre los 41 miembros del consejo de Europa, como por ejemplo en la pretensión de obligar a los servidores almacenar durante cierto tiempo los datos de tráfico en la red, que permitiría a las autoridades examinar los movimientos de un usuario, ponen en duda la eficacia práctica de las resoluciones que puedan adoptar este comité de expertos, lo que añadido al problema jurídico de la territorialidad de las jurisdicciones y la universalidad de las telecomunicaciones, sombrean las posibles soluciones al respecto. Es positivo, sin embargo, el consenso existente entre los Estados a la creación de un tipo delictivo específico para la difusión de pornografía infantil, cuestión a la que igualmente se oponen algunos grupos o asociaciones de usuarios, ya que, alegan por su parte, que en cualquier caso la pornografía infantil ya está perseguida por el derecho común, y que por ello no es precisa la reforma de las leyes penales, en tanto que los delitos contra la libertad sexual ya persiguen y castigan duramente estas acciones ilícitas.

Por otra parte, las grandes empresas de Internet, enemigas acérrimas de cualquier intervención estatal que limite o controle sus negocios, aspiran a que el establecimiento de reglas mínimas en la red garanticen en todo caso la transparencia y el pluralismo, y que la regulación que se pueda hacer por parte de los

poderes públicos beneficien a los usuarios y a ellas mismas. En este sentido, se ha sabido en estos últimos días que tres asociaciones francesas, dos antirracistas y una unión de estudiantes judíos, mantienen una agria disputa con la empresa Yahoo, ya que áquellas pretenden que se impida a los ciudadanos franceses el acceso por ese portal hasta páginas de contenido nazi, lo que así ha sido sentenciado por un Juez de Gran Instancia de París, que ha dado un plazo de 3 meses para que el Portal establezca un sistema de filtrado que evite que los ciudadanos franceses accedan a esa página. A pesar de que la empresa Yahoo es supranacional, y sus ordenadores están fisicamente situados en EE.UU. el Juez aplica la ley francesa, al considerar que aunque el sitio web esté fuera de su jurisdicción, no equivale a que lo estén también los ciudadanos que lo visitan, y afirma por ello que el impedir el acceso a esta página, es una exigencia etica y moral que comparten todas las sociedadaes democráticas.

Internet ha supuesto, como señala el profesor Pérez Luño, un factor de incremento de criminalidad al potenciar la difusión de sabotajes, virus y abordajes a los sistemas por parte de un número imprevisible e incontrolado de piratas informáticos. Las autopistas de la información entrañan un grave riesgo para la protección de los programas. Asimismo, la facilidad de intercambiar información genera importantes peligros para la salvaguarda de datos personales. Nuevos y variados delitos, aparecen cada día y son cometidos con mayor frecuencia, revelando en no pocas ocasiones la insuficiencia, y en otros casos la inexistencia, de regulación positiva estatal que enmarque la actividad en la red y de seguridad, que no supone necesariamente restricción ni cortapisa a sus usuarios.

No es admisible que en justificación de la inanición estatal se aduzca sorpresa o desconocimiento de los riesgos que la red en particular o de las nuevas tecnologías en general generan, ya que desde hace tiempo especialistas en evaluación del impacto de la informática en las libertades vienen alertando sobre estos peligros concretos y determinados.

En sus orígenes Internet se manifestó como un espacio absolutamente libre sin que ninguna autoridad o poder lo regulará poco o nada, y sus más acendrados adeptos basaban tal carácter libre en la autonomía de este respecto a las autoridades estatales, en la negación de los conceptos y categorías jurídicas tradicionales y en una concepción y confianza utópica y libertaria del ciberespacio. Quizás en tiempos pasados fuera defendible esa idea, pero las crecientes actividades delictivas en la red pueden hacer pensar lo contrario. En todo caso, no se puede dejar de lado ni infravalorar hoy día los evidentes logros que la red ha supuesto en nuestras vidas, es un avance irrenunciable y un signo de progreso, pero ello no debe conducir sin más a aceptar pasivamente o a claudicar ante los riesgos de producción delictiva que amenazan a la navegación por el ciberespacio.

Internet implica un importante riesgo de ataque delictivo a bienes jurídicos protegidos por el derecho penal, que no cabe olvidar que viene siendo definido como una constitución en negativo, ya que al tipificar como delitos aquellas agre-

siones a los bienes jurídicos esenciales del ser humano, a los derechos fundamentales e intereses legítimos más básicos de las personas, a las que otorga la más importante y grave sanción en forma de reproche social, es el elemento de salvaguardia último, la ultima ratio de estos derechos intereses fundamentales.

Como siempre, el avance de la tecnología irá muy por delante del avance de la ley y de su adecuación a la realidad social de ahí que sea extraordinariamnte complejo el fijar apriorísticamente un catálogo cerrado de infracciones penales comisibles en la red, o sirviéndose de ella. No obstante, podemos establecer que en la actualidad, y siempre con un ánimo esencialmente enumerativo-explicativo, y nunca exhaustivo o limitativo, por medio de Internet se pueden perpetrar atentados criminales contra los siguientes bienes jurídicos básicos, según la exposición que han efectuado Ruiz Vadillo y Pérezo:

- La intimidad, la imagen y la dignidad de las personas, derechos fundamentales reconocidos en la CE de 1978 en el art. 18, que además establece que la ley limitará el uso de la informática para garantizaresos derechos y preservar el ejercicio de todos los derechos fundamentales, en el 20 y en el 55, el cual limita los supuestos de suspensión de estos derechos a los estados de excepción y sitio en los términos establecidos en las leyes respectivas.

Indudablemente, por los medios informáticos, es cierta la posibilidad de averiguación y/o difusiónde secretos mediante la apertura de mensajes de correo electrónico, a estos penales efectos homologable a la correspondencia privada, la interceptación de telecomunicaciones, la intromisión, el apoderamiento o la modificación de datos personales incluidos en ficheros informáticos de gestoras de servisios, provedores de acceso a internet, centrales de compra, bancos por Internet, etc. Así su cesión o transmisión, o la propagación indiscriminada de estos datos en la red. (art 197 a 212 CP).

A este respecto es de destacar que la ley orgánica 15/99 de 13 de diciembre, de protección de datos de carácter personal, tiene por objeto garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas y especialmente los del honor, intimidad personal y familiar. Así, se establecen en esta ley la obligatoriedad de la exactitud de los datos, él no uso para fines distintos que hayan sido recogidos, el derecho de información y de rectificación, de cancelación por el interesado de los datos relativos a supersona, de oposición al registro de los datos personales, el necesario consentimiento de la persona afectada para el tratamiento de los datos, la imposibilidad de declaración en la recabación de los mismos sobre la ideología religión o creencias de las personas, la reserva de ley para datos que se refieran al origen racial, a la salud y la vida sexual, la exclusiva inclusión en ficheros de las administraciones públicas competentes, y según su propia normativa reguladora, de los datos personales relativos a infracciónes penales o administrativas. (Esta es una cuestión actualmente que tiene un gran debate social acerca de la legitimidad de la publicacion en cualquier medio de las listas de per-

sonas que han sido condenados por determinados hechos delictivos, normalmente de gran transcendencia social y gravedad, como delitos de violencia familiar y/o contra la libertad sexual)

- Atentados a La libertad sexual, mediante la exhibición en la red de imágenes, relatos o informaciones que supongan exhibicionismo o provocación sexual o fomenten la pornografía en menores de edad, el uso de menores en este tipo de actividades, la difusión entre los mismos de material pornográfico.

Tengamos en cuenta que el CP de 1995 regula los siguientes delitos contra la libertad sexual, los cuales pueden ser fácilmente cometidos en la red, y de hecho algunos se están cometiendo en exceso :

- Artículo 186, que castiga al que, por cualquier medio directo, vendiere, difundiere o exhibiere material pornográfico entre menores de edad o incapaces, (pudiera ser el caso de páginas Web aparentemente destinadas al público infantil que contienen material de esa clase, vinculos desde otras páginas aparentemente inofensivas a páginas porno, etc.)

- Artículo 187. Que sanciona al que induzca, promueva, favorezca o facilite la prostitución de una persona menor de edad o incapaz, (realizador de páginas de formato pornográfico utilizando a menores)

- Artículo 189, que tipifica la conducta del que utilizare a menores de edad o a incapaces con fines o en espectáculos exhibicionistas o pornográficos, tanto públicos como privados,(similar al anterior) o para elaborar cualquier clase de material pornográfico, o financiare cualquiera de estas actividades.

- el art 189, que regula la conducta del que produjere, vendiere, distribuyere, exhibiere o facilitare la producción, venta, difusión o exhibición por cualquier medio de material pornográfico en cuya elaboración hayan sido utilizados menores de edad o incapaces, aunque el material tuviere su origen en el extranjero o fuere desconocido. (cualquier acto de favorecimiento o difusión, intermediación, puesta a disposición de páginas web para estos fines, etc. aunque no se sea el autor o relizador del material)

- También se prevé pena para el que poseyera dicho material para la realización de cualquiera de estas conductas,(No se castiga la sola posesión, que es impune, sino la tenencia preordenada a la realización de estas actividades, tipo en el que podría enmarcarse la importación por parte de cualquiera de imágenes de otras páginas web con este tipo de contenido pornográfico infantil para difundirlo en su propia página o en otras diferentes, o la tenencia de este material, producido por otros, para estos fines de difusión, venta o exhibición.)

- La propiedad intelectual e industrial, el mercado y los consumidores, cometido por la distribución o comunicación ilícita con ánimo de lucro y en perjuicio de terceros de obras sujetas a derechos de autor o derivados de la propiedad intelectual o industrial, como el ofrecimiento o la introducción en el comercio, con fines industriales o comerciales, de marcas, modelos o productos del ingenio humano amparados por los derechos de la propiedad industrial, con independencia de su soporte o de su medio de comunicación, siempre y cuando no medie la autorización de los titulares de dichas propiedades. Bajo estos tipos delictivos pueden estar inmersas todas las conductas relativas a difusiones de piezas musicales en formato mp3, duplicado de programas informáticos, etcétera. Los artículos 270 a 277 del código penal de 1995 definen estos tipos delictivos, que habrá de poner en relación, al ser tipos penales en blanco, con las respectivas leyes de propiedad intelectual industrial que amparan la titularidad y derechos de las obras literarias, artísticas, musicales, bases de datos, programas de ordenador y otros actividades derivadas del saber humano.

- Delitos contra el mercado y los consumidores, como puede ser la publicidad engañosa, que igual que se efectúa en la vida real puede difundirse en la red, y que en tanto en cuanto esa publicidad engañosa incidan en un error en los consumidores, que les lleve a tomar una decisión que perjudique grave y manifiestamente a los consumidores, pudiera integrar el delito tipificado en el art. 282 CP.

De otra parte, el artículo 278 castiga al que para descubrir un secreto de empresa se apodera por cualquier medio de datos, documentos escritos electrónicos, soportes informáticos u otros objetos que se refieran al mismo, incluso utilizando para ello el apoderamiento de mensajes de correo electrónico o la interceptación de telecomunicaciones.

- La seguridad nacional y el orden público, en tanto en cuanto la facilidad de acceso y de distribución de mensajes en la red, puede contribuir con su publicación en las páginas web a la difusión de actividades y mensajes terroristas, racistas, xenófobos o que afecten al orden público establecido mediante la incitación a los desórdenes públicos. Tampoco es despreciable el espionaje informático de secretos de estado. Lo mismo se puede decir respecto a los delitos que en la actualidad se prevé incluir en el código penal relativos a la exaltación de actividades terroristas o a la vejación de las víctimas del terrorismo, de fácil comisión a través de la red. (art 472 a 603 CP)

- Delitos contra la hacienda pública, toda vez que cada día en mayor número, numerosas páginas sirven de soporte para realizar transacciones comerciales que eluden el pago de impuestos, sobre todo los indirectos, mediante la no identificación del lugar físico en que tales transacciones se realizan, unido a las circunstancias de de que muchas de las empresas que desarro-

llan actividades comerciales en Internet no tienen cobertura física, careciendo de domicilio social, de licencia fiscal ni de registro de clase alguna, limitándose a ser meros intermediarios informáticos. Hoy es motivo de preocupación entre los Estados el cumplimiento de las obligaciones fiscales de las transacciones por Internet, lo que llevará en un futuro no muy lejano a una regulación fiscal en este sentido.

Aparece pues como perfectamente tangible la posibilidad de comisión por parte de las empresas proveedoras e intermediarias del delito contra la hacienda pública previsto en el artículo 305 del código penal en tanto en cuanto a la cantidad defraudada exceda de 15 millones de pesetas, bien al quedar sin tributación indirecta (IVA) las transacciones en la red, bien mediante el incumplimiento de las obligaciones fiscales directas (impuesto sobre sociedades) por parte de las empresas, que no declaran sus beneficios fiscales anuales. La radicación de estas en paraísos fiscales es asimismo preocupación de los estados, en base a la dificultad de determinar el domicilio real de las mismas, y por ello la dificultad del cobro de los impuestos que se generen.

- El patrimonio de las personas, tanto físicas como jurídicas. Siguiendo la sistemática de Fernández García, la delincuencia informática desenvuelve sus actividades ilícitas en el ámbito de las empresas, entidades financieras públicas y privadas o incluso entre los particulares, pudiéndose destacar a título de ejemplo las siguientes acciones delictivas: alteración de saldos de cuentas corrientes, de fechas valor de los diferentes asientos, transferencias electrónicas de fondos, liquidaciones de intereses, extracciones de cajeros automáticos, uso indebido de tarjetas de crédito para transacciones en Internet, alteraciones de pagos, cobros, nóminas, depósitos ajenos, reducción de primas de seguros, préstamos no autorizados, restablecimiento de pólizas de seguros vencidas o su con prima no abonada, pagos de indemnizaciones, siniestros ficticios, falseamiento de datos en contratos de seguros y bancarios en la red, daños en los ordenadores mediante la difusión indiscriminada de virus informáticos en correos electrónicos, etcétera.

Las conexiones no informadas a páginas radicadas en el extranjero, con el consiguiente pago de la comunicación telefónica internacional, puede constituir una defraudación en forma de estafa, en cuanto se engaña por omisión de información al internauta incauto que accede a ese lugar.

El código penal de 1995, a estos efectos de tipificación de acciones especiales y complejas, considera en su artículo 239 como llaves las tarjetas magnéticas, en tanto que estas contienen unas claves con las que se puede acceder a diversos servicios, entre ellos los bancarios. En esta línea, puede considerarse que las claves de acceso a determinados servicios de Internet son llaves falsas a los efectos del código penal, que producen que cualquier sustracción de efectivo sea considerada como robo y no como hurto. El artículo 248.2 tipifica la estafa informática, esto es, a aquel que valiéndose de cualquier manipulación informática o arti-

ficio semejante consigan la transferencia no consentida de cualquier activo patrimonial en perjuicio de tercero. El 255 sannciona la defraudación en telecomunicaciones por más de 50.000 ptas, y el 256 el uso indebido, esto es, sin consentimiento del titular, de cualquier equipo de telecomunicación, conducta en la que se podría englobar el uso no autorizado de medios de telecomunicación e informáticos que supongan ese quebranto económico. Por fin, el artículo 264,2 castiga los daños informáticos, y ello por virtud de que por cualquier medio se destruya, altere, inutiliza los datos, programas y documentos electrónicos ajenos contenidos en redes soportes o sistemas informáticos.

- Libertad y seguridad de las personas, art. 169 a 173 del CP, utilizando para ello los medios que la red nos proporciona, ya sea mediante la amenaza de causación de daños materiales o personales, ya sea mediante el impedimento de realización de aquellas actividades licitas que cualquier persona puede realizar en el ámbito de su libre arbitrio y utilizando los medios electrónicos precisos, comp pudiera ser el impedimento de acceso a la red.

- Falsedades, (art 386 a 399 CP), ya que con frecuencia para acceder a determinados servicios la persona interesada ha de rellenar un cuestionario que tiene un evidente carácter de documento, aunque éste sea virtual. La suposición de la intervención de una persona que no es la que efectivamente inserta los datos correspondientes en el formulario oportuno, normalmente con fines ilícitos, implica necesariamente, en tanto en cuanto a ese documento tenga efectos en el tráfico jurídico, una real y verdadera falsedad documental tipificada como delito en el código penal. Igualmente puede considerarse falsedad documental la inserción de datos falsos en estos campos.

A este respecto, debe de tenerse en cuenta que el CP de 1995 ha ensanchado el concepto de documento a todo soporte material que exprese e incorpore datos, hechos o narraciones con eficacia probatoria o cualquier otro tipo de eficacia jurídica. (art 26)

Asimismo, de conformidad con el Real decreto legislativo 14/9917 de septiembre, de firma electrónica, puede considerarse como un delito falsario cualquier uso fraudulento de la firma electrónica que identifica formalmente y con plenitud de efectos jurídicos al autor o autores del documento que recoge la firma, en tanto en cuanto ese documento tenga virtualidad y transcendencia para incorporarse al tráfico jurídico.

- Delitos contra el honor de las personas, injurias y calumnias castigadas en los artículos 205 a 210 del código penal, cuando a través de las comunicaciones se imputa falsamente y con conciencia de esa falsedad a personas determinadas la comisión de delitos públicos, así como la difusión de expresiones que atenten a la dignidad de otra persona, menoscabando su fama o su propia estimación, con la especial agravación de que no solamente tales

acciones se cometan utilizando un medio público, sino además fácilmente accesible por la generalidad de las personas, y por ello de amplia difusión, con lo que el mal que se puede infringir hacia la honra de las personas puede ser especialmente trascendente.

- Delitos contra la constitución, art 535 y 536 CP, que prevén castigo para la autoridad o funcionario público que intercepte la correspondencia privada, postal o telegráfica de las personas (en un claro ejemplo de mala técnica legislativa no se hablA en este tipo de los correos electrónicos),o la interceptación de telecomunicaciones, siempre que tales actos no se adecuen a los requerimientos legales, o el art 560 que se refiere a los que causaren daños a las instalaciones de telecomunicaciones.

3. INTERNET Y DERECHO PENAL.

La relación entre la informática, Internet y el derecho son extraordinariamente complejos. Desde un punto de vista jurídico penal la problemática se puede referir, entre otros aspectos, al sistema punitivo, a la interpretación de los tipos penales para la introducción en sus supuestos de hecho de la nueva fenómenológia cibernética, e incluso al sistema de Penas, esto es, la clase y entidad de las sanciones a imponer cuando se realicen estas conductas. El derecho penal forma parte de los mecanismos sociales que tienen por finalidad obtener determinados comportamientos individuales, procurando alcanzar sus fines mediante la declaración de ciertos comportamientos como indeseables y amenazando su realización con sanciones de un rigor considerable, sin duda las más rigurosas que se conocen socialmente, pues no en vano los comportamientos que las leyes penales sancionan ofenden a los principios más intocables de la sociedad. El derecho penal, a la vez que norma represora, tiene una clara finalidad de prevención, en su doble faceta de prevención general y especial. Por ello siempre es interesante que las leyes penales recojan en su tipología delictiva aquellas conductas humanas, del tipo y por los medios de ejecución que sean, que ofenden los bienes jurídicos esenciales. Ello tiene un doble efecto positivo: elimina las indeseables áreas de impunidad y da seguridad jurídica para todos, por que así sabemos aquello que se puede y no se puede hacer, al menos desde el punto de vista del ordenamiento jurídico penal del Estado.

En esta materia de delitos informáticos y en Internet, la tarea que ha de llevarse a cabo ha de consistir, primero en saber que comportamientos realizados mediante un ordenador en la red tengan la condición de indeseables, y después, determinar si esos comportamientos no están ya incorporados a la ley penal en sus figuras genéricas delictivas, y en su caso, proceder a su correspondiente análisis para llevar a cabo su inclusión en los códigos penales. En este sentido no faltan voces, como la del profesor Romeo Casabona, que mantienen la no existencia de un delito informático, sino de una pluralidad de delitos que tienen como nota común: su vinculación con el ordenador. Gómez Peral afirma que es precisa la

determinación de un marco jurídico que defina el ámbito de la actividad cibernética delimitando los supuestos admisibles a la par de aquellos otros rechazables.

Por nuestra parte, entendemos con Ruiz Vadillo, que no todo cambio en las tecnologías ha de suponer una modificación de los correspondientes tipos penales en cualquiera de sus manifestaciones, siendo ello solamente obligado cuando resulten necesario por falta de tipicidad, por ausencia de incriminación de conductas censurables, que no tienen encaje en las formas genéricas delictivas. Situaciones, por más que éstas sean han novedosas, que tienen su cabida en los correspondientes ordenamientos jurídicos penales, no deben dar lugar a la aparición de nuevas tipologías delictivas. Nadie imagina que sea necesario tipificar como figura delictiva autónoma la muerte por accidente de tráfico, cuando existen las imprudencias graves y leves con resultado de muerte en las que perfectamente tiene cabida cualquier evento derivado de la circulación. Por esa misma razón, no parece exigible que se regule un delito de injuria específico cometido en la red, o uno de descubrimiento de revelación de secretos averiguado os mediante la infiltración en ficheros de datos reservados, cuando existen los delitos autónomos de estafa o revelación de secretos en los cuales perfectamente tienen cabida tales acciones específicas, y que contemplan especialmente las modalidades electrónicas. Opino que es positivo que el código penal, respetando sus principios informadores de tiplicidad y legalidad, se simplifique todo lo posible, evitando la irrupción de innumerables subtipos penales que no haría más que dificultar la interpretación de las normas penales e introducir, en suma, criterios de inseguridad jurídica difícilmente asumible, pues no podemos dejar de lado que la seguridad juridica es un principio reconocido en la CE de 1978 en su art. 9,3. No se deben prever de forma indiscriminada y exhaustiva toda la posible tipología de delitos específicos en Internet, pero sí prever las diversas modalidades por las que los delitos pueden ser cometidos, entre ellas, las de las comunicaciones electrónicas. Sin duda esta simplificación contribuirá decisivamente a la clarificación del sistema penal.

La propia doctrina, como Martín Casallo y Davara Rodríguez, critican la existencia en los códigos penales de lo que se viene llamando como delito informático, entendiendo por tal la realización de una acción que, reuniendo las características delictivas, sea llevada a cabo utilizando un elemento informático y/o telemático, o vulnerando los derechos del titular de un elemento informático, ya sea hardware o software. Vemos que en tal definición se incluye tal posible variedad de conductas delictivas alrededor de la informática, que la definición puede devenir totalmente inservible, como pone de manifiesto Bueno Arus, al señalar que el concepto de delito informático es un concepto ambiguo, con el que se puede aludir bien a los delitos que recaen sobre objetos pertenecientes al mundo de la informática (destrucción por sustracción de programas o de material, alteración destrucción o reproducción de datos almacenados, utilización indebida de los ordenadores), como también se pueden incluir en su concepto la comisión de los delitos más variados y tradicionales (delitos contra la intimidad, contra la fe pública, contra el patrimonio, contra el honor e intimidad de las personas, contra la seguridad nacional, falsedades, etcétera)

En la elaboración del código penal de 1995, ya se tuvo en cuenta que el código penal de 1973 no cumplía adecuadamente sus fines de prevención y represión de la llamada delincuencia informática, que no era ni siquiera contemplada como tal en su texto. Términos como ordenador, informática, telemática, correos electrónicos y otros similares eran totalmente desconocidos por nuestro antiguo texto legal. Se planteó por tanto, no solamente el alcance y regulación positiva de la delincuencia que utiliza las novedosas tecnologías de la información, sino incluso si lo que procedía era su inclusión en el nuevo código penal o su regulación en una ley especial.

Esta posibilidad de regulación de los delitos informáticos en legislación especial fue descartada, con el fin de que el código penal fuera el gran texto punitivo que contemplara la mayor parte de las acciones humanas que justifican el reproche delictivo que el delito implica. Además, expone Fernández García, fue relevante la circunstancia de que en muchas ocasiones, el simple uso de un ordenador como medio para cometer un delito, incluso aunque sea en la red o este sea objeto material del propio delito, nada añade de especial al delito cometido, por lo que, como acabamos de ver inmediatamente antes, entiende este autor que los tipos comunes son suficientes para que en su marco queden cobijadas estas acciones delictivas específicas. Se llegó por tanto a la disyuntiva siguiente: ¿Era necesaria la creación de nuevos tipos que respondiesen a una imprescindible modernización del derecho penal respecto al avance de las comunicaciones, o lo que procedía era realizar una labor de adecuación a la realidad de las nuevas tecnologías de aquellos tipos penales generales en los que incide especialmente la delincuencia informática ?.

El legislador de 1995, se ha inclinado por esta segunda postura, ha rehusado la técnica de la ley especial, y ha preferido adaptar los tipos penales preexistentes a las necesidades de tipificación derivadas de la delincuencia informática, equiparando a este fin las nuevas conductas delictivas a los viejos tipos, modernizandolos en lo necesario. Esta solución se le antoja a algún sector doctrinal como insuficiente, ya que puede no dar una respuesta adecuada a los problemas planteados, dar una respuesta insatisfactoria, o peor aún, no previendo determinadas conductas injustas, lo que inevitablemente conducirá a su atipicidad, a la ausencia de sanción o reproche penal.

Aunque Juanes Peces, Presidente del Tribunal Superior de Justicia de Extradura, haya señalado recientemente que uno de los más grandes deficits del CP de 1995 es precisamente la regulación de los delitos relacionados con las nuevas tecnólogias, en todo caso, en el CP de 1995 sí se prevén algunas figuras específicas en atención a la singularidad de las conductas que se pueden cometer por medios informáticos, y así se puede señalar lo ya dicho respecto del concepto documento incluido en el artículo 26, el apoderamiento o apertura de mensajes de correo electrónico para descubrir los secretos o vulnerar la intimidad de otro, descrito en el artículo 197, la estafa cometida valiéndose de manipulación informática o artificio semejante que consiga la transferencia no consentida de cual-

quier activo patrimonial prevista en el artículo 248,1, el castigo como reo de delito de daños al que destruya, altere, o nuutilice o de cualquier otra forma dañen los datos programas o documentos electrónicos ajenos contenidos en redes, soportes y sistemas informáticos tipificado en el artículo 264,2, el de defraudación en las telecomunicaciones y uso indebido de terminales informaticos de los art. 255 y 256, el delito relativo al mercado consistente en la acción de apoderamiento por cualquier medio de datos, documentos escritos o electrónicos, soportes informáticos u otros objetos, para lograr de esta forma el descubrimiento de un secreto de empresa definido en el artículo 278,1, el delito contra la propiedad intelectual del artículo 270, mediante la reproducción, plagio, distribución o comunicación pública, en todo o en parte de una obra literaria, artística o científica, o la transformación, interpretación o ejecución artística fijada en cualquier tipo de soporte o comunicada a través de cualquier medio, siempre y cuando tal conducta se ejecute con ánimo de lucro y en perjuicio de terceros y no se cuenta con la autorización de los titulares de los correspondientes derechos de la propiedad intelectual por sus escenarios, o, por fin, el castigo que de los precursores a la comisión de los delitos de falsedad se hace en el artículo 400, que pena la fabricación o tenencia de útiles, materiales, instrumentos, sustancias, máquinas, programas de ordenador o aparatos, específicamente destinados a la comisión de los delitos falsarios.

Sin embargo, ninguna modalidad específica se regula para los atentados contra la dignidad y el honor de las personas, los delitos contra la libertad sexual, la hacienda pública, la libertad y la seguridad de las personaso las falsedades

Lo que sí entiendo que es una regulación defectuosa y arcaica en el nuevo código penal de 1995 es la llamada responsabilidad escalonada de los delitos y faltas que se cometían utilizando medios o soportes de difusión mecánicos, recogidos en el artículo 30 del texto legal. Ya comienza la deficiencia de la regulación en la propia definición de los medios o soportes, al incluir solamente los medios de difusión mecánicos y no los electrónicos, aunque posteriormente en el punto 2 del citado artículo se amplía extensivamente esta responsabilidad, dado que cuando se refiere a la responsabilidad de los directores del programa en que se difunda el hecho constitutivo de delito, o a los directores de la empresa emisora, en tanto en cuanto se refiere a medios de comunicación no escritos, los cuales obviamente no actuan en soporte mecánico, sino en las ondas, pudiera considerarse como un camino abierto a la incriminación en cascada de las responsabilidades delictivas a los responsables de empresas, y programas, portales, págs. de Internet, etc. No obstante, una mayor clarificación y adecuación de estas responsabilidades penales en cascada, cuando no se conozca realmente a los autores de los delitos, sería más que interesante y deseable, y contribuiría a acentuar el vigor de los principios de culpabilidad, totalmente preponderante en el sistema penal español, así como el de seguridad jurídica, previsto constitucionalmente y verdadero soporte de un estado de derecho en cualquier orden legislativo que nos sirva de referencia.

Pensemos, por ejemplo, en el caso de la pornografía infantil en Internet. Es realmente difícil incriminar estas conductas, si no se sabe el autor material de las fotos, por ejemplo, ni su productor, ni su comprador, ni aquél que las difunde en una página, ni el país en que se encuentra, etc. La pregunta que se plantea es sideberemos recurrir a esta responsabilidad en cascada e incriminar a los titulares de las páginas en que se incluyen, o a las empresas responsables de los portales por permitir conscientemente la inclusión de estas fotografías o por omitir la diligencia debida al no controlar sus contenidos.

Si la aplicación de lo que se han venido llamando "responsabilidad en cascada", que ha sido considerada por buena parte de la doctrina como una verdadera lotería criminal, ya ha sido complicada cuando nos hemos referido a los delitos cometidos por medio de la imprenta, concepción clásica de los códigos penales anteriores, aún puede ofrecer una muy mayor dificultad en tanto en cuanto queramos atribuir esta responsabilidad a los directores o responsables de publicaciones de la red, portales o páginas web. No obstante, cabe decir, que ya desde 1983, la jurisprudencia del tribunal supremo ha venido moderando este mecanismo, rechazando toda interpretación objetivista, que residencie el delito solamente en el hecho de desconocer el verdadero autor del delito o de que, aun conociendolo, éste se hallaba en el extranjero. Ciertamente, el principio de culpabilidad penal recogido hoy en el artículo 5 del código penal de 1995, que determina que no existirá pena sin dolo o imprudencia, obligaría a que por parte de los directores de estas publicaciones, materiales o virtuales, tengan, bien conocimiento cierto de los actos punibles que se están ejecutando, bien que se conduzcan con ausencia de aquellas medidas de precaución necesarias para que estos hechos no se produzcan.

Considero, que dado lo delicado de la extensión de la responsabilidad criminal aquellas personas que no son realmente los autores del hecho, así como de las singularidades y de las grandes diferencias que existen entre los medios de comunicación tradicionales y la comunicación informática, en este caso sí que sería deseable una regulación específica que determinara este tipo de responsabilidad.

Otra cuestión no satisfactoriamente resuelta, esta más de carácter procedimental que sustantiva, es la que se deriva de la competencia de los Tribunales para el enjuiciamiento de hechos delictivos cometidos a través de Internet, cuando el autor material no se haya domiciliado en España, lo que acontece en numerosas ocasiones, y como tampoco están físicamente en territorio español los ordenadores y servidores a través de los cuales se comete el delito.

A este respecto deberemos de tener en cuenta que cualquier dato o imagen insertada en la red es accesible desde cualquier parte del mundo, que no existen iguales normas penales entre todos los paises, de tal suerte que lo que es licito aquí puede ser ilícito allí, que existen paises con los que no se han concertado tratados de extradición o de cooperación en materia internacional, y por fin, la territorialidad de las normas de policía y de perseguibilidad de los actos ilícitos.

Los Tribunales españoles son competentes para enjuiciar los hechos punibles cometidos en el territorio español, (art 23 de la LOPJ), lo que nos lleva a examinar en cada caso concreto el lugar en que se entienda que se ha cometido el delito, variable según la infracción de que se trate. En el supuesto de que el lugar de comisión del hecho sea el extranjero, hará imposible le intervención de la Justicia española, salvo que sean de aquellos que el propio art 23, 3 establece que son perseguibles en España con independencia de quién y el lugar en que se cometan, entre los que se encuentran delitos contra las seguridades exterior e interior de España, atentados al Jefe de Estado y su familia, falsificación de moneda, trafico de drogas, pornografía, genocidio, terrorismo y otros.

En mi opinión, para solucionar este inconveniente, la colaboración entre estados debe ser más intensa, y en determinados casos especialmente graves, establecer el principio de persecución supracional de los mismos, mediante la concertación de los oportunos tratados internacionales. La puesta en funcionamiento de un Tribunal Penal internacional sería extraordinariamente positivo.

Y esto es lo que da de sí el CP en materia de delitos informáticos o en la red de Internet

Quizás a algunos esta regulación les pueda parecer escasa, pensando en que los delitos informáticos debieran de tener una mayor regulación específica, pero no hay que olvidar que en los tipos comunes del código penal tienen cabida buena parte de las acciones humanas, con independencia del medio o instrumento con el que se cometan, así como que, si incluyéramos una exhaustiva regulación jurídico penal de esta tipología delictiva, por mor de la interpretación literal y restrictiva que de cualquier tipo penal hay que efectuar, podríamos lograr precisamente el efecto contrario, esto es, esferas de impunidad nunca deseables, por falta de previsión legal. Opino que una buena técnica legislativa será aquella que regule y legisle sobre los delitos informáticos y de Internet en función de la imposibilidad de castigar determinadas conductas moralmente reprochables con los instrumentos legales que actualmente poseemos, sin perjuicio naturalmente, de que se deberá hacer un esfuerzo innovador en el desarrollo legislativo acompasado las previsiones legales al desarrollo y evolución propia de la técnica, incluyendo aquellas conductas tan singulares que dificílmente puedan ser castigadas con los instrumentos al uso.

Pero existen más problemas de orden legislativo que exceden al campo penal. Si entendemos el ordenamiento jurídico estatal como un todo, que debe obedecer a unas reglas de sistemática y seguridad, de modernidad, de interrelación y de similitud entre todas ellas, el panorama español no es muy halagüeño, pues al lado de leyes novedosas, que en mayor o menor medida y con mayor o menor fortuna recogen inevitablemente los avances tecnológicos, como el código penal de 1995 (aunque no pueda calificarse como un dechado de perfección a este respecto), o la ley de enjuiciamiento civil que entrará en vigor en enero de 2001, se encuentran otras absolutamente obsoletas, que no dan respuesta adecuada a la

problemática que actualmente plantean las nuevas tecnologías, de la trascendencia, eficacia y aplicabilidad en un estado de derecho como la ley de enjuiciamiento criminal y el código civil, ambas leyes nacidas en el siglo XIX, sobre lo cual cualquier comentario al respecto sobra en relación a la existencia de tecnología punta en campo alguno del conocimiento humano.

4. INTERNET Y REPONSABILIDAD CIVIL.

El artículo 109 del código penal establece que la ejecución de un hecho delictivo dará lugar a reparar los daños y perjuicios por el causados. Ello quiere decir que el responsable criminalmente de un delito o falta lo es también civilmente, y que por ello, estará obligado a reparar el mal causado, además de cumplir la sanción penal que cada delito prevea. Esta reparación, deberá efectuarse, según el artículo 110 mediante la restitución, la reparación o la indemnización de daños y perjuicios.

A raíz de este pronunciamiento penal es evidente que cualquier autor de un delito informático o en la red es responsable también de los daños y perjuicios que se causan por la comisión de tal delito, y por ello debe indemnizar los en virtud de la responsabilidad civil contra. Así, el causante de daños en un ordenador por la transmisión de un virus informático, estará obligado a reparar los o a abonar el importe de la reparación, el defraudador por disposición de fondos, a devolver íntegramente el importe de lo defraudado, el que viola los derechos de la propiedad e intelectual o industrial, a indemnizar a sus titulares en la medida en que su acto le haya perjudicado, el causante de injurias o calumnias de la red, o violados del derecho a intimidad, a reparar los daños morales y infringido, etc. etc

En el supuesto de delito, la responsabilidad civil aparece claramente determinada, en en cuanto es subsidiaria es inseparable de aquel. Es lo que se vienen terminando por la doctrina responsabilidad civil "ex delicto".

Pero además, se pueden plantear supuestos en los cuales pudiera existir responsabilidad civil sin responsabilidad penal, como pueden ser los casos de la responsabilidad civil de contractual, esto es, la responsabilidad civil derivada del incumplimiento del contrato firmado entre partes, y responsabilidad civil extra contractual, es decir, a derivada de los actos del hombre que, sin estar ajustadas enteramente a las normas legales en vigor, no infringe un las leyes penales, no son delictivas.

El código civil, recoge estos supuestos de responsabilidad civil, en el artículo 1101 en cuanto a la responsabilidad civil contractual, al señalar que quedan sujetos a la indemnización de los daños y perjuicios causados, los que en el cumplimiento de sus obligaciones incurrieren en dolo negligencia o morosidad, y en el artículo 1902 que obliga a reparar el daño causa-

do a los que por acción u omisión cause daño a otro, interviniendo culpa o negligencia.

La primera de ellas, la responsabilidad civil derivada del contrato, está de considerará como una responsabilidad civil objetiva, esto es, se sujeta a la obligación de indemnizar por el simple incumplimiento contractual, sin necesidad de culpa o negligencia. Respecto de la segunda, responsabilidad civil extra contractual, es de matiz más subjetivo, requiere que el acto del hombre sea intencionado o no se ajusten a los parámetros de conducta existentes, tenencia por negligencia en el actuar humano.

Aplicados estos principios de la responsabilidad civil al hecho informático, podrá dar lugar a la exigencia de responsabilidad civil en todos los supuestos de incumplimiento de los cibercontratos, a este respecto nada alejado al resto de los convenios jurídicos, en los supuestos de incumplimiento que de sus obligaciones hagan los proovedores de acceso a internet, por los productos o programas informáticos defectuosos, en los supuestos de daños ocasionados por el hardware o software, incluso por la navegación en la red, a los titulares de ficheros informáticos por el acceso de terceros a datos personales en ellos contenidos, atc.

La escasa regulación legal especial de los fenomenos y consecuencias jurídicas derivadas de las nuevas tecnologías, hace que igualmente sean escasos los supuestos específicos de responsabilidad civil por parte de sus operadores.

No obstante, citar que el RDL 14/99, de firma electrónica, establece la responsabilidad civil de los prestadores de servicios de certificación por los daños y perjuicios causados en el ejercicio de su actividad, cuando incumplan las obligaciones que les impone el RDL o actúen con negligencia. Además, se atribuye al prestador de servicios la obligación de probar que actuó con la debida diligencia.

De otra parte, la LO 15/99 de protección de datos de carácter personal, atribuye a los ciudadanos que, como consecuencia del incumplimiento de los preceptos de la Ley, sufran daño o lesión, tendran derecho a ser indemnizados por el responsable o encargado del tratamiento de los datos.

Aquí concluye mi intervención. Rememorando el lenguaje de Windows, he pretendido hacer un paseo por lo más relevante de la legislación penal y civil al respecto. Espero y deseo que haya sido de su interés.