EGUZKILORE
Número 20.
San Sebastián
Diciembre 2006
197 - 215

DELITO E INFORMÁTICA: ALGUNOS ASPECTOS DE DERECHO PENAL MATERIAL

Joaquín GIMÉNEZ GARCÍA
Magistrado Sala II Tribunal Supremo

I. EVOLUCIÓN SOCIAL Y CAMBIO PENAL

Toda Sociedad está en constante movimiento, y más todavía, si cabe, la sociedad actual caracterizada por una globalización de los mercados, una interconexión en las economías de los diversos países y unos movimientos migratorios que procedentes de los países menos favorecidos se dirigen a los países desarrollados en busca de mejores perspectivas de futuro, y, en ocasiones, huyendo de un horizonte de hambre y sin futuro.

Paralelamente, estos cambios van generando una modificación de los valores para hacerlos más universales y por tanto comunes a todas las culturas que conviven o coexisten en la Sociedad. Paralelamente a estos cambios sociales y valorativos se producen cambios en los ámbitos de intervención del sistema penal.

El Código Penal, definido con acierto como una Constitución Negativa, se integra por el catálogo de acciones que atentan contra el cuadro de valores que permiten una convivencia de una sociedad cada vez más plural. Es en definitiva un mínimo ético aceptado de forma generalizada por la Sociedad a través de sus legítimos representantes y elaborado en sede parlamentaria, de suerte que su actuación viene definida por tres notas:

a) Por ser *fragmentaria* al recoger sólo las infracciones más graves y aquellas en las que ha existido un generalizado consenso para así considerarlas, porque en definitiva, la razón de la obligación de abstenerse de las acciones estimadas como delictivas en el Código, no es tanto la realidad de un sistema coactivo representado por la realidad de la sanción, lo que siendo necesario, es la última ratio para los infractores, la verdadera razón de la obligatoriedad de la norma penal es el proceso de convicción aceptado en la sociedad de que así debe ser. Por eso la Ley es la expresión de la voluntad colectiva concretada en el Parlamento.

b) Por ser *subsidiaria* en la medida que la respuesta penal debe ser la última y parte del fracaso de las anteriores respuestas, aunque hoy está admitiéndose el carácter promocional del Derecho Penal mediante delitos caracterizados por el adelantamiento de las barreras de protección, política aceptable pero con controles, porque el Código Penal no es ni puede convertirse en un Código de urbanidad o buenas costumbres.

c) Por ello, su intervención es o debe ser *mínima* en el doble sentido de referirse a las acciones más graves, y con una respuesta punitiva proporcionada e indispensable para el restablecimiento del Código violado.

Estos cambios sociales y estos principios rectores del sistema penal, dan lugar a un doble movimiento constituido por la permanente adaptación del Código a las cambiantes exigencias sociales. Por un lado, se expulsan del Código conductas que en el momento actual no requieren la respuesta penal, por ejemplo, el escándalo público o el adulterio/amancebamiento, que representaban la criminalización de acciones reprochables desde una determinada moral religiosa, que convertía el delito en un pecado secularizado.

Por otro lado ingresan y se incorporan al Código ataques a nuevos bienes jurídicos antes ignorados, como ocurre con los bienes jurídicos colectivos: Medio ambiente, Ordenación del territorio, Delito fiscal, o se penalizan nuevas formas de comisión delictiva de delitos.

El cambio social viene ligado a la evolución tecnológica. Hoy día Internet ha supuesto una revolución en el mundo de las comunicaciones y del conocimiento, con la peculiaridad de que permite, a los países atrasados, avanzar enormemente. El caso de la India es paradigmático.

Este cambio tecnológico tiene una evidente incidencia en el mundo penal. Con Zaffaroni se puede decir que *"....el impacto de la explosión tecnológica es un problema que la política criminal conoce sobradamente. La técnica siempre es un arma y cada avance fue explotado criminalmente en forma tal, que siempre el criminal está más tecnificado que la prevención del crimen...."*.

Por decirlo con otras palabras, las redes criminales descubrieron el espacio común europeo y la permeabilidad de las fronteras antes de que en Europa surgiera la concepción de espacio común de justicia, libertad y seguridad, ya existía un *"espacio delictual común"*.

Denominador común de esta revolución tecnológica, en el escenario en el que se da, es un mundo globalizado, con una universalización de la informática que permite que no sólo la información, sino multitud de contratos se efectúen entre partes situadas en distintas partes del globo, o que desplazamientos de dinero o mercancías se efectúen en décimas de segundo. Paradójicamente estas sociedades informatizadas son vulnerables en extremo porque la facilidad de la información es también facilidad para la intervención de terceros en los sistemas informáticos, la interceptación de mensajes y en definitiva nuevos ámbitos de indefensión de los ciudadanos y a las dificultades inherentes a la prueba de cargo respecto de la criminalidad organizada internacional, que tiene como uno de sus dogmas la destrucción de todo vestigio probatorio –STS 1064/2002 de 7 de Junio– se añaden específicos problemas por las dificultades probatorias que ello entraña y que, refuerzan, más si cabe la importancia de la prueba por indicios a prueba indirecta como la más disponible para integrar la actividad probatoria de cargo capaz de provocar el decaimiento de la presunción de inocencia. Por otra parte la tecnificación de los medios utilizados por los criminales no suele estar aparejada con la capacitación necesaria de los operadores policiales y judiciales, y por ello cabe la posibilidad de espacios de impunidad en estos nuevos escenarios.

II. DELINCUENCIA E INFORMÁTICA

Desde un *triple enfoque* se puede entender la incidencia de la informática en el campo de la delincuencia.

Podemos hablar de la informática, como *nuevo medio comisivo* de delitos que ya existen en el Código.

En segundo lugar podemos hablar de *delitos informáticos strictu sensu*, es decir el objeto de estos nuevos delitos sería el ataque al propio sistema informático.

En tercer lugar podemos hablar de la informática como *medio probatorio* lo que nos reenvía al tema de informática y proceso probatorio.

Me referiré exclusivamente a los apartados primero y segundo.

III. DELITOS QUE UTILIZAN LA INFORMÁTICA COMO MEDIO DE COMISIÓN

En estos casos, los delitos mantienen su propia naturaleza y caracteres, su única especificidad, lo nuevo, es el medio de comisión, que lo hacen a través del sistema informático.

Este medio comisivo produce efectos propios siendo el más característico una intensificación del efecto lesivo, ya que los perjudicados pueden ser muchos, y por otra parte el daño se magnifica como ocurre con la difusión de virus que se transmiten con facilidad enorme y con una enormidad de daños.

También esta nueva forma de comisión puede afectar a la estructura de algunos delitos, y así, por ejemplo, el delito de estafa en su versión informática no exige un engaño precedente y consiguientemente desaparece toda la problemática de que el engaño sea bastante.

Se pueden indicar tres grupos de delitos cuyo medio comisivo puede ser la informática: a) Delitos socioeconómicos, b) delitos relativos a la intimidad/privacidad y libertad sexual, y finalmente, c) los atentados contra la Seguridad Nacional e Internacional.

Pasamos a una breve referencia.

1. Delitos Socioeconómicos

Dentro de este capítulo se pueden encontrar los siguientes:

A) El robo mediante la inutilización de los sistemas de alarma a los que se refiere el art. 238-5 Cpenal

En este sentido se puede citar la STS de 26 de Junio de 1999 que calificó de robo de este apartado el desprendimiento o cualquier artificio destinado a evitar el normal funcionamiento de dispositivos de seguridad incorporados a objetos puestos a la venta es, cada vez más frecuente, establecimientos comerciales. Se está en un supuesto de fuerza típica, por la específica previsión legal que supuso la incorporación de este párrafo.

B) Estafa informática

Constituida por las manipulaciones en programas informáticos *"....valiéndose de alguna manipulación informática o artificio semejante consigan transferencia no consentida...."*. Art. 248-2º. En esta estafa informática no se precisa engaño antecedente como ya se ha anunciado, precisamente, el primer caso de delincuencia informática que arribó al Tribunal Supremo –STS 19 de Abril de 1991– supuso la absolución por el delito de estafa al empleado de banco que mediante apuntes contables falsos efectuaba por ordenador, consiguió un enriquecimiento injusto. Se estimó que la figura aplicable era la de apropiación indebida. Todo ello en relación al Cpenal de 1973.

Se afirma en la STS de 20 de Noviembre de 2001 que en el Cpenal de 1995 se tipifica una modalidad específica de estafa consistente en los actos de asechanza a patrimonios ajenos realizados mediante manipulaciones y artificios que no se dirigen a

otras personas, sino a máquinas, en cuya virtud, estas, a consecuencia de una conducta artera, actúa con automatismo en perjuicio de tercero, sin que sea preciso engaño previo.

La STS 1557/2004 de 31 de Diciembre, absolvió al recurrente de un delito de estafa informático –confección de páginas virtuales amarillas– . Por estimar que no se acreditó la voluntad de defraudar en la medida que no quedó claro que el recurrente utilizara indebidamente el nombre de "Telefónica" para infundir confianza y porque, en definitiva puso algunos elementos técnicos a favor de las personas que contrataron la página web para captar clientes.

Recientemente, se publicaba una información del Departamento de Estado Americano relativo a cinco de las estafas informáticas más utilizadas en los Estados Unidos. Todas ellas tienen como elemento común el país de origen: Nigeria, de suerte que tales *"timos"* reciben el nombre de *"fraude 419"* (artículo del Cpenal de Nigeria que los describe): a) mujeres que previamente han conocido y seducido a su interlocutor por Internet, aquélla le comunica que ha sufrido un robo y lesiones en Nigeria, donde ha tenido que acudir por razones de profesión y solicita dinero porque la embajada americana se desentiende del caso y le solicita su ayuda económica; b) abogado que se pone en contacto con un ciudadano para comunicarle que ha heredado una fortuna de un pariente lejano, la muerte se produjo en Nigeria y debe enviarle dinero para atender a diversos gastos; c) director de personal de empresa nigeriana que busca trabajadores con muy buen sueldo pero el solicitante debe enviarle unos miles de dólares para abonar los gastos derivados de su contratación (visados, tasa de inmigración, etc. etc.); d) subasta on line en la que el timador paga una cantidad superior al precio del objeto, mediante orden de pago internacional, pero paga mucho más dinero, comunica seguidamente su error al vendedor y le solicita la devolución del exceso, a lo que el vendedor accede, comprobándose después que la orden de pago inicial no es válida. El vendedor se queda sin el producto vendido y sin el dinero devuelto a pretexto del error y e) lavado de dinero negro, es una variante de *"nuestra"* compra del billete de lotería premiado, un funcionario corrupto quiere lavar dinero y solicita ayuda a través de Internet ofreciendo entre el 10 al 50 % del total del dinero a blanquear a quien le ayude, ahora bien, el incauto debe empezar por mandar dinero a bancos y abogados porque el timador no puede dejar rastro, y efectuado, ya recibirá su premio. (Fuente: El País, 12 de Marzo de 2007).

C) Falsedades Documentales

El concepto de documento a efectos penales ha tenido una ampliación en actual Código. El art. 26 considera como tal *"todo soporte material que exprese o incorpore datos, hechos o narraciones con eficacia probatoria*". Por su parte, el art. 390 se refiere a la alteración en un documento de la forma allí expresada. Por ello deviene en posible la conceptuación de documento a disco, DVD, cinta magnetofónica, fotografía, etc. etc.

En general la naturaleza de las falsificaciones documentales es la de ser delitos mediales para otro fin. Piénsese en cambios efectuados en el historial clínico informatizado de una persona o en el expediente académico, o incluso en documentos notariales o registrales, o incluso, judiciales que se encuentren en la base de datos correspondiente.

Se trataría normalmente de situaciones concursales dado el carácter instrumental que tienen las falsedades documentales. Así por ejemplo la STS 951/2006 de 2 de Octubre confirmó la condena de quien obtuvo los datos particulares de un tercero y con ellos solicitó y obtuvo una tarjeta del Corte Inglés, que solicitó por Internet, y con ella en su poder, efectuó diversas compras. No se condenó por estafa porque no existió engaño en la exhibición de la tarjeta falsa, al no existir una previa comprobación de los datos personales del que exhibió la tarjeta.

D) Publicidad engañosa

El art. 283 contempla la facturación en perjuicio del consumidor de cantidades o productos o servicios por cantidades superiores al servicio prestado mediante la alteración de los aparatos de mediación. Todos recordamos el fraude de algunas gasolineras por alteración en sus aparatos suministradores de combustible. En general, se estará en presencia de conductas fraudulentas engañosas, cometidas a través de estas alteraciones, que, penalmente, se resuelven en virtud del principio de consunción del art. 8-3º aplicando el delito que integre mayor punibilidad. El art. 286 introduce nuevas acciones penales consistentes en la facilitación de servicios de radiodifusión sonora, televisiva o interactiva, prestados electrónicamente con ánimo de lucro y en perjuicio del prestador.

E) Blanqueo de capitales

El art. 301. Transferencias a cuentas opacas a paraísos fiscales de capitales procedentes de la droga o del producto de otros delitos.

F) Delitos contra la Propiedad Intelectual/Industrial

Arts. 270 y siguientes. Se trata de una situación que ya ha planteado problemas sobre todo desde la perspectiva de la propiedad intelectual en relación a los derechos de autor. Así en Bruselas la Biblioteca Digital Europea ha tenido problemas jurídicos en relación a los derechos de autor de los autores cuyas obras se ofrecían digitalizadas y una situación semejante se ha visto en España en relación a la Biblioteca Virtual Miguel de Cervantes, la primera en la digitalización de libros que ha sido condenada recientemente por haber puesto a disposición del público una obra sin contar con la autorización de los titulares de los derechos.

La Audiencia Provincial de Alicante, en una reciente sentencia de 9 de Enero de 2007 de la Sección VIII, ha declarado con claridad que ni la ausencia de ánimo de lucro ni la condición más o menos pública de las entidades participantes ampara o permite ignorar los derechos de propiedad intelectual de los autores de las obras afectadas por la digitalización. Los hechos concretos se referían a haberse incluido por parte de la Universidad de Alicante y de la Fundación Virtual Miguel de Cervantes en su catálogo de obras digitalizadas de libre acceso gratuito de una obra sin expresa autorización de la titular de los derechos de explotación ni de los herederos del autor de la obra.

La STC 104/2006 de 3 de Abril de 2006 en relación a la condena por un delito continuado contra la propiedad intelectual y de descubrimiento y revelación de secretos de empresa manifiesta que:

"...no cabe duda de que la tecnología informática facilita la comisión de los delitos contra la propiedad intelectual, no sólo en cuanto a la grabación o reproducción no autorizada de los CD's, sino sobre todo en lo relativo a la distribución y venta de los productos sin autorización de los legítimos titulares de los derechos de propiedad intelectual....", y añade *"....que la utilización de las tecnologías de la información a la vez que facilitan la comisión del delito dificultan su persecución...."*.

El caso enjuiciado se refería a la compra de tarjetas descodificadoras para bajarse música sin pagar los derechos de propiedad intelectual.

Es evidente una correcta coordinación y supervisión jurídica puede evitar la innecesaria judicialización de conflictos, siempre perjudicial.

El derecho de autor es una herramienta jurídica con un contenido económico imprescindible para la economía de cualquiera, pero la responsabilidad de los desajustes que se produzcan no deben endosarse en medio a través del cual se difunde la obra –la red informática– , sino a la falta de previsión en articular resortes que permitan esta difusión haciéndola compatible con el pago de los derechos correspondientes a las personas beneficiarias de este acceso a la literatura.

Se trata de los delitos cuyo objeto *no* se refiere a los propios elementos lógicos o técnicas de las redes informáticas o programas informáticos, y por tanto excluidos del supuesto del art. 270-3º ó el 273 en relación a patentes informáticas. La defraudación de estos elementos constituiría un delito informático *strictu sensu*, como luego se verá, si bien, en realidad es una variante de los delitos contra la propiedad intelectual/industrial.

Evidentemente, la digitalización de libros respecto de los que ha caducado la protección de los derechos de autor, y que por tanto han pasado a formar parte del patrimonio común de la Sociedad, no ofrece ningún problema, como no lo presenta el *"colgar"* en la red libros en esa situación. La Biblioteca Nacional ha puesto recientemente en marcha una Hemeroteca Digital relativa a la prensa histórica editada en un tiempo tal que garantiza la seguridad de tratarse de publicaciones que no tienen riesgo de ser "colgadas" en la red por haber decaído todo derecho de propiedad intelectual. En este sentido hay que recordar que a finales del pasado año, se publicaron en el Diario Oficial de la Unión Europea de directivas sobre aspectos de los derechos de propiedad intelectual.

La Directiva 2006/116/CE de 12 de Diciembre fija el plazo de los derechos de autor sobre las obras literarias y artísticas que se extenderán durante la vida del autor y 70 años más después de su muerte, con lo cual se unifica en la Unión Europea el plazo de protección de los derechos de autor. Esta directiva contiene disposiciones sobre obras cinematográficas y audiovisuales.

La segunda Directiva 2006/115/CE de 12 de Diciembre se refiere a los derechos de alquiler y préstamo y otros derechos afines de los derechos de autor en el ámbito de la propiedad intelectual.

2. Delitos contra la intimidad/privacidad y libertad sexual

A) Amenazas/Coacciones. Art. 169 y 172. También aquí la única especificidad es el empleo, como medio camino del sistema informático. Una reciente sentencia de la Audiencia Provincial de Santander, Sección III, de 22 de Diciembre de 2006, con-

dena por falta de amenazas del art. 620.2 Cpenal 1995 las amenazas proferidas mediante frases y expresiones intimidatorias vía MSM por el acusado tras la ruptura con la denunciante.

B) Pornografía Infantil Venta y difusión de material pornográfico a menores, o venta a mayores pero de material en el que los sujetos son menores. Art. 186 y 189.

Son varias las Sentencias de la Sala II que abordan el tema de la pornografía infantil a través del Internet. La STS de 2 de Noviembre de 2006, aborda el tema de la prueba de cargo y de la *notitia criminis*: intercambio de archivos de pornografía infantil, ante lo que, vía mandamiento judicial se solicitó de los proveedores del acceso, los datos necesarios para identificar a los usuarios de varias direcciones así como las líneas telefónicas utilizadas. Tras ese inicio de las actuaciones las pruebas se obtuvieron como consecuencia del resultado de varios registros domiciliarios en los que se ocuparon ficheros y archivos.

STS 913/2006 de 20 de Septiembre. El acusado visitaba páginas web de pornografía infantil que se ofrecían en direcciones de correo compuestas de grupos de usuarios que forman las llamadas *"comunidades Microsoft"* que insertaban en la red fotos de contenido pornográfico. *No* se apreció la pertenencia a organización. Se trataba de un visionado en solitario.

Por el contrario, la STS 1444/2004 de 10 de Diciembre en caso también de difusión de pornografía infantil en Internet entendió apreciable la concurrencia de la organización. En la fundamentación se dice:

> *"Pues hay que comenzar señalando que las nuevas hipótesis surgidas con motivo de la utilización de innovadoras tecnologías en la práctica de la fenomenología criminal, vienen a alterar también antiguos contenidos conceptuales que resultan desfasados desde una adecuada interpretación de la finalidad de la norma penal, sin perjuicio del obligado y estricto respeto a las exigencias del principio de legalidad.*
>
> *En tal sentido, cuando de conductas delictivas cometidas por varios partícipes a través de redes informáticas, como Internet, se trate, el propio instrumento comisivo "la red", bastará para integrar tanto la utilización de medios idóneos para configurar la actuación coordinada propia de la organización delictiva, como para alcanzar la finalidad pretendida, ala que ya antes aludíamos, de una mayor facilidad de comisión del delito y capacidad de lesión del bien jurídico protegido, añadiendo especiales dificultades tanto a la prevención como para la persecución del ilícito.*
>
> *Lo esencial en estos nuevos fenómenos delictivos está, precisamente, en que la simple utilización de la red de comunicaciones informáticas supone ya el aporte del elemento de coordinación y el empleo de medio excepcional que se proyecta hacia una mayor lesividad, imprescindibles, aunque no del todo suficientes, para la consideración de la existencia de una organización criminal.*
>
> *Precisándose a partir de ello, tan sólo, la puesta en relación de los diferentes sujetos intervinientes con el propósito de difusión de las imágenes con una atribución de concretos cometidos, para ver completados, en estos casos, los requisitos exigibles para la integración del concepto "organización".*
>
> *Sin que haya de requerirse para configurar la trama estructurada, en este ámbito de la comunicación "redial", un conocimiento personal, directo y recíproco de los diferentes integrantes del grupo, ya que el mismo se produce precisamente por medio de*

la red, alcanzándose el concierto mutuo, la distribución de "papeles" y la coordinación potenciadora de la incrementada agresividad lesiva de las conductas, a través del acatamiento y cumplimiento, por cada uno de los partícipes, de las reglas que así mismo se dan los grupos constituidos en torno a los "lugares de encuentro" que constituyen las direcciones y páginas "web" de la propia red.

No es lo mismo, por tanto, ni merece igual consideración punitiva, la conducta del infractor aislado que capta, elabora y distribuye por sí solo material pornográfico, incluso mediante INTERNET, que el supuesto de hallarnos ante una pluralidad de usuarios que, coincidentes en ese "lugar de encuentro" virtual, coordinan sus acciones para potenciar las posibilidades de consumo de las imágenes dañinas para los derechos de los menores, permitiendo, además, su difusión incluso a otras personas ajenas al grupo organizado.

Por ello, en el supuesto que aquí nos ocupa, ha de afirmarse, en coincidencia con el criterio mantenido por la Audiencia, que concurre la agravante específica de "organización", prevista en el artículo 189.2 del Código Penal, toda vez que no sólo el recurrente actuó en colaboración con los otros integrantes del "grupo" de proveedores y consumidores del material pornográfico prohibido, con una específica atribución de funciones, cual la confección y aporte de "álbumes" de fotografías por él elaboradas a un "depósito" centralizado en una específica página "web", sino que, además, con ello posibilitaba también el acceso de terceros a esa oferta, como antes decíamos, ampliando la agresión al derecho a la indemnidad sexual de las víctimas de la infracción que es, en definitiva, la razón de ser esencial y el fundamento de la previsión legal agravatoria de la conducta".

Por su parte, la STS 1058/2006 de 2 de Noviembre de 2006 condenó como autor de un delito de distribución y difusión de material pornográfico. El condenado *"....poseía material pornográfico infantil y ha procedido a la distribución y exhibición del mismo por medios informáticos, a través de uno de los ordenadores sito en..... tras las investigaciones policiales y la entrada y registro practicada en el referido domicilio se incautó ..... dos discos duros informáticos..... de contenido sexual y pornográfico con niños...."*.

Destacamos el f.jdco. segundo en el que se rechaza la impugnación del atestado efectuado por la Brigada de Investigación Tecnológica de Madrid.

"....La impugnación no debe ser atendida. La sentencia de instancia, Fundamento de derecho primero, apartado 1º y 7º, analiza la cuestión planteada relativa a las investigaciones de la Brigada de Investigación Tecnológica de Madrid, que se inician con un oficio del Comisario Jefe de fecha 29.3.2005, en el que tras exponer el conocimiento que se tiene de que a través de distintos canales del Servicio de Internet IRC, (Internet Relay Chat) se producen intercambios de archivos con pornografía infantil, facilitando dicho servicio de Internet que los usuarios puedan intercambiar archivos, quedando estructurados los Servidores a su vez en Canales, habiéndose comprobado por dicha Brigada que en el canal, "100% Preteen Girl Sex Pics", el cual se encontraba alojado en el servidor de IRC, Undernet" diversos usuarios ofrecían archivos de pornografía infantil, lo que llevó a la localización a partir de su dirección IP, de varios usuarios que, a través de "File Server" han compartido o puesto a disposición de los usuarios del canal anteriormente citado archivos de imagen y/o vídeo protagonizados por menores de edad, se solicita del Juzgado Decano de Instrucción de Madrid, solicitando que se librase Mandamiento Judicial dirigido a los proveedores de acceso a Internet (Aúna Telecomunicaciones y Compañía Telefónica de España S.A.U.), con el fin de que informasen de cuantos datos posean en orden a identificar a los usuarios de diversas direcciones IP, así como las líneas telefónicas desde las que se efectuaron las conexiones (folios 3 a 5),

siendo uno de ellos el usuario IR6279/F-Server de la dirección IP 81.34.106.196 y las impresiones referidas a dicho usuario las de los folios 12 a 15, y como expedido el referido mandamiento por el Juzgado de Instrucción 23 de Madrid (folios 29, 30 y 31), se informa por Telefónica España SAU, (folio 33), con fecha 22.4.2005, que los muestreos efectuados en la conexión interesada, se obtiene que la IP. 81.34.106.196 corresponde a una ADSL dinámica que inicia conexión a través de la línea telefónica 954.18.33.5, cuya titular corresponde a la madre del acusado con domicilio en.....

Las anteriores diligencias pueden ser consideradas de naturaleza objetiva, cuya ratificación deviene innecesaria, desde el momento en que no son sino el inicio de las actuaciones judiciales y de la obtención de las verdaderas pruebas de cargo, que la propia sentencia de forma exhaustiva valora en el Fundamento de derecho primero:

a) La diligencia de entrada y registro en el domicilio antes indicado en virtud del auto dictado por el Juzgado de Instrucción 3 de Sevilla de fecha 2.6.2005, en cuya acta levantada bajo la fe pública del secretario judicial se hace constar que se accede al ordenador y a los ficheros del acusado, imprimiéndose los archivos localizados en los que guardaba el material pornográfico de menores, con la firma del secretario y en presencia del acusado, e interviniéndose dos discos duros con números de serie 5013520X735510 y 3HROB77W que fueron sellados bajo la misma fe pública y en CD localizado en la habitación del acusado de contenido sexual y pornográfico con niños, reconociendo el acusado dicho contenido y su propiedad (folio 44).....

b) Las propias declaraciones del inculpado José María Brenes (folios 58 a 60) en la Jefatura Superior de Policía, Grupo de Delincuencia Tecnológica, asistido de letrado, en los que admitió haber realizado intercambio en la red Undernet....

c) El informe pericial 83PI/2005 de 11.11.2005, emitido por la Comisaría General de la Policía científica –Unidad Central de Identificación, Sección de Tecnología de la Imagen– , Grupo de Pericias informáticas, sobre la infracción existente en los dos discos duros intervenidos, y que llega a la conclusión de la existencia, especialmente en uno de ellos, el C, de una gran cantidad de material pedófilo y la transferencia a otros usuarios a través de Internet, utilizando la aplicación MIRC....".

C) Injurias y Calumnias - arts. 205 a 216.

D) Descubrimiento y revelación de secretos. Art. 197, subtipo agravado si la acción del descubrimiento lo es por los responsables de la seguridad de los ficheros telemáticos, informáticos, electrónicos, etc.

3. Atentados contra la Seguridad Nacional/Internacional

Delito de descubrimiento de secretos o el ciberterrorismo.

Ultima reflexión sobre estos tres grupos de delitos:

Se trata de delitos diversos, que atentan a distintos bienes jurídicos y que se encuentran dispersos en el Cpenal.

El único punto de conexión es la identidad del medio comisivo – la informática. Ello plantea nuevos problemas relativos a la autoría y a la competencia territorial a la que luego me referiré.

IV. DELITOS INFORMÁTICOS STRICTU SENSU

Según Juan José González Rus, delito informático en sentido propio es el cometido a través de un sistema informático y contra el sistema informático, ya contra los elementos lógicos –software– , o el soporte físico –hardware– .

Por lo tanto, delito informático *no* es equivalente a delito cometido a través de la informática.

Una modalidad de delito informático sería el sabotaje o difusión de virus en la red. Eso sería un delito de daños a lo que se uniría la afectación del almacenamiento de datos o tratamiento de la información.

Así pues los delitos informáticos estarían constituidos por los ataques a la propiedad industrial/intelectual informática y por el delito de daños informáticos.

Ataque a la propiedad intelectual informática: art. 270-3.

Ataque a la propiedad industrial –patentes– art. 270.

Delito de daños: art. 264-2º, que contempla tres tipos de daños: a los programas informáticos, a los documentos electrónicos y a los sistemas informáticos.

¿Estamos en presencia de un nuevo bien jurídico?

Desde la perspectiva del Código español, la respuesta es, a mi juicio, negativa, porque en definitiva, incluso en relación a estos delitos *strictu sensu* se está en presencia de delitos preexistentes –daños o delitos contra la propiedad intelectual o industrial– hoy por hoy no hay un nuevo bien jurídico autónomo y en relación a la estructura conducta típica modalidad dolosa y culposa, sujetos activos, *iter criminis* y penalidad, no parece que exista una autonomía, aunque es cierto que la información contenida en las redes, soportes o sistemas informáticos se considera ahora como un activo patrimonial tutelable mediante esta figura del delito de daños, daños que tienen un perfil más concreto que la figura genérica del art. 263 Cpenal.

El bien jurídico protegido es el patrimonio si bien éste a lo que no se traduce en un ingreso del bien en el patrimonio del agente causante. El objeto material se contrae a los datos, programas o documentos electrónicos contenidos en las redes o sistemas informáticos, es decir a los elementos lógicos, de ahí la previsión de una pena superior a la del tipo básico de daños, por la grave perturbación que estas actuaciones dañosas ocasionan en el normal funcionamiento de empresas públicas y privadas.

La conducta típica es destruir, alterar, inutilizar o dañar de cualquier otro modo, fórmula de cierre que trata de abarcar toda actividad dañosa.

Debe recaer la acción dañosa sólo sobre los elementos lógicos (software) sin que sea exigible un daño materialmente apreciable en el soporte (el hardware). Esta es la opinión predominante en la doctrina española (Romeo Casabona). Precisamente la especificidad de los daños informáticos es ésa, que son daños inmateriales. Además, si han causado daños a los soportes se estará en un delito del art. 263 y 264.1 a resolver a favor de este último en virtud del principio de especialidad. Si el daño recae sólo sobre el hardware se estaría en un delito de daños tipo básico del art. 263.

En relación a la exigencia de que los daños superen la barrera de las 50.000 ptas. cantidad que es el umbral del delito, en una primera aproximación parece claro que debe exigirse la vigencia de esa cuantificación, lo que puede plantear problemas por

las dificultades que pueden surgir a la hora de peritar el daño. En el caso de que los virus no destruyan, dañen o inutilicen los programas, sino tan sólo causen una incomodidad al usuario de forma temporal, *no* se estaría en un delito de daños. Sería el caso de los bloqueos y ataques de duración temporal.

V. CUESTIONES SOBRE LA PERSECUCIÓN PENAL DE LOS DELITOS INFORMÁTICOS O COMETIDOS A TRAVÉS DE LA INFORMÁTICA

Como reflexión inicial que colorea y ofrece un común denominador en toda esta materia de derecho e informática, hay que decir que la Sociedad de la Información, las nuevas tecnologías han acentuado la desmaterialización del derecho.

El antiguo paradigma de la escritura sobre el papel, se ha transformado en el paradigma de la información digital y qué duda cabe que Internet ha acelerado la desmaterialización del derecho, el *"cuerpo"* de las cosas se ha hecho inmaterial, si se quiere virtual. No es un hecho nuevo pero evidentemente se ha acentuado en la Sociedad de la Información. Como afirma el profesor Trazegnies Grande el inicio de la desmaterialización del derecho se inicia con la apariencia del dinero, con el papel moneda que no tiene un valor en sí mismo, es sólo papel pero que tiene un valor económico por un convencionalismo universal, de igual modo que el concepto de lugar se relativiza. Por Internet como dice Reyna Alfaro circulan grandes cantidades de información digitalizada que tienen un contenido jurídico y económico indudable, y esta nueva realidad exige nuevos enfoques y ajustes en muchos aspectos de naturaleza penal y procesal penal.

Una breve referencia sobre estos problemas:

1. Competencia territorial

Se plantean problemas en orden a determinar el lugar de comisión del delito, ya que el autor está en un lugar, la víctima en otro, el hecho delictivo en un tercero y así sucesivamente. Ello puede dar lugar a una discusión de competencia territorial que sólo produce demoras y dilaciones en la tramitación de la causa.

La propia Sala II del Tribunal Supremo en reiteradas ocasiones ha hecho referencia al relativismo con que deben ser analizadas las cuestiones de competencia territorial porque, en definitiva, todos los jueces implicados tienen la misma competencia objetiva.

Precisamente, para evitar la proliferación de cuestiones de competencia, el Pleno no Jurisdiccional de la Sala II del Tribunal Supremo en reunión de 3 de Febrero de 2005 tomó el acuerdo de que *"....el delito se comete en todas las jurisdicciones territoriales en las que se haya realizado algún elemento del tipo, en consecuencia, el juez de cualquiera de ellas que primero haya iniciado las actuaciones, será, en principio competente para la instrucción de la causa...."*.

Con ello, se consagra la vigencia del Principio de Ubicuidad como criterio decisivo para evitar estériles cuestionamientos entre jueces de idéntica competencia objetiva.

En tal sentido, se aplicó esta doctrina en el Recurso 20155/2006, Auto de 20 de Septiembre de 2006. Se trataba de una estafa cometida por Internet. De acuerdo con

el Principio de Ubicuidad se acordó que era competente el juez de Getxo nº 2 por ser el juzgado que primero inició la investigación, coincidente con el del domicilio de la víctima. Se trataba de la compra de unos sintonizadores por Internet, el domicilio del proveedor estaba en Zaragoza, habiendo efectuado la víctima con domicilio en Getxo el abono correspondiente en la c/c de la empresa estafadora.

2. Delincuencia transnacional

Los delitos cometidos a través de Internet, traspasan las fronteras y ponen en conexión/colisión diversos ordenamientos jurídicos de los varios países implicados en los que se cometen diversos elementos típicos del delito. Ello puede suponer el inicio de varias investigaciones *"nacionales"* por unos mismos hechos, de lo que se deriva la conveniencia, más bien necesidad, de un único enjuiciamiento que abarque la totalidad de hecho delictivo aunque hayan existido diversos escenarios territoriales, con ello, además de evitar duplicidades y eliminar dilaciones, se evitan roces con el principio *non bis in idem.*

Un reciente ejemplo de unificación de investigación judicial a favor de aquello que está en mejores condiciones de llevarlo a cabo la tenemos en el caso del naufragio del *"Prestige*", en el que se aperturaron diligencias en Francia, que se han unido a la investigación efectuada por el Juzgado de Corcubión, que de este modo va a investigar todas las consecuencias producidas, y paralelamente, se concluirá con un único enjuiciamiento por parte de la Audiencia Provincial de A Coruña.

En sintonía con la aparición de una potente delincuencia transnacional, y como consecuencia de la concepción de la Unión Europea como un espacio de libertad, seguridad y justicia, los estados miembros singularmente a partir de los sucesos del 11-S en Nueva York, han centrado sus esfuerzos en potenciar las investigaciones criminales en la lucha contra la delincuencia organizada con tres fuentes concretas: tráfico de drogas, tráfico de seres humanos y terrorismo. Estimo que ello no impide la ampliación a otras figuras delictivas como las denominadas delitos informáticos. De hecho en el Informe explicativo del Convenio de 2000, sobre asistencia judicial en materia penal, en referencia al Convenio Europeo se cita expresamente el delito informático entre el listado de delitos que allí se relaciona.

Uno de estos instrumentos ha sido la creación de los equipos conjuntos de investigación, que ya aparecen recogidos en el Tratado de la Unión Europea así como en el Convenio relativo a la asistencia judicial en material penal el 29 de Mayo de 2000.

La finalidad es la de crear en el ámbito de la Unión Europea un instrumento específico y vinculante que permita a los estados llevar a cabo acciones coordinadas y concertadas a través de investigaciones conjuntas que se desarrollen en el territorio de dos o más estados.

Se trata de la puesta en funcionamiento de un instrumento al servicio del proceso, de carácter multilateral y transnacional que introduce nuevas pautas y modelos en la persecución criminal.

La Ley 11/2003 de 21 de Mayo de 2003 reguló estos equipos conjuntos de investigación. Excede en este trabajo un estudio de la Ley, me referiría a dos aspectos: a) en relación a la legislación del país que debe respetar, se dice en la Disposición Adi-

cional Primera, que esa legalidad está representada por la del país en el que vaya a actuar el equipo conjunto, y b) en la Disposición Adicional Tercera se prevé que se puedan comunicar informaciones a las policías autónomas cuando la misma sea conveniente para el ejercicio de las competencias que tienen encomendadas en los respectivos Estatutos de Autonomía.

Parece claro que en el futuro estos equipos conjuntos pueden y deben ocuparse del cibercrimen, dada su esencial estructura transnacional.

3. Investigación rápida

Los delitos de naturaleza informática tienen unas penas relativamente cortas, alrededor de tres años de prisión. Defraudaciones informáticas, art. 225: hasta doce meses de prisión, hurto de tiempo informático, el mismo. Daños informáticos 264: hasta tres años de prisión, Propiedad intelectual/industrial, arts. 270-273: hurto de dos años de prisión, publicidad engañosa, art. 282, hasta un año. Distribución de material informático, art. 186: hasta dos años. Ciertamente en caso de pornografía infantil las penas son superiores (art. 189), revelación secretos de empresa, art. 278 y siguientes, hasta dos años, etc. etc., que generalmente están afectados por un plazo de prescripción de tres años –art. 131– , por lo que resulta necesario que la investigación se inicie con prontitud.

4. Problemas de autoría

Se concretan en la individualización de las conductas atribuibles a las personas concernidas, y en este sentido cobran especial interés los servidores de Internet, pues va a ser, a través de ellos, a través de la información que puedan facilitar, como se podrá llegar a las personas penalmente responsables, ya que tales servidores actúan como técnicos intermediarios del proceso de conversación o comunicación, siendo frecuente la aparición de asociaciones criminales lo que puede justificar las agravaciones específicas de organización. Al respecto me remito a la jurisprudencia de la Sala II antes citada.

En relación a la responsabilidad de las personas jurídicas, veremos que el Convenio Europeo sobre delincuencia informática apuesta decididamente por la posibilidad de estimar los responsables criminalmente.

En España, hoy por hoy no es posible y en este sentido seguimos siendo tributarios del principio *"societas delinquere non potest"*. Por ello es preciso extraer toda la potencialidad del art. 31 Cpenal.

No obstante se preludia en el propio Cpenal 1995 un posible cambio en la medida que en algunos artículos, tal vez por un lapsus, se acuerde la imposición directamente a la organización de una pena de multa. Así en el art. 369-2º podemos leer *"....en los casos previstos..... se impondrá a la organización, asociación o persona titular del establecimiento una multa...."*.

Más aún, en la proyectada reforma del Cpenal se apuesta por la responsabilidad de las personas jurídicas.

En la Exposición de Motivos del proyecto se puede leer:

"....Muy claro ha de quedar entendido que esa responsabilidad no pretende ni puede sustituir, ocultar, empañar, o diluir la de las personas físicas. El sistema que se presenta tiene unas características marcadas, cuya primera condición es no reducir la responsabilidad de la persona jurídica al papel de simple pagadora de la multa impuesta a los administradores, respuesta llena de dificultades procesales que venía dando el párrafo segundo del artículo 31, que por eso se suprime. La responsabilidad de las personas jurídicas se concibe como propia aunque nacida de los delitos cometidos, por cuenta o en provecho de las mismas, por las personas físicas que las gobiernen o por quienes, estando sometidos a la autoridad de esas personas físicas realicen los hechos porque así se les indique o por no haberse ejercido sobre ellos el debido control, prescindiendo de la específica concreción y medida de la responsabilidad penal de los subordinados, que no atañe a la de la persona jurídica. La fuerza del factor humano en la configuración de la imputación del hecho a la persona jurídica permite, además, vencer adecuadamente la objeción referente a su llamada incapacidad de culpabilidad o de conducta dolosa o imprudente, pues esas dimensiones personales y subjetivas continúan residenciadas en la persona física.

Como es lógico, esas penas imponibles a las personas jurídicas han de ser modulables: gravemente desigual sería la regulación de la responsabilidad penal de éstas si, como acontece con la de las personas físicas, no se previera también un régimen de aminoración o agravación de esa responsabilidad. A tal fin se establecen una serie de causas de atenuación que giran en esencia sobre la valoración positiva de la reparación del daño y de la adopción de medidas eficaces para prevenir los que en el futuro pudieran causarse de ellas. La agravación, lógicamente, se produce cuando las conductas delictivas se repiten....".

Consecuentemente en el texto articulado del Proyecto, en el art. 33 se añade un nuevo apartado, el 7º, relativo a las penas aplicables a las personas jurídicas, y se añade un nuevo art. 31 bis. en el que se dice que la responsabilidad de las personas jurídicas, que *no* excluye la individual, sino que la viene a completar.

5. Identidad de los perjudicados

Es frecuente que este medio comisivo afecte a múltiples perjudicados residentes en diversos territorios incluso de distintos países, por ello puede tener incidencia la estructura del delito continuado versus delito/masa con aplicación del art. 74, sin perjuicio de la concreta precisión que existe en casos concretos, como es el caso de la agrupación delictiva prevista en el art. 189-3º en supuestos de pornografía infantil.

6. Importancia de la prueba pericial

Se trata de una delincuencia sofisticada, que paralelamente exige de la Policía Científica la existencia de cuerpos especializados, como ocurre con el Departamento de Delitos Telemáticos de la Guardia Civil y la Brigada de Investigación Tecnológica de la Policía Judicial, cuyos informes, como ocurre con todos los de la Policía Científica gozan, *prima facie* de una presunción de veracidad y de neutralidad por contar con todas las garantías técnicas y orgánicas, lo que no impide el derecho del inculpado a contradecir estas pruebas y a su impugnación.

En relación a la impugnación de tales informes periciales me remitiré al Acuerdo de Pleno no Jurisdiccional de 21 de Mayo de 1995, ratificado en el Pleno de 23 de Febrero de 2001, de la Sala II del Tribunal Supremo, según los cuales:

"....Siempre que exista impugnación manifestada por la defensa, se practicará en el juicio oral, rechazando la propuesta que mantiene que si la impugnación no se refiere al contenido de la pericial sino que se refiere a presupuestos objetivos de validez, que se constata que concurrieron, no sería causa de impugnación....".

7. Importancia de los Registros Domiciliarios

De ordinario los ordenadores se encuentran en domicilios particulares o en establecimientos públicos, empresas, despachos profesionales, cibercafés, etc.

Al respecto hay que recordar, que según la LECriminal, art. 546, hace falta mandamiento de entrada y registro de domicilios particulares y edificios públicos, bien que la protección constitucional del domicilio, según el art. 18-2º de la Constitución aparece reservado al domicilio de las personas físicas, y en tal caso, hay que recordar que así lo tiene declarado la STC 69/99 de 26 de Abril *"....el núcleo esencial del domicilio constitucionalmente protegido es el domicilio personal y familiar...."*, y como recuerda la STEDH de 16 de Abril de 2002, hay países de la Unión Europea que no reconocen inviolable el domicilio de las personas jurídicas.

En todo caso, por lo que se refiere a los "cibercafés" como establecimientos abiertos al público, no exigen mandamiento judicial de conformidad con el art. 557 LECriminal. Ahora bien, en cuanto la intervención policial concierna a las comunicaciones privadas que en esos lugares efectúan los clientes, las mismas tienen la protección del art. 18-3 de la Constitución, por lo que la intervención de los ordenadores exigirá la autorización judicial motivada.

VI. EL CONVENIO EUROPEO SOBRE DELINCUENCIA INFORMÁTICA. BUDAPEST 20 DE NOVIEMBRE DE 2001

En su preámbulo se justifica su existencia por la necesidad de impulsar una política penal común. Se trata de que la sociedad internacional se dote de un instrumento internacional válido para la lucha contra el cibercrimen mediante la adopción de una legislación apropiada y de mejora de la cooperación internacional.

Se describen las diversas modalidades de criminalidad informática en el título II, agrupadas en cuatro categorías:

1) Infracciones contra la confidencialidad, la integridad y la disponibilidad de datos y sistemas informáticos, y dentro de ellas se describe el acceso ilegal, la interceptación ilegal, el atentado a la integridad de los datos y del sistema, y el abuso de dispositivos.

2) Las infracciones informáticas dentro de las que se encuentran la falsificación informática y el fraude informático.

3) La pornografía infantil, entre la que se encuentra la producción con vistas a su difusión en la red, el ofrecimiento opuesto a disposición de pornografía infantil, la difusión o transmisión, y el hecho de procurarse o procurar a otro pornografía infantil y, finalmente, la posesión de pornografía infantil o su almacenamiento.

Asimismo el Convenio establece el ámbito de la pornografía con dos delimitaciones: a) se entiende por pornografía infantil a todo material pornográfico que represente de manera visual a un menor realizando un comportamiento sexual explícito, o

a un mayor realizando con menor un comportamiento sexual explícito, o imágenes realistas que representen a un menor realizando un comportamiento sexual explícito y b) la segunda limitación establece la edad para considerar a una persona menor, la que se fija en 18 años con posibilidad de rebajarlo hasta los 16 años, lo que no deja de ofrecer censura ya que si el disfrute pleno de derechos civiles –la mayoría de edad– se fija a los 18 años, es un contrasentido que se les puede considerar mayores a los efectos de la represión de la pornografía a partir de los 16 años.

4) Contra la propiedad intelectual y conexos.

En el campo procedimental se establecen unas reglas para facilitar el desarrollo de las investigaciones y que representan unas nuevas fórmulas de colaboración judicial. Se solicita de los estados firmantes que adopten las medidas legislativas necesarias para lograr la efectividad de la Convención y a tal fin se pide que los Estados velen por la conservación rápida de los datos almacenados en los servidores, que se comuniquen los datos relativos a los abonados a las autoridades en relación a las conductas descritas a petición del estado requirente, al registro y comiso de los datos almacenados, a la obtención de los datos concernidos en tiempo real y la interceptación de tales datos en tiempo real.

Se hace una especial referencia a la necesidad de conciliar la eficacia y efectividad del Convenio con los derechos, su respeto, de acuerdo con el Pacto Internacional de Naciones Unidas de 1966 y el Convenio Europeo de 1950.

Textualmente, el art. 15 que es el que se refiere al campo de las garantías, textualmente dice:

> *1. Cada Parte se asegurará de que la instauración, puesta en funcionamiento y aplicación de las facultades y procedimientos previstos en la presente sección queden sujetos a las condiciones y garantías previstas por el derecho interno de cada una de las Partes, con la observancia de una protección adecuada de los derechos humanos y libertades, especialmente de los derechos derivados de las obligaciones asumidas en aplicación del Convenio para la protección de los derechos humanos y libertades fundamentales del Consejo de Europa en 1950 y del Pacto Internacional de derechos civiles y políticos de las Naciones Unidas en 1966 o en otros instrumentos internacionales aplicables relativos a los derechos humanos, y que deben integrar el principio de proporcionalidad.*
>
> *2. Dichas condiciones y garantías incluirán, entre otras y siempre que sea posible atendiendo a la naturaleza de la facultad o procedimiento de que se trate, la supervisión judicial o similar supervisión independiente la motivación que justifique la aplicación, la limitación del ámbito de aplicación y la duración de la facultad o del procedimiento de que se trate.*
>
> *3. Las Partes evaluarán la repercusión de las facultades y procedimientos de esta Sección sobre los derechos, responsabilidades e intereses legítimos de terceros, como exigencia derivada del interés público y, concretamente, de una correcta administración de justicia.*

En materia de grados de ejecución y participación delictiva, el Convenio insta a los Estados parte a que sancionen también el delito en tentativa y la conducta del cómplice *"….siempre y cuando sea cometida* (su acción) *intencionadamente…."*, lo que es obvio porque la complicidad no se contempla si no es con conocimiento y consentimiento de que se está ayudando de forma no relevante al proyecto criminal del autor.

En materia de autoría es importante la precisión del art. 12 que prevé la responsabilidad de las personas jurídicas.

En lo referente a las sanciones, el art. 13 exige que *"....sean efectivas, proporcionadas y disuasivas comprendiendo penas privativas de libertad...."*, y en relación a las personas jurídicas prevé la imposición de sanciones y medidas penales o no penales, también de manera efectiva, con expresa referencia a las sanciones pecuniarias.

Finalmente el art. 23 se refiere a los principios generales relativos a la cooperación, en los siguientes términos:

> *"....Las partes cooperarán, de conformidad con las disposiciones del presente capítulo y mediante la aplicación de los instrumentos internacionales relativos a la cooperación internacional en materia penal, acuerdos basados en la legislación uniforme o recíproca y en su propio derecho interno, lo más ampliamente posible, con la finalidad de investigar los procedimientos relativos a las infracciones penales sobre sistemas y datos informáticos o para obtener pruebas electrónicas de una infracción penal...."*.

VII. REFORMA ANUNCIADA DEL CPENAL

En cumplimiento de la Decisión Marco 2005/222/JAI de 24 de Febrero de 2005, relativa a los ataques contra los sistemas de información, se prevé la incorporación de un nuevo párrafo al art. 197 Cpenal para sancionar las violaciones de privacidad o reserva de datos contenidos en los sistemas informáticos. Se trata de la tipificación de los actos invasivos de la privacidad.

> *"3. El que por cualquier medio o procedimiento y vulnerando las medidas de seguridad establecidas para impedirlo, accediera sin autorización a datos o programas informáticos contenidos en un sistema informático o en parte del mismo, será castigado con pena de prisión de seis meses a dos años"*.

Se prevé como tipo agravado la comisión de esta conducta –y las demás del mismo artículo– , por miembros de una asociación criminal.

A modo de última reflexión, se puede decir que el medio informático, Internet, no es culpable de la creación del cibercrimen, asimismo Internet no es controlable ni sometido a censura pero también hay que decir que Internet no es un mundo al margen de la Ley.

La Ley penal, frente al nuevo mundo de la información y de las redes informáticas está en una doble tensión. Por un lado, este medio ofrece nuevos campos a la delincuencia, pero por otro, también la Ley penal va a beneficiarse de estas nuevas tecnologías, singularmente en el campo del proceso y de la investigación, y desde la perspectiva sustantiva, también la Ley penal va a incidir en esta nueva situación, de suerte que ese mundo no es un mundo al margen de la Ley y del derecho penal.

BIBLIOGRAFÍA CONSULTADA

MATA Y MARTÍN, Ricardo. "Criminalidad Informática: una introducción al cibercrimen". *Actualidad Penal*, año 2003, número 36.

ORTS BERENGUER y ROIG TORRES. "Delitos Informáticos y Delitos Comunes cometidos a través de la Informática". Tirant lo Blanch.

REYNA ALFARO, Luis Miguel. "La criminalidad informática: cuestiones para una reflexión inicial". *Actualidad Penal*, año 2002, número 21.

SÁNCHEZ BRAVO, Alvaro. "El Convenio del Consejo de Europa sobre Cibercrimen". *Diario La Ley* nº 5.528, 22 de Abril 2002.

SÁNCHEZ GARCÍA DE PAZ, Isabel y BLANCO CORDERO, Isidoro. "Problemas de Derecho Penal Internacional en la persecución de delitos cometidos a través de Internet". *Actualidad Penal*, año 2002, número 7.

USTARAN, Eduardo. "Pornografía en Internet: una respuesta legal". *Diario La Ley*, 1977, Tomo I.

VELASCO NÚÑEZ, Eloy. "Aspectos procesales de la investigación y de la defensa de los delitos informáticos". *La Ley*, nº 6.506, 16 Junio 2006.

VARIOS AUTORES. "Delitos contra y a través de las nuevas tecnologías. ¿Cómo reducir la impunidad?". *Cuadernos de Derecho Judicial* C.G.P.J. Centro de Documentación-2006.