DERECHO PENAL Y NUEVAS TECNOLOGÍAS : PANORAMA ACTUAL Y PERSPECTIVAS FUTURAS

Dra. Esther Morón-Lerma (*)

1. – Escenario del debate : de nuevo, libertad « versus » control

Resulta ya un lugar común reconocer el carácter multidireccional de las nuevas tecnologías de la información y adoptar, por tanto, una perspectiva interdisciplinar (jurídica, sociológica, económica, psicológica) en su análisis o estudio. En este trabajo, corresponde afrontar algunos de los múltiples interrogantes que se suscitan desde la perspectiva penal y político-criminal.

Esa multidisciplinariedad caracteriza las infopistas de la información y, en particular, la red Internet. La repercusión de la revolución digital alcanza prácticamente a todos los sectores sociales. Las redes se articulan como ámbito de intercomunicación personal (correo electrónico, chat), como rápido modo de acceso a todo tipo de información y amplio escenario de ocio (cibernavegación, foros de discusión, grupos de noticias), como instrumento y entorno laboral (videoconferencia, teletrabajo) y como contexto de negocios y relaciones económicas (mercado virtual) ([1]). De ahí la diversidad y pluralidad de cuestiones concitadas ante esta generalizada implantación de Internet : aspectos técnicos de seguridad, problemática jurídica general acerca de la tutela de datos personales que circulan internacionalmente, intervención e interrelación de los distintos sectores del ordenamiento jurídico (civil, administrativo, penal), reglamentación del tráfico jurídico en ese mercado, responsabilidad de los operadores de telecomunicación y prestadores de servicios, etc.

(*) Profesora de Derecho Penal. Universidad Autónoma de Barcelona (España) esther.moron@uab.es

([1]) Para un análisis de las propiedades o cualidades « mediáticas » de Internet, como medio de comunicación, de información, de memorización, de producción, de comercio e intercambio, de ocio y entretenimiento y de interacción, vid. J. Echeverría, 1999 : 52 ss. Como afirma el citado autor, las tecnologías que posibilitan el tercer entorno (Internet es su expresión más desarrollada) pueden simular los escenarios de interrelación típicos del primer o segundo entorno (jardines, estanques, casas, oficinas, plazas, ciudades) y pueden también construir escenarios nuevos (J. Echeverría, 2000:96).

Se trata, pues, de un amplio elenco de cuestiones, que, aunque trascienden, con mucho, la estricta disciplina del derecho penal (F. Morales, 2001:115), deben ser tenidas en cuenta en las soluciones o propuestas que el derecho penal (de los diversos países) ofrezca, si se quiere lograr un marco jurídico sometido a criterios de eficacia y racionalidad, que brinde verdaderas garantías a todos los internautas o usuarios de la red.

En el actual y convulso estado de las cosas, resulta imposible emprender un análisis jurídico sobre la cibercriminalidad, sin reseñar previamente algunos factores que sobrevuelan e inciden notablemente en dicho análisis, de los que, en este momento, simplemente, interesa destacar dos. El primero de ellos reside en la propia especificidad de Internet, de estructura anárquica, caótica y descentralizada y el segundo, en el profundo impacto y alarma social que las modernas tecnologías de la información todavía siguen suscitando. Y empezando por este último conviene formular algunas consideraciones.

Ciertamente, Internet se ha consolidado como valiosísimo instrumento de comunicación entre la comunidad internauta y, por tanto, también entre los delincuentes (o ciberdelincuentes, como suele denominárseles) ([2]). En este sentido, especialmente a tenor de los acontecimientos ocurridos el 11-S de 2001, se ha visto potenciada la magnitud de Internet, como espacio, no sólo ya de progreso y avance, sino también de peligros ([3]).

Es decir, la incertidumbre engendrada por un avance tecnológico tan notable y la influencia de una opinión pública, en ocasiones, muy alarmada, han contribuido a que se haya generalizado una sensación de intranquilidad en un momento de progreso y de primado indiscutible de la técnica, que, sin embargo, puede ser utilizada por delincuentes y, en esa medida, quedar al servicio de fines criminales. Y ésta es la primera idea que procede subrayar, a saber, la creciente sensación de amenaza ante el posible abuso de la técnica por delincuentes.

([2]) En el tercer entorno, lo más frecuente es mantener reuniones virtuales de todo tipo. En lugar de videoconferencias entre imágenes físicas, se desarrollan conversaciones e interacciones a través de las máscaras digitales elegidas por cada intervieniente. Y aunque no es posible celebrar reuniones masivas, la actual tecnología sí permite que cien personas confluyan activamente en un mismo lugar virtual (J. Echeverría, 2000 : pp. 54-55).

([3]) Así lo ejemplifica, paradigmáticamente, el informe publicado por el FBI, su NIPC -Centro de Protección de la Infraestructura Nacional- , en noviembre de 2001, advirtiendo de que tecnologías como los *chats* de Internet (IRC), las páginas *web* basadas en tablones de anuncios y las cuentas de correo electrónico, permiten a grupos extremistas adoptar la estructura conocida como « leaderless resistance » (resistencia sin líder). En estos grupos, sus miembros pueden organizarse y gobernarse desde los *e-mails* o desde sitios *web* seguros y operar de un modo coordinado, sin que sus miembros tengan nunca que verse. Dichas herramientas permiten, pues, que miembros dispersados ampliamente por todo el mundo puedan compartir información de cara a un objetivo común, a veces, violento.

Por tanto, como se observa, a diferencia de lo que ocurría en los comienzos de Internet, momentos en los que sólo se advertían sus extraordinarias ventajas y en los que se reivindicaba la autorregulación a cargo de los propios internautas, actualmente la situación es muy distinta. Se asocia la Red a una nueva fuente de riesgos, que está conduciendo a que se reclame, con urgencia, una mayor intervención jurídica.

Además, lo novedoso del fenómeno Internet (y retomo ahora el primero de aquellos factores indicados), su especificidad como medio de comunicación (interpersonal y de masas, en el que, a su vez, el receptor puede convertirse en emisor de contenidos) junto con la consiguiente dificultad de aprehensión normativa del fenómeno, constituye otro de los factores que motiva esa demanda de tutela penal. Y este efecto amplificador se observa, por ejemplo, en la relevancia jurídico-penal que se pretende otorgar a ciertas conductas meramente nocivas o en el grado de responsabilidad exigible a los operadores de las redes.

En refrendo de lo anterior pueden citarse algunas propuestas legislativas de carácter internacional, que suponen una clara moralización de conductas sexuales, como ocurre con la regulación de la pornografía infantil en el Convenio europeo de Cibercriminalidad ([4]), exigiéndose responsabilidad no ya al propio autor de posibles contenidos ilícitos (esto es, al que los crea y oferta) sino al consumidor de dichos datos (es decir, el que los demanda); o soluciones de ámbito comunitario, como la Propuesta de Decisión-Marco del Consejo europeo, 19.04.2002, relativa a los ataques de los que son objeto los sistemas de información, que prevé penas de prisión de uno a cuatro años para dichas conductas (en las que se incluyen los accesos inconsentidos) o la Directiva 2002/58/CE del Parlamento europeo y del Consejo, de 12 de julio de 2002, que faculta a los Estados miembros a obligar a los prestadores de servicios a conservar datos de tráfico durante un tiempo limitado que delega al arbitrio de los Estados.

Asimismo, cabe mencionar ciertas iniciativas emprendidas unilateralmente por algunos Estados, como, pongamos por caso, Gran Bretaña, en el que a través de la extensión de la *RIPA* (*Regulation of Investigatory Powers Act*), se obliga a los ISP con más de 10.000 usuarios a estar preparados para interceptar correo electrónico, faxes y datos de navegación de sus clientes, cuando se lo pidan las fuerzas de la ley – previsión en vigor desde el 1 de agosto de 2002 ([5]) – y que pretende legitimar a ciertos funcionarios de la Administración Pública (ministerios, todas las corporaciones locales y diversos servicios públicos) a requerir datos, sin auto-

([4]) Convenio europeo sobre cibercriminalidad [Budapest, 23.XI. 2001].

([5]) Así, vid. http://www.baquia.com, de 12.06.2002 y Ciberpaís, jueves 15 de agosto 2002, p. 5.

rización judicial, a los ISP – previsión esta última cuya discusión en el Parlamento se halla pospuesta ([6])--; o las iniciativas de Francia o de Suiza que, en términos análogos, prevén la obligación a cargo de los ISP de conservar datos de los clientes durante un año – en el caso de Francia-- o seis meses – según la propuesta suiza--. Por último, en el marco del derecho norteamericano, se observan, también, recortes de garantías y, en algunos casos, indiscriminadas restricciones de derechos, como ocurre en gran parte de las medidas adoptadas para combatir el terrorismo ([7]).

Esa demanda de mayor intervención jurídica puede producir una tendencia expansiva que complique el arbitrio – *per se*, difícil – de tutela de todos los intereses que deben protegerse en Internet y que, además, en esa constante tensión entre las garantías para los derechos y la eficacia en la lucha contra la delincuencia, acabe otorgando primacía a la seguridad pública y al control.

En suma, como indicaba al comienzo del presente trabajo, la propia singularidad de Internet junto a esa creciente incertidumbre social, repercuten en casi cualquier reflexión jurídica que se aborda sobre la red. Así pues, la constatación del influjo de esos factores metajurídicos constriñe, en este caso, a la adopción de una especial cautela.

No obstante, y observando esa aconsejable prudencia, sí pueden darse por zanjadas algunas cuestiones.

En primer lugar, y enlazado con esa necesidad de tutela en la red, debe aceptarse que en Internet coexisten bienes susceptibles de entrar en liza. Así ocurre, por ejemplo, con la libertad de expresión e información-- ejercida en este caso a través de medios telemáticos-- y derechos individuales, entre los que puede hallarse el derecho a ser tratado como un ser humano igual a los demás, el derecho al honor, e incluso intereses de carácter colectivo, como el modelo de convivencia plural y multicultural del que parte la Constitución.

Por tanto, aunque la red ha sido reivindicada como « *medio profundamente democrático* », que hace posible la comunicación de muchos puntos a muchos puntos (J. Barnes, 1997:255), como medio *no invasivo*, puesto que se encuentra ligado a los pasos concretos de los usuarios en

([6]) Así, vid. http://www.5dias.com/especiales/suplementos/5red/20020622/14mensajes.htm.

([7]) Entre las medidas adoptadas para combatir el terrorismo, destaca la profusa normativa aprobada al efecto (*USA Patriot Act*, *Online Personal Privacy Act*, *Cyber Security Enhancement Act*, además del controvertido programa Carnívoro), en la que adquieren una especial relevancia las disposiciones destinadas a la lucha contra el cibercrimen y/o crimen organizado *online* y uno de cuyos denominadores comunes se cifra en la ampliación de las prerrogativas concedidas a las autoridades para vigilar las comunicaciones a distancia; véase, más exhaustivamente, E. MORÓN, 2002:143 ss. Para un análisis de la *USA Patriot Act*, vid. J. PERARNAU, 2002 : pp. 136-139.

la selección de los contenidos o servicios a disfrutar, como *medio económico* y como medio *no escaso*, no resulta admisible un ejercicio irrestricto de la libertad de expresión o de comunicación a través de Internet, sino que, al igual que ocurre en otros medios, la libertad de expresión debe sufrir ciertas limitaciones (L. Picotti, 2000:216). En concreto, las limitaciones que impone la necesaria tutela de otros bienes y derechos en la red, según se pormenorizará más adelante.

Y, precisamente, porque conviven bienes que entran en conflicto, otra de esas cuestiones – exentas ya de controversia – radica en la necesidad de regulación de Internet y del establecimiento de un control sobre la misma, que contribuya a preservar esos bienes confrontados, debiendo exigirse que sea ejercido por instituciones democráticas.

Así que, en la articulación de ese control – que aflora y traslada a la red el viejo debate entre derechos individuales e intereses públicos – deberá tenerse en cuenta la especificidad de Internet y las dificultades existentes para poder llevar a cabo una eficaz investigación e identificación de los delitos cometidos en la red, problemas a los que sólo podré referirme, en esta ocasión, muy brevemente.

Como puede deducirse, el control directo sobre los autores materiales de los ilícitos en la red – para ser descubiertos y perseguidos como autores de contenidos ilícitos – resulta extremamente complejo. De una parte, los internautas pueden esconderse bajo el anonimato (identidades digitales, *remailers*, cibercafés, etc.) o suplantar identidades ajenas (*spoofing*), enmascarando la auténtica dirección de origen y permitiendo desdibujar el origen geográfico del sistema informático utilizado como instrumento para la ejecución del delito ([8]); existe además multiplicidad y dispersión de accesos (Internet se caracteriza por su estructura anárquica o caótica, en forma de « gran telaraña mundial », como indica la denominación de una de sus principales aplicaciones, la www; de modo que el cibernauta que comete un ilícito puede hacer el ataque desde varios ordenadores interpuestos que dificulten y demoren el rastreo digital), por mencionar algunos de los posibles obstáculos materiales.

Pues bien, teniendo presente lo anteriormente sostenido, es decir, de una parte, la inquietud e incertidumbre social, la demanda de intervención jurídica y la consiguiente tendencia expansiva, pero, también, lo imprescindible de la regulación de Internet, de limitación de algunos

([8]) Como gráficamente expone Echeverría (J. ECHEVERRÍA, 2000:93-94), cada usuario que accede a un lugar digital dispone de la posibilidad de elegir una máscara en la guardarropía digital disponible, modificarla, imprimirle una gestualidad y voz específica y crear su propio *avatar* (monigotes electrónicos capaces de moverse, actuar e interrelacionarse con otras máscaras digitales en un mundo virtual tridimensional). Una vez construida una identidad específica, los visitantes de ese escenario virtual pueden comunicarse, moverse y manifestar sus sentimientos por medio de gestos y palabras.

bienes jurídicos para la tutela de otros y la necesidad de articulación de un control, procede analizar ya los diversos cauces jurídicos por los que, en la actualidad, discurre la depuración de responsabilidad en las redes telemáticas.

Y en el arbitrio de los posibles criterios en torno a la responsabilidad jurídica en Internet, resultan asumibles distintas metodologías de trabajo. Una de ellas conduce a examinar el modelo normativo existente, que, en este caso, se centraría, básicamente, en el estudio del código penal. Sin embargo, es preferible adoptar por ahora un segundo enfoque, cifrado en proporcionar algunas pautas que presiden el análisis jurídico en Internet, desde una doble perspectiva, es decir, atendiendo, en primer lugar, al tipo de contenidos que circulan en Internet y, posteriormente, a la forma en que pueden ejecutarse los ataques en la red.

2. – Responsabilidad por los contenidos que circulan en la red

Respecto a la responsabilidad por los contenidos que circulan en la red, únicamente se incidirá en un par de aspectos esenciales, que atañen a la necesaria distinción de contenidos en Internet y, una vez discernidos dichos contenidos, a la exigencia de responsabilidad a los prestadores de servicios, sólo respecto de algunos de esos contenidos.

2.1. – *Necesidad de distinción de contenidos en Internet*

Según lo indicado anteriormente, una de las notas características de Internet reclama la constante ponderación de bienes en conflicto, lo que suele acarrear la limitación de algunos de ellos. De modo que la represión penal, pongamos por caso, de posibles conductas xenófobas o racistas, intentará conciliar, con cierto equilibrio, los distintos valores confrontados en estos delitos : de un lado, libertad de expresión y de otro, derechos fundamentales, como el derecho a la igualdad o al honor; o, en el caso, por ejemplo, de la pornografía infantil, libertad de expresión y derecho del menor a la propia imagen, como manifestación del derecho a la intimidad (F. Morales, 2001, 122), formulado muy esquemáticamente.

Si conseguir ese equilibrio es ya difícil en la realidad analógica (prensa escrita, televisión, radiodifusión), resulta aún más complejo cuando el debate se traslada a la red, en la que siempre subyace una pugna, recrudecida tras lo ocurrido el 11-S, entre libertad y control.

En ese balance, que conduce a la necesaria restricción de algunos bienes, uno de los aspectos más controvertidos estriba en identificar y

seleccionar tales límites. Es decir, en los casos referidos de conflicto con la libertad de expresión, determinar cuál es la frontera o el umbral a partir del cual no resulta posible tolerar una opinión por lo que supone de amenaza para la paz social y la convivencia pacífica o de lesión de otros valores constitucionalmente garantizados y que, en mi opinión, deben reconducirse a derechos fundamentales.

En el logro de ese equilibrio de garantías, como primer paso, deviene indispensable distinguir entre los *contenidos dañosos o nocivos*, que no pueden considerarse por sí mismos lesivos de esos valores o intereses (derecho al honor, a la dignidad humana, etc.) – dependen de estándares culturales – y en los que no subyace, por tanto, la vulneración de un derecho reivindicable como límite y los *contenidos ilícitos*, que sí representan comportamientos atentatorios de aquellos derechos y que, en esa medida, suelen estar previstos como delictivos por las legislaciones internas de los países.

Y esa diferencia resulta trascendental, puesto que sólo los *contenidos ilícitos* deben ser combatidos – y, por tanto, controlados – desde lo público. Por el contrario, los *contenidos dañosos* reclaman una intervención privada a cargo de los propios usuarios (*software* de filtrado, señales acústicas o visuales, etiquetas de advertencia (9), como se verifica en otros medios de comunicación analógicos.

Por tanto, la primera conclusión inferible de todo lo expuesto se traduce en que la articulación de ese control-- que contribuye a proteger bienes confrontados-- sólo será reivindicable respecto de las comunicaciones con *contenido ilícito*.

2.2. – *Responsabilidad por los contenidos ilícitos*

Asumida la necesidad de control sobre tales contenidos, corresponde examinar, y abordo ya la segunda cuestión anunciada, el modo en que resulta ejercitable ese control. En realidad, debería verificarse análogamente al modo en que se lleva a cabo en el que podríamos denominar « derecho penal analógico », es decir, persiguiendo a los autores materiales del hecho. Sin embargo, se ha destacado ya la enorme dificultad material de poder llevar a cabo un control directo sobre los autores materiales de esas comunicaciones ilícitas en la red. A ello deben añadirse las divergencias jurídicas respecto a la interpretación de esos valores que entran en conflicto, como ocurre, por ejemplo, con el dis-

(9) Así, por ejemplo, la iniciativa lanzada recientemente, en EE UU, Canadá y Méjico, por Yahoo!, AOL y Microsoft, mediante la instalación de unas etiquetas de advertencia, en aquellas *web* cuyo contenido pueda ser perjudicial o dañino para los menores, permitiendo una selección personalizada más precisa que la de los actuales sistemas de filtrado (listas negras, que pueden anular *sites* inofensivos).

tinto contenido que se otorga a la libertad de expresión, en EE UU o Canadá y en los países de la Unión Europa. Dichas discrepancias imposibilitan, en ocasiones, llegar a acuerdos legislativos internacionales en la materia (así ha ocurrido en el Convenio europeo sobre cibercriminalidad, en el que no se ha incluido la exhibición o difusión de material de contenido racista y xenófobo) y provocan, como consecuencia práctica de tal disensión normativa, el alojamiento de las páginas *webs* con contenidos ilícitos (como los contenidos xenófobos o racistas) en servidores ubicados en países con legislaciones menos restrictivas, a modo de « paraísos informáticos » (E. Morón, 2002:128-129).

De ahí que esa enorme dificultad (potenciada por la complejidad técnica de la cibercriminalidad) en la investigación y persecución -*sucesiva*-- de los autores materiales haya determinado la necesidad de implicar, con finalidad *preventiva*, a los agentes que, profesionalmente, se encargan de prestar y gestionar el acceso y los servicios en la red. Sin embargo, constatada la repercusión de esa tendencia expansiva, también, en este ámbito, exigiendo una responsabilidad ilimitada, conviene, de nuevo, reflexionar con una adicional cautela acerca de cómo debe configurarse la responsabilidad de esos operadores por comunicaciones que, en realidad, no han creado. Al respecto, destacan tres o cuatro criterios generales que, a mi juicio, deben orientar cualquier propuesta jurídica (L. Picotti, 2000:217; E. Morón, 2002:133 ss.).

a) Los operadores de Internet son agentes intermediarios de la red, que cumplen una función jurídico-social y económica. Surgen como operadores imprescindibles, puesto que, a diferencia de lo que ocurre en otros medios, no hay una comunicación directa entre el punto de origen y destino. Por tanto, parece razonable implicar a tales profesionales mediante la imposición de ciertas obligaciones de control sobre los contenidos ilícitos que circulan en las redes telemáticas, precisamente para poder garantizar las legítimas exigencias de tutela en la utilización de Internet.

b) Ahora bien, en el momento de perfilar las obligaciones imponibles a estos operadores profesionales, debe tenerse en cuenta que no cumplen todos la misma labor. Es decir, en la medida en que Internet permite llevar a cabo diversas actividades (correo electrónico, navegación, participación en foros de debate o en chats, etc.), los operadores asumen también distintos roles en virtud del servicio que proporcionan y gestionan. De ahí que la delimitación de las obligaciones jurídicas de control de las comunicaciones y, eventualmente, de impedimento del acceso a la información, deba consagrar una responsabilización *diferenciada*, en atención a sus respectivas esferas de actividad y competencia. Lo que conduce a rechazar deberes de control o de supervisión genéricos o indiscriminados.

c) A partir de esa implicación diferenciada, el principio general reside en que los operadores de redes puedan ser considerados responsables de los contenidos ajenos siempre que concurran, fundamentalmente, dos requisitos : en primer lugar, que se tenga conocimiento de dichos contenidos y en segundo lugar, que sea técnicamente posible y exigible impedir la utilización por parte de terceros de dichos contenidos, es decir, que sea posible y exigible el bloqueo de la información. Desde luego, este segundo criterio es difícil de concretar y, al respecto, se sugieren una pluralidad de parámetros : la posibilidad técnica de la medida de control, la no interferencia con la circulación legal de datos, el alcance práctico de la eficacia impeditiva de la difusión de los contenidos penalmente ilícitos, que, en estos casos, suele ser escaso, puesto que los propios internautas establecen enlaces para que se pueda seguir accediendo a esos mismos contenidos.

Respetados esos criterios generales, la solución más oportuna discurre, a mi parecer, por la aprobación de normativa específica, de dimensión necesariamente supranacional, dada la naturaleza transfronteriza de este tipo de criminalidad, que persiga, como fin básico, la eficaz represión de los autores de contenidos penalmente ilícitos, pero que no por ello deje, sobre todo, conocida la dificultad de persecución de dichos autores, de proponer específicas obligaciones jurídicas de control, respecto de los operadores profesionales y de prever, en consecuencia, su sanción en caso de inoperancia.

En este sentido, debe señalarse la reciente aprobación de normativa europea [Directiva sobre el comercio electrónico ([10])] y la promulgación por los diversos países de la consiguiente legislación de transposición [así, en España, la Ley 34/2002, de 11 julio, sobre servicios de la sociedad de la información y de comercio electrónico (LSSICE)] ([11]), como primeros cauces de regulación de la responsabilidad de los prestadores de servicios en la sociedad de la información. A pesar de que no puede abundarse, en este momento, en el estudio de dichas soluciones normativas, cabe destacar que tanto la Directiva europea, que regula, en sus artículos 12 a 15, la responsabilidad penal de los prestadores de servicios intermediarios y que se corresponde, mayoritariamente, con lo previsto en los artículos 13 a 17 de la Ley española de servicios de la sociedad de la información y de comercio electrónico, por la que se transpone la

([10]) Directiva 2000/31/CE, del Parlamento europeo y del Consejo, de 8 de junio de 2000, relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular, el comercio electrónico en el mercado interior.

([11]) Puntualmente afectada por el contenido de la Ley 59/2003 de 19 de diciembre de firma electrónica y de la Ley 32/2003 de 3 de noviembre de telecomunicaciones (en particular, en el caso de esta última, en materia de prohibición de comunicaciones comerciales realizadas a través de correo electrónico o medios de comunicación electrónica equivalentes, derechos de los destinatarios de servicios y régimen sancionatorio).

citada Directiva, consagran, en lo esencial, los criterios generales expuestos con anterioridad ([12]).

En el ámbito penal, en cambio, el legislador interno español no ha incorporado ninguna previsión específica que recoja los estándares declarados en la Directiva europea sobre comercio electrónico y en la LSSICE, por ejemplo, de un modo análogo a lo establecido en el artículo 30 CP, para la prensa (J.J. López Ortega, 2002:119). De ahí que, por el momento, la depuración de responsabilidad penal de los prestadores de servicios reclama, como criterio esencial, la advertencia de dos situaciones generadoras de un régimen distinto. De una parte, los supuestos en que el prestador bien elabora (esto es, crea) la información bien desempeña un específico deber de control o vigilancia sobre ciertos contenidos ajenos que se introducen en la red, cuya punibilidad no resulta cuestionada. En estos casos, se responderá, a través de los cauces de la autoría, bien por los contenidos propios o bien en los supuestos en que se seleccionan los contenidos ajenos, excediéndose de la mera facilitación del servicio ([13]). Y, de otra, aquellos otros (alojamiento de datos o facilitación de enlaces o instrumentos de búsqueda), que ofrecen mayor controversia, en los que la imputación de los hechos discurrirá a través de la *participación*, siempre que concurran los requisitos anteriormente expuestos.

Concluido el primer punto de vista seleccionado-- en función de los contenidos--, se analizarán, a continuación, muy brevemente, diversos ilícitos vinculados a Internet atendiendo al modo de ataque y, especialmente, se hará hincapié en algunas de las conductas que suscitan mayor controversia, como son las conductas de *hacking* o de mero intrusismo informático.

3. – Responsabilidad por el modo de ataque en la red

Como se sabe, los ilícitos perpetrables a través de Internet no son reconducibles a una categoría única y homogénea. La proliferación y diversidad de formas que pueden adoptar los ataques contra los sistemas de información constituye una de las características de la cibercriminalidad.

([12]) Vid., ampliamente, E. Morón, 2002 : pp. 137-163.

([13]) Debe señalarse que, en ese último supuesto, como ha advertido ya la doctrina (J.J. López Ortega, 2002:116 y E. Morón, 2002:163), la acción del prestador será, por lo general, consecuencia de la infracción de un deber de cuidado en la selección de los contenidos, por lo que la exigencia de responsabilidad se verá limitada a los tipos penales que prevean la comisión imprudente.

3.1. – *Conductas lesivas de la privacidad informática*

Como primer grupo de supuestos, han surgido nuevos riesgos para la privacidad informática, ejemplificables, paradigmáticamente, en las conductas de monitorización digital, que se concretan en comportamientos de desigual gravedad.

I) En efecto, han aparecido formas de intromisión de la vida privada de los usuarios especialmente graves e insidiosas. Al respecto, baste citar el uso de « programas rastreadores » (*sniffers*), que, lanzados al ciberespacio, interceptan la información que circula por la red y permiten, por tanto, el control inconsentido e invisible del correo electrónico ([14]), así como el recurso a « programas espía » (*spyware*), que, introducidos en el terminal del usuario sin su consentimiento, acceden a datos, archivan información oculta o rastrean sus actividades. Estos ataques deben reputarse como graves agresiones a la privacidad y, por tanto, resultan comportamientos subsumibles, en la mayor parte de los casos, en los delitos contra la intimidad ([15]).

II) Otras conductas invasoras de la intimidad revisten menor lesividad, como ocurre con el empleo de los programas « chivatos » (*cookies*). Las *cookies* son subrutinas informáticas o archivos emitidos por un servidor de información, que se almacenan en el disco duro del ordenador visitante. Cuando el usuario visita de nuevo ese sitio *web*, los datos son reenviados al servidor proporcionándole información actualizada sobre el mismo. Con esta técnica, el servidor puede identificar al usuario cada vez que accede a él y memorizar todas las consultas efectuadas. El sucesivo envío de *cookies* y su conservación permite al emitente lograr una fotografía digital del internauta, conocer su dirección, gustos, preferencias o entretenimientos, pudiendo efectuar un rastreo completo de las actividades del usuario en la red (S. Muñoz, 2000:180). La proliferación de estas conductas – y las subsiguientes de envío de publicidad inconsentida- – ha provocado una respuesta normativa que reivindica la necesidad de que sólo se permita la utilización de tales dispositivos con fines legítimos y con el conocimiento de los usuarios afectados. Así, la Directiva 2002/58/CE, del Parlamento europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electróni-

([14]) Se trata de dispositivos destinados a « husmear » la información que viaja por una red informática, buscando una cadena numérica o de caracteres en los paquetes que atraviesan un nodo (D. Ferrandis, 2001:182).

([15]) El art. 197.1 CP español castiga al « que, para descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento (...) intercepte sus telecomunicaciones o utilice artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen o de cualquier otra señal de comunicación », con pena de prisión de uno a cuatro años y multa de doce a veinticuatro meses. Vid., ampliamente, F. Morales, 2002:72 ss.

cas ([16]), regula los supuestos en que dichos dispositivos ostentan un propósito legítimo (como el de facilitar el suministro de servicios de la sociedad de la información) ([17]), debiendo autorizarse su uso, siempre que se cumplan determinadas condiciones. De una parte, que se facilite a los usuarios información clara y precisa al respecto, para garantizar que están al corriente de la información que se introduce en el equipo terminal que están utilizando. De otra, que los usuarios dispongan de la posibilidad de impedir que se almacene en su equipo terminal un « chivato » (*cookie*) o dispositivo semejante. Por tanto, la Directiva europea obliga a que las *cookies* no puedan activarse sin que el usuario lo haya autorizado al menos en una ocasión ([18]).

III) Y, por último, deben mencionarse las conductas de *spaming*, que suelen proseguir a los ilícitos analizados y que consisten en el envío inconsentido de mensajes por correo electrónico a una multitud de desconocidos, ofertando la publicidad de un producto o de un servicio por razones puramente comerciales. Con esta práctica, cualquier buzón de correo electrónico puede ser saturado de mensajes comerciales no deseados e, incluso, un sistema informático entero puede verse bloqueado, si se ejecuta un programa para que se le envíen mensajes repetidos en cortos espacios de tiempo (S. Muñoz, 2000:145 y A. Téllez, 2001:85). Tal como se ha advertido, recientemente, se ha aprobado normativa específica, a nivel internacional y nacional, destinada a la regulación y prohibición del envío de publicidad masiva no solicitada.

a) A nivel internacional, la Directiva europea sobre el comercio electrónico ([19]), en su artículo 7, relativo a las comunicaciones comerciales no solicitadas, otorga libertad a los Estados miembros para optar entre el sistema *opt-in* o el *opt-out* ([20]). Se consagra, además, caso de que se

([16]) La Directiva 2002/58/CE deroga y sustituye a la Directiva 97/66/CE del Parlamento Europeo y del Consejo, de 15 de diciembre de 1997, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las telecomunicaciones.

([17]) Así, en el considerando (25), se declara que estos dispositivos « pueden constituir un instrumento legítimo y de gran utilidad, por ejemplo, para analizar la efectividad del diseño y de la publicidad de un sitio web y para verificar la identidad de usuarios partícipes en una transacción en línea ».

([18]) Según se establece en el cdo (25), la información sobre la utilización de distintos dispositivos que se vayan a instalar en el equipo terminal del usuario en la misma conexión y el derecho a impedir la instalación de tales dispositivos se pueden ofrecer en una sola vez durante una misma conexión y abarcar asimismo cualquier posible utilización futura de dichos dispositivos en conexiones posteriores.

([19]) Directiva 2000/31/CE, del Parlamento europeo y del Consejo, de 8 de junio de 2000, relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular, el comercio electrónico en el mercado interior.

([20]) Con arreglo al sistema *opt-in*, se exige la autorización o el consentimiento previo por parte del interesado para el envío de cualquier tipo de publicidad no solicitada a través de Internet. Por el contrario, bajo la fórmula del *opt-out*, el internauta debe manifestar su consentimiento para ser orillado o apartado de cualquier procedimiento de recogida de datos, inscribiéndose en una lista de exclusión voluntaria para no recibir comunicaciones comerciales.

elija esta última fórmula, el deber de garantizar que los prestadores de servicios que realicen comunicaciones comerciales no solicitadas por correo electrónico consulten regularmente las listas de exclusión voluntaria. Por el contrario, la Directiva 2002/58/CE, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas, consagra, en su artículo 13, el sistema *opt-in* o exigencia de consentimiento previo por parte del interesado para el envío de cualquier tipo de publicidad no solicitada a través de Internet. Se contempla la excepción de que, en caso de que el cliente haya proporcionado información a una empresa tras una relación comercial, ésta pueda introducirla en sus bases de datos. No obstante, el consumidor siempre puede acogerse al *opt-out* y solicitar la exclusión de la lista.

b) En el derecho interno, la respuesta normativa puede arbitrarse en torno a diversos cauces. Así en España, de una parte, la ley de protección de datos personales (LOPDP) ([21]) reclama, en su artículo 30, relativo al tratamiento de datos personales con fines de publicidad y de prospección comercial, la exigencia general de consentimiento del interesado ([22]). De otro lado, la Ley 34/2002, de 11 julio, sobre servicios de la sociedad de la información y de comercio electrónico (LSSICE), a través de la cual se articula la transposición al ordenamiento español de la Directiva europea de comercio electrónico, ha optado-- en sintonía con las recientes exigencias europeas (ex art. 13 Directiva 2002/58/CE) y en ejercicio del margen de libertad otorgado por la Directiva europea de comercio electrónico-- por el sistema más restrictivo del *opt-in*. El artículo 21 LSSICE, prohíbe, pues, el envío de comunicaciones publicitarias o promocionales por correo electrónico u otro medio de comunicación electrónica equivalente, que previamente no hayan sido solicitadas o expresamente autorizadas por los destinatarios de las mismas.

Ahora bien, según ha sido ya advertido por la doctrina (S. Muñoz, 2000:149; E. Morón, 2002:38-39), el carácter universal y transfronterizo de Internet requiere, imperiosamente, una ordenación mundializada de lo admitido y de lo prohibido en materia de publicidad, que permita uniformar los criterios. En la actualidad, es cada vez más frecuente la emisión, desde cualquier lugar del planeta, de comunicaciones electrónicas prohibidas en los lugares donde se reciben y difíciles de evitar y de reprimir.

([21]) Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

([22]) El artículo 30.1 LOPDP establece que « Quienes se dediquen a la recopilación de direcciones, reparto de documentos, publicidad, venta a distancia, prospección comercial y otras actividades análogas, utilizarán nombres y direcciones u otros datos de carácter personal cuando los mismos figuren en fuentes accesibles al público o cuando hayan sido facilitados por los propios interesados u obtenidos con su consentimiento ».

Concluido el análisis de esa primera esfera de nuevos riesgos para la privacidad informática, se abordará a continuación el examen particularizado de otras posibles formas que, bajo ese segundo punto de vista adoptado, pueden revestir los delitos en la red.

En efecto, atendiendo al modo de ataque, los ilícitos resultan también deslindables, entre otros criterios, en virtud de la motivación última de la conducta, que puede residir en la vulneración de passwords (*hacking*), en la vulneración de programas informáticos (*cracking*), o en la destrucción de datos, programas o soportes informáticos (*cyberpunking*).

La dificultad de disponer de información precisa en este ámbito, junto a esa diversidad de ilícitos vinculados a la red, ha favorecido el surgimiento de algunos equívocos conceptuales. Así, por ejemplo, se emplea el término *hacking* para aludir al autor de copias ilegales de programas, identificando dicho término con el de « pirata informático ». De otra parte, el término *cracking* se acuña para definir la conducta de quien actúa en los sistemas informáticos con ánimo vandálico o dañino, destruyendo datos o programas. Y, por último, se recurre a la citada expresión de « pirata informático » para aglutinar todas las conductas enunciadas, es decir, las de mero intrusismo informático (o de *hacking*), las de vulneración de derechos de autor (o inicialmente de *cracking*) y las de daños informáticos (o si se prefiere de *cyberpunks* o *cyberpunking*) ([23]).

Esas discrepancias conceptuales – y la ausencia de definiciones comunes de las infracciones relativas a los ataques contra los sistemas de información- – obstaculizan un conocimiento certero sobre la naturaleza de tales ataques y entorpecen una cooperación internacional policial y judicial más eficaz en el logro de su represión. La urgente necesidad de disponer de herramientas teóricas comunes aconseja, pues, acometer algunas precisiones terminológicas que arrumben, en la medida de lo

([23]) Muestra de dicho desorden conceptual devienen, incluso, algunos pronunciamientos comunitarios en el marco europeo. Así, por ejemplo, la descripción incorporada por la Propuesta de Decisión-Marco europea, 19.04.2002, en su apartado 1.1, letra a) de la Exposición de motivos, de la conducta de *acceso no autorizado a sistemas de información*, en la que se declara : « Esto incluye el concepto de 'piratería informática'. La piratería consiste en tener acceso de manera no autorizada a un ordenador o a una red de ordenadores. Puede tomar distintas formas que van desde el mero uso de informaciones internas a ataques directos y la interceptación de contraseñas. Se realiza generalmente pero no siempre-con una intención dolosa de copiar, modificar o destruir datos. La corrupción deliberada de sitios Internet o el acceso sin previo pago a servicios restringidos puede constituir uno de los objetivos del acceso no autorizado ». Esta descripción aglutina bajo un único concepto acceso no autorizado a sistemas de información- diversas conductas de distinta caracterización y gravedad, lo que, a nuestro juicio, difícilmente contribuye al objetivo perseguido por la propia norma de hallar una terminología común, logro que requiere como tarea previa el preciso deslinde conceptual entre comportamientos con caracteres y notas compartidas pero con matices propios.

posible, esos equívocos suscitados y, sobre todo, que proporcionen un utillaje conceptual lo más unívoco posible.

En el estudio individualizado de estas tres modalidades de conducta, se propondrá, por consiguiente, en primer lugar, una breve caracterización de la conducta; a continuación se examinará su encaje en nuestro derecho positivo y, por último, se someterá dicha regulación a un examen crítico, que conducirá, en algunos casos, a plantear propuestas de reforma legislativa.

3.2. – *Conductas de « piratería informática » o de* cracking

Las conductas de *cracking*, con arreglo a su significación originaria, se caracterizan por eliminar o neutralizar los sistemas de protección de un sistema informático, ya sea de un programa o del propio sistema operativo de la máquina ([24]). Habitualmente, se rompe la protección de un programa que impide su copia no autorizada o la de una aplicación *shareware* que impide su uso, pasada una determinada fecha ([25]).

Este comportamiento se cifra, pues, en la copia inconsentida y, en su caso, posterior distribución ilegal, de programas informáticos (denominados *warez*, esto es, programas comerciales que han sido sometidos a la acción de un *crack*), con vulneración de los derechos de autor.

En el derecho penal interno la conducta del *cracker*, al margen de los supuestos de tipificación penal específica, suele encontrar primordialmente tratamiento en los delitos relativos a la propiedad intelectual o en los daños, en este caso informáticos. Así, cabe mencionar en España, el artículo 270 del Código Penal (delitos relativos a la propiedad intelectual ([26])) o el artículo 264.2 CP (daños informáticos).

([24]) El término *cracker* fue acuñado en 1985 para diferenciar - -y defender- estas conductas de las de los *hackers*, ante el mal uso periodístico de este último término (M. MOLIST, 2001:18). Esta tendencia a deslindar estos dos comportamientos se ha perpetuado, de modo que, actualmente, en algunas ocasiones, se suele acudir a las expresiones de *black hack* o *black hat*, como sinónimos de *cracker*, para distinguirlas de la conducta del *hacker*, al que también se hace referencia con las antónimas de *white hack* o *white hat*.

([25]) Vid., en este sentido, D. FERRANDIS, 2001:175 y M. MOLIST, 2001:18.

([26]) No puede abundarse en el estudio de las conductas atentatorias de la propiedad intelectual o lo que comúnmente se denomina « piratería informática o de *software* ». A estos efectos, sin embargo, merece la pena destacar la protección especial de los programas de ordenador, prevista en el art. 270, último párrafo CP, incriminador de las conductas destinadas a inutilizar o neutralizar de modo no autorizado de cualquier dispositivo técnico que se haya utilizado para proteger programas de ordenador, otorgando, así, una tutela ya reclamada por la Directiva 91/250, de 14 de mayo, adoptada por el Consejo de las Comunidades Europeas, sobre protección de programas de ordenador, instando a los Estados miembros a adoptar las disposiciones de derecho interno necesarias para su cumplimiento. Concretamente, dicha en dicha Directiva se establece que los Estados miembros, de conformidad con sus legislaciones nacionales, deben adoptar medidas oportunas para evitar la puesta en circulación de una copia de un programa de ordenador conociendo su origen ilícito, la tenencia

3.3. – *Comportamientos de « mero intrusismo informático » o de* hacking

3.3.1. – Caracterización de la conducta y perfil del sujeto activo

Las conductas de *hacking* se definen como conductas de mero intrusismo informático, esto es, comportamientos de acceso a un sistema informático, de un modo no autorizado o más allá de lo autorizado. A esta aproximación general debe añadirse una pieza clave en la caracterización del *hacker* como autor, puesto que su « idiosincrasia », en estos comportamientos, contribuye a la propia definición de la conducta.

El sujeto activo, es decir, el *hacker* conoce a fondo el funcionamiento de los sistemas operativos, de los lenguajes de programación y de los protocolos de Internet. La motivación de sus accesos suele radicar en profundizar en ese conocimiento, poniéndose a prueba en una constante superación de retos. Se infiltra subrepticiamente en los sistemas para descubrir puertas falsas o fallos, estudiarlos, averiguar a qué se deben y para demostrar que puede acceder aunque se le impongan barreras lógicas de entrada mediante *passwords*. Generalmente, el *hacker* no toca ni borra nada, excepto los *logs* necesarios para hacer desaparecer su rastro.

Formulado el perfil del *hacker*, como sujeto que lleva a cabo una intrusión desprovista de cualquier motivación distinta a la curiosidad y al reto, procede ya examinar el plano real de las vías que recoge el código para castigar esta conducta.

3.3.2. – Encaje de derecho positivo

Respecto al encaje en el código penal vigente de estas conductas de mero intrusismo informático, pueden distinguirse dos hipótesis, una no problemática y la otra que deviene más controvertida y que será la que se analice con algo más de detenimiento.

a) La intrusión puede concebirse como un medio necesario para conseguir el resultado final, consistente, quizá, en el ataque a una pluralidad de intereses, como, por ejemplo, la vulneración de la intimidad ajena, la destrucción de datos, el acceso a un secreto de empresa, el descubrimiento de un documento secreto relativo a la Administración Pública, entre otros. En estos casos, la conducta quedará consumida por estos delitos, como fase o estadio típico inicial de los mismos. La princi-

con fines comerciales de una copia de un programa de ordenador conociendo o pudiendo suponer su naturaleza ilegítima, así como la puesta en circulación o tenencia con fines comerciales de cualquier medio apto para facilitar la supresión o neutralización de cualquier dispositivo técnico utilizado para la protección de un programa de ordenador (artículo 7).

pal dificultad radicará en la prueba del elemento subjetivo (mediante el correspondiente juicio de inferencias) de estas conductas, es decir, en demostrar que el *hacker* no obra sólo con un deseo de demostración de pericia técnica, sino también con la finalidad, pongamos por caso, de apoderarse de un secreto de empresa.

b) Por el contrario, puede ocurrir que las conductas de *hacking* no determinen tales resultados o que, aun determinándolos, no hayan sido ejecutadas con ese propósito. En estos supuestos radica el problema, puesto que la mayor parte de los delitos anteriormente mencionados incorporan específicos elementos subjetivos, de los que, por definición, adolece el comportamiento del *hacker*. Así ocurre, por ejemplo, en España, con el delito de vulneración del « habeas data » (art. 197.2, segundo inciso CP), que castiga el acceso sin autorización a los datos reservados de carácter personal o familiar, en el que se postula la incorporación implícita del elemento subjetivo previsto en el apartado primero o segundo de dicho precepto y que se cifra en la perpetración del acceso con *el ánimo de descubrir la intimidad ajena*; o con el delito de interceptación de las comunicaciones en sistemas informáticos o redes telemáticas, previsto en los delitos relativos a la intimidad (art. 197.1, segundo inciso CP) o en los delitos reguladores del secreto de empresa (art. 278.1, segundo inciso CP), que contienen un específico elemento subjetivo consistente en que estas intromisiones se lleven a cabo con *el ánimo de descubrir los secretos o vulnerar la intimidad ajena o un secreto de empresa*; o con el delito de daños informáticos (art. 264.2 CP), que castiga la destrucción, alteración, inutilización u otro daño de los datos, programas o documentos electrónicos ajenos contenidos en redes, soportes o sistemas informáticos, y cuya comisión reclama la presencia de *un ánimo de dañar los datos* contenidos en los sistemas, en el que se cifra el dolo del tipo.

Ahora bien, aun desechados los supuestos anteriores, en el Derecho penal español, puede sugerirse como hipótesis de trabajo una doble vía. En primer lugar, cabría pensar en la aplicación del *delito de utilización abusiva de equipos de telecomunicación* (art. 256 CP), que castiga el uso de cualquier equipo terminal de telecomunicación, sin consentimiento de su titular, siempre que se ocasione-- al titular del equipo y no a un tercero-- un perjuicio evaluable económicamente superior a cuatrocientos euros. Y, en segundo lugar, sería dable, también, la aplicación del *delito de daños imprudentes* (art. 267 CP), aunque, supeditado a la exigencia de que se produzca un perjuicio económico superior a ochenta mil euros.

En cualquier caso, según se observa, ambas hipótesis se alejan, en su regulación, del posible interés puesto en peligro con los accesos inconsentidos, que, sin duda, no es necesariamente económico y, aun en el

supuesto de que lo fuera (piénsese, por ejemplo, en los daños en el crédito que puede sufrir una empresa de *software* objeto de intrusiones), no tiene por qué tener repercusión o traducción inmediata en cantidades dinerarias.

3.3.3. – Propuesta de incriminación autónoma

Lógicamente, frente a estos obstáculos, han surgido en España nuevas propuestas. De una parte, se postula el encaje del intrusismo en los delitos contra la intimidad (concretamente, en el art. 197.1 CP), al considerar que las claves de acceso integran el derecho a la intimidad (D. De Alfonso, 2002:520-521). De otra, se reivindica la conveniencia político-criminal de introducir un tipo penal autónomo que castigue estas conductas (M.L. Gutiérrez, 1995:1179-1180). De hecho, recientemente, ha aparecido normativa de carácter internacional (Convenio europeo sobre Cibercriminalidad ([27])) y de ámbito comunitario (Propuesta de Decisión-Marco europea ([28])), que, específicamente, prevé estas conductas, aunque con bastante confusionismo en la definición y regulación formuladas (E. Morón, 2002:69 ss.) ([29]).

Uno de los principales motivos aducidos para la incriminación autónoma, en el código, se basa en que, según demuestran los estudios criminológicos realizados en otros países, comportamientos inicialmente de mero intrusismo informático, desprovistos de toda intención distinta al propio acceso no autorizado, terminan convirtiéndose en otros ilícitos más graves, como fraude, espionaje, sabotaje, etc. Y de ahí la conveniencia de adelantar la barrera de protección penal, incriminando conductas que, sin provocar un resultado lesivo de algún bien jurídico concreto, se presumen peligrosas, como primera fase de un ilícito más grave.

Sin duda, las conductas de mero intrusismo informático pueden ser conductas antesala de otros ilícitos. Ahora bien, si éste es uno de los

([27]) Convenio europeo sobre cibercriminalidad [Budapest, 23.XI. 2001].

([28]) Propuesta de Decisión-Marco del Consejo europeo relativa a los ataques de los que son objeto los sistemas de información, presentada por la Comisión, Bruselas, 19 abril 2002, COM (2002) 173 final, 2002/0086 (CNS).

([29]) La imprecisión conceptual constituye una de las principales objeciones que cabe formular a la Propuesta de Decisión-Marco europea, que, al definir la conducta de « acceso no autorizado a sistemas de información », declara : « Esto incluye el concepto de 'piratería informática'. La piratería consiste en tener acceso de manera no autorizada a un ordenador o a una red de ordenadores. Puede tomar distintas formas que van desde el mero uso de informaciones internas a ataques directos y la interceptación de contraseñas. Se realiza generalmente pero no siempre- con una intención dolosa de copiar, modificar o destruir datos. La corrupción deliberada de sitios Internet o el acceso sin previo pago a servicios restringidos puede constituir uno de los objetivos del acceso no autorizado ». No resulta adecuado identificar la conducta del *hacker* con la del « pirata informático », para designar al autor de copias ilegales de programas o como categoría omnicomprensiva de cualquier conducta ilícita en la red (accesos inconsentidos, vulneración de derechos de autor, daños informáticos, etc.).

motivos que debe fundamentar la incriminación del intrusismo, quizá deba examinarse previamente si el código proporciona una respuesta penal adecuada a esos otros ilícitos más graves, en los que probablemente el reproche será menos conflictivo. Y, en este sentido, la reforma operada por el código español de 1995 en materia de criminalidad informática ha sido profunda y ofrece respuestas.

Un segundo argumento esgrimido se cifra en que la intervención penal en dichos supuestos evitaría la impunidad de otros de mayor entidad, pero de difícil descubrimiento y prueba.

Aunque, probablemente, ello es así, acudir a la incriminación de nuevos tipos penales obedeciendo sólo al propósito de facilitar la prueba de estos delitos, es cuestionable desde el punto de vista de la legitimidad del derecho penal. De hecho, en materia de criminalidad económica, por ejemplo, los problemas de prueba sólo se admiten si son motivos acompañantes de una fundamentación esencial, que radica en la necesidad de tutelar auténticos bienes jurídicos, previamente precisados.

Y quizá, en este punto, se halle ahora la discusión; es decir, en torno a si puede reconocerse la aparición de un nuevo bien jurídico cifrado en la seguridad de los sistemas informáticos. Desde luego, ésta es la opción que parece subyacer, al menos, en la Propuesta de Decisión-Marco europea referida. Sin embargo, en la configuración de los tipos penales que la Propuesta destina a proteger ese hipotético bien jurídico, reina cierta inseguridad. Se exige, por ejemplo, la concurrencia de adicionales elementos subjetivos [intención de causar un daño a una persona física o jurídica o intención de obtener un beneficio económico], que no necesariamente se vinculan con ese nuevo interés tutelado.

Probablemente, dicho titubeo legislativo resulta lógico en un periodo, afectado por una innovación informática vertiginosa, pero en el que no se dispone todavía, en algunos países entre los que se encuentra España, de una respuesta jurídica sancionadora, que se halle ya consolidada, frente a los abusos o ilícitos perpetrados en las redes. Ni siquiera por parte de los instrumentos primarios de regulación, como el derecho administrativo. En definitiva, no se goza aún de una tradición o cultura informática suficientemente asentada, como para afrontar esa arriesgada vía, cifrada en abordar la tutela integral del citado bien jurídico y que supondría modificar el modelo de incriminación vigente.

En cambio, a mi entender, la adopción de medidas de seguridad preventivas (de enorme relevancia en la delincuencia informática) junto con la aprobación de normas de comportamiento o códigos de práctica en el uso de las nuevas tecnologías (así lo recomienda la Directiva 95/46/CE (art. 27.1), que regula los códigos de conducta) y la articulación de oportuna legislación no penal (análoga a la prevista en la regulación de pro-

tección de datos), puede beneficiar en mayor medida el adecuado fomento de las redes mundiales de la información.

3.4. – *Comportamientos de « daños informáticos »*

3.4.1. – Definición de la conducta

Las conductas de daños informáticos o de vandalismo electrónico (*ciberpunk*, *script-kiddie*, *lamer*) se concretan en asaltos sobre máquinas o sistemas informáticos para ocasionar perturbaciones sobre dichos sistemas o para modificar o destruir datos. Esto es, se trata de comportamientos preordenados por el ánimo de perturbar los sistemas informáticos o de destruir los datos que contienen.

Actualmente, una de las acciones más peligrosas del *cyberpunk* o vándalo electrónico radica en el acceso inconsentido a los sistemas informáticos, con el fin de implementar un virus que produzca los resultados anteriormente indicados.

3.4.2. – Encaje de derecho positivo

El encaje de estos comportamientos en el vigente código penal español se halla en el delito de daños informáticos (art. 264.2 CP), que castiga la conducta de quien destruya, altere, inutilice o de cualquier otro modo dañe los datos, programas o documentos electrónicos ajenos, contenidos en redes, sistemas o soportes informáticos. Este precepto permite recoger gran parte de los atentados que sufre la información, aunque no se trata de un precepto exento de problemas, de los que destacaré sólo dos, uno de orden más jurídico-dogmático y otro derivado de la propia complejidad técnica de la materia ([30]).

Se trata de un delito previsto entre los delitos contra el patrimonio y que constituye una forma agravada del delito tradicional de daños sobre cosa ajena, que exige la producción de un perjuicio superior a 400 euros. Por tanto, la primera dificultad se cifra en decidir si la aplicación del delito de daños informáticos tiene que cumplir esa condición del tipo básico y, a continuación, caso de que efectivamente se exija, debe concretarse cómo valorar monetariamente el perjuicio que causa la destrucción, alteración o inutilización de los datos, tarea que no siempre resulta fácil ([31]).

([30]) Vid., más ampliamente, A.C. ANDRÉS, 1999:3 ss.

([31]) Piénsese en la dificultad de evaluar, la introducción de un virus que borra una tesis doctoral a punto de terminarse, o la introducción de un virus en el sistema informático de un complejo hospitalario, que, provoca, la anormalidad en su utilización y funcionamiento, entre otros múltiples y controvertidos supuestos.

A ello deben añadirse las dificultades técnicas inherentes a la materia, que entorpecen una adecuada descripción de los comportamientos delictivos. Así, por ejemplo, no aparecen contemplados separadamente los efectos de muy diversa entidad que puede producir, pongamos por caso, un virus. En este sentido, no reviste igual gravedad que el resultado del sabotaje sea la aparición de un mensaje en pantalla, o bien la reducción de la velocidad de proceso de la máquina o bien la destrucción total de los datos o información que contiene el ordenador. De ahí que quizá el código debiera distinguir, como mínimo, entre los ataques que tienen como objeto la destrucción o inutilización de los datos o programas y los ataques que se proyectan sobre el funcionamiento del sistema y que se cifran en perturbaciones, molestias o alteraciones en el correcto funcionamiento del mismo.

3.4.3. – Propuesta *de lege ferenda*

Respecto a las diversas vías de reforma, existen varios modelos de incriminación a seguir. Uno de ellos supondría corregir las deficiencias que, en relación a los abusos informáticos, perviven en algunos ámbitos del código, introduciendo específicas previsiones en esos preceptos, a fin de que puedan valorarse los perfiles propios de los intereses protegidos (incluido el propio delito de daños informáticos). Otro más arriesgado consistiría en trasladar el precepto a un capítulo de nueva creación, que recogiese éste y todos los demás atentados contra los sistemas informáticos, entre los que podría hallarse la incriminación del mero intrusismo informático, al que antes aludía. Por el momento, resulta preferible acudir a la primera vía, aun en contra de la tendencia de la normativa internacional y europea actual.

4. – Perspectivas de futuro

En cuanto a las propuestas de futuro y a la conveniencia de incorporar modalidades típicas *ad hoc* que castiguen estos nuevos riesgos a través del Derecho interno, me inclino, pues, por la cautela.

En no pocos ejemplos de Derecho Comparado, la regulación civil, administrativa o mercantil de Internet es todavía incipiente o muy reciente, y aun cuando se hayan introducido recientemente (como en el Código penal español de 1995) profundas reformas y se disponga de este modo de suficientes vías para reprimir la criminalidad informática, resulta todavía prematuro evaluar la efectiva necesidad de intervención penal, que, como se sabe, es la rama del ordenamiento jurídico que debe intervenir en último lugar y cuando el resto de sectores se han demostrado ineficaces.

La criminalidad informática constituye, sin duda, un problema global que exige estrategias internacionales para su efectivo control y prevención. Y, en la lucha contra la ciberdelincuencia, es indispensable la armonización internacional de ciberdelitos y la articulación de reformas procesales que hagan efectiva la persecución de estas infracciones y cooperación internacional entre los Estados, judicial y policial. En este sentido, se ha dado un decidido impulso, a escala internacional, a la lucha contra la cibercriminalidad, mediante la aprobación de legislación específica al efecto ([32]).

Por tanto, y sin excluir la conveniencia de mejoras puntuales en la legislación penal, sobre todo, resulta indispensable una mayor inversión en unidades especializadas, a fin de que se disponga de los recursos adecuados en la investigación y persecución de esta compleja parcela de la criminalidad.

Referencias

ANDRÉS, Ana Cristina. 1999. « Los daños informáticos en la Unión Europea », en *La Ley*, n. 4725, pp. 1-5.

BARNES, Javier. 1997. « Internet y el derecho. Una nota acerca de la libertad de expresión e información en el espacio cibernético », *en Ordenación de las telecomunicaciones, Cuadernos de Derecho Judicial.* VI : Madrid, pp. 235-272.

COSTANZO, Pasquale. 1996. « Aspetti evolutivi del regime giuridico di Internet », en *Il Diritto dell'informazione e dell'informatica.* Milano : Giuffrè, pp. 831-846.

DE MARTINI, Corrado. 1996. « Telematica e diritti della persona », en *Il Diritto dell'informazione e dell'informatica.* Milano : Giuffrè, pp. 847-866.

([32]) En el ámbito comunitario europeo, se ha presentado por la Comisión (Bruselas, 19.04.2002) una propuesta de decisión-marco relativa únicamente a los ataques de los que son objeto los sistemas de información y, a escala internacional, se halla pendiente de ratificación el Convenio europeo sobre Cibercriminalidad, firmado ya por 27 Estados. En dicho impulso han confluido diversos factores. De una parte, el incremento en la creación, divulgación e infección a causa de virus informáticos y de los cuantiosos daños económicos provocados por éstos (en 2001, por ejemplo, *Nimda* provocó pérdidas de 630 millones de dólares, *Code Red*, de 2620 millones, *SirCam*, de 1150; en 2000 *I love You*, de 8750 millones y, en 1999, *Melissa* causó pérdidas de 1100 millones y *Explorer* de 1020 millones de dólares); asimismo, el aumento también en los ataques contra encaminadores y de denegación de servicio; por último, la alarma social suscitada ante los peligros que encierra la utilización de las nuevas tecnologías por delincuentes informáticos y, sobre todo, a tenor de lo acontecido el 11-S, por organizaciones terroristas; esto es, la inquietud creciente ante la amenaza de lo que se ha venido a denominar « ciberterrorismo ».

DONATO, Barbara. 1996. « La responsabilità dell'operatore di sistemi telematici », en *Il Diritto dell'informazione e dell'informatica.* Milano : Giuffrè, pp. 135-150.

ECHEVERRÍA, Javier. 1999. *Los Señores del aire : Telépolis y el Tercer Entorno*, Barcelona. Barcelona : Destino.

ECHEVERRÍA, Javier, 2000. *Un mundo virtual.* Barcelona : Plaza & Janés, de Bolsillo.

DE ALFONSO, Daniel, 2002. « El hackering blanco. Una conducta ¿punible o impune? », en *Internet y derecho penal, Cuadernos de Derecho Judicial.* X : Madrid, pp. 509-523.

European Council. 1997. *Implementation of Recommendation n° R (89)9 on Computer related Crime*, Strasbourg.

FERRANDIS, Daniel, 2001. « Glosario », en ORTS, Enrique y ROIG, Margarita, *Delitos informáticos y delitos comunes cometidos a través de la informática.* Valencia, pp. 173-183.

GUTIÉRREZ, Mari Luz, 1995. « El intrusismo informático (Hacking) : ¿Represión penal autónoma? », en *Informática y Derecho*, vol. 12-15 : pp. 1175-1183.

LENZ, Karl-Friedrich. 1998. « Strafrecht und Internet », en ESER, Albin (Hrsg.), *Festschrift für Haruo Nishikara zum 70. Geburtstag.* Nomos Verlagsgesellschaft, Baden-Baden.

LÓPEZ ORTEGA, Juan José. 2002. « Libertad de expresión y responsabilidad por los contenidos en Internet », en *Internet y derecho penal, Cuadernos de Derecho Judicial.* X : Madrid, pp. 83-125.

MAGNI, Sabrina y SPOLIDORO, Marco Saverio. 1997. « La responsabilità degli operatori in Internet : profili interni e internazionali », en *Il Diritto dell'informazione e dell'informatica.* Milano : Giuffrè, pp. 61-89.

MANNA, Adelmo. 2001. « Considerazioni sulla responsabilità penale dell'Internet provider in tema di pedofilia », en *Il Diritto dell'informazione e dell'informatica.* Milano : Giuffrè, pp. 145-151.

MOLIST, Mercè. 2001. « Hackers éticos », en *Ciberp@is,* n. 15 : pp. 14-19.

MORALES, Fermín. 2001. « La intervención penal en la Red. La represión penal del tráfico de pornografía infantil : Estudio particular », en *Derecho penal, sociedad y nuevas tecnologías* : Madrid, pp. 111-133.

MORALES, Fermín, 2002. « Internet : riesgos para la intimidad », en *Internet y derecho penal, Cuadernos de Derecho Judicial.* X : Madrid, pp. 63-81.

MORÓN, Esther, 2002. *Internet y Derecho Penal : Hacking y otras conductas ilícitas en la Red.* Navarra : Aranzadi.

MUÑOZ, Santiago, 2000. *La regulación de la red. Poder y Derecho en Internet*. Madrid : Taurus.

PERARNAU, Joan. « Internet amenazada », en *Internet y derecho penal, Cuadernos de Derecho Judicial*. X : Madrid, pp. 127-144.

PICOTTI, Lorenzo. 1999. « Profili penali delle comunicazioni illecite via Internet », en *Il Diritto dell'informazione e dell'informatica*. Milano : Giuffrè, pp. 283-334.

PICOTTI, Lorenzo. 2000. « Fundamento y límites de la responsabilidad penal de los proveedores de acceso y servicio en Internet », en *Revista de Derecho y Proceso Penal*, vol. 3 : pp. 211-222.

PICOTTI, Lorenzo. 2000. « Reati informatici » (voz), en *Enciclopedia Giuridica Treccani*. Aggiornamento, VIII : Roma, pp. 1-33.

SEMINARA, Sergio. 1997. « La pirateria su Internet e il diritto penale », *en Rivista trimestralle di diritto penale dell'economia*. Padova : Cedam, pp. 71-114.

SEMINARA, Sergio. 1998. « La responsabilità penale degli operatori su Internet », en *Il Diritto dell'informazione e dell'informatica*. Milano : Giuffrè, pp. 745-774.

SIEBER, Ulrich. 1984. *Informationstechnologie und Strafrechtsreform*, Köln.

SIEBER, Ulrich (Coord.). 1994. *Information Technology Crime. National Legislations and International Initiatives*. Köln.

SIEBER, Ulrich. 1997 « Responsabilità penali per la circolazione di dati nelle reti internazionali di computer », *en Rivista trimestralle di diritto penale dell'economia*. Padova : Cedam, pp. 743-785.

SIEBER, Ulrich. 1998. *Legal Aspects of Computer-related Crime in the Information Society. Comcrime-study*. Würzburg.

TÉLLEZ, Abel, 2001. *Nuevas tecnologías. Intimidad y protección de datos. Estudio sistemático de la Ley Orgánica 15/1999*. Madrid. Edisofer.

ZENO-ZENCOVICH, Vincenzo. 1996. « Sistema giuridico e 'diritto delle telcomunicazioni' », en *Il Diritto dell'informazione e dell'informatica*. Milano : Giuffrè, pp. 551-563.

ZENO-ZENCOVICH, Vincenzo. 1998. « La pretesa estensione alla telematica del regime della stampa : note critiche », en *Il Diritto dell'informazione e dell'informatica*. Milano : Giuffrè, pp. 15-28.

RÉSUMÉ

L'internet a produit une véritable révolution technologique, avec un niveau d'accroissement sans précédent dans l'histoire des technologies de

la communication. L'immense flux et échange d'information et, par conséquent, l'intense mobilité des données personnelles et économiques générées par le vaste éventail de services offerts requièrent un cadre de sécurité juridique qui garantisse la protection des biens et des droits sur le réseau. Ainsi, face à l'usage délictueux d'internet, il apparaît nécessaire de réfléchir sur la réglementation de la responsabilité pénale des contenus illicites sur le réseau.

Summary

The Internet has created a veritable technological revolution, with a growth level that is unprecedented in the history of technologies and communication. The huge information flow and exchange, and consequently, the intense mobility of personal and economic data generated by the vast range of services offered, requires a framework of legal security to guarantee the protection of goods and rights on the network. Thus, in view of the illegal use of the Internet, it seems necessary to reflect upon the regulation and criminal responsibility of illicit content on the network.

Resumen

Internet ha supuesto una verdadera revolución tecnológica, con un índice de crecimiento sin precedentes en la historia de las tecnologías de la comunicación. El inmenso flujo e intercambio de información y, por tanto, la intensa movilidad de datos personales y económicos, generados por el amplio abanico de servicios ofrecidos, reclama un marco de seguridad jurídica que garantice la tutela de bienes y derechos en la red. Así, frente al uso delictivo de Internet, resulta necesario reflexionar sobre la regulación de la responsabilidad penal por contenidos ilícitos en la red.