LOS CIBERCRÍMENES EN EL ESPACIO DE LIBERTAD, SEGURIDAD Y JUSTICIA

INTRODUCCIÓN: La lucha contra el cibercrimen es una tarea esencialmente transnacional y, bajo este presupuesto, las Instituciones de la Unión Europea han abordado su persecución y castigo desde la perspectiva de sus Tratados Constitutivos y su normativa derivada. Este artículo, luego de identificar los presupuestos de la cibercriminalidad trasnacional, analiza la regulación europea tanto en el marco de primer pilar (las Comunidades Europeas) como en el marco del tercero (la Cooperación Policial y Judicial en Materia Penal).

Última revisión: 5 de septiembre de 2006.

Autor: Antonio Pedro Rodríguez Bernal

A. Introducción.

La TIC (Tecnología de la Información y el Conocimiento) ha ocasionado una revolución sin precedentes cuyo alcance todavía es insospechado. La Globalización ha sacudido los pilares de las instituciones y las bases de nuestra Sociedad, hasta el punto de sugerir el nacimiento de otra sociedad paralela – a la meramente física – que se conoce como Sociedad de la Información y del Conocimiento[1]. Y mientras esta sociedad paralela echa sus primeros dientes y robustece sus músculos, se discute sobre los problemas que ha engendrado su aparición y sobre cómo solucionarlos. Incluso se discute si es necesario solucionarlos o dejar que los problemas se resuelvan por sí solos.

Los términos *cibercrimen, ciberdelitos, ciberdelicuencia,* se han hecho hueco entre nosotros. En pocos años la sociedad ha tenido que aprender a convivir con esta realidad, extraída de películas de ciencia ficción que unos años atrás nos asombraban. Desde el propio hogar, el usuario de un ordenador, conectado a Internet, puede convertirse en un protagonista activo del progreso. Puede negociar, comprar, vender, subastar, informarse, suministrar información, comunicarse y también, en no pocos casos, delinquir.

Ante la aparición de las nuevas tecnologías el derecho se enfrenta a retos casi inasequibles. Regular una materia en continuo desarrollo, donde los avances informáticos producen nuevas formas de relación humana, y donde esos avances, lejos de detenerse en punto determinado de su evolución, parecen prolongarse, elásticamente, hasta no se sabe dónde. El tradicional inmovilismo de las normas jurídicas, que requieren complicados procesos de creación, se ve impotente para regular un sector en continuo movimiento, que parece querer escapar a toda normativa.

La Unión Europea ha comprendido pronto el fenómeno y su importancia para la integración de sus miembros. Las normas promulgadas en el seno de la Unión abren el camino para el desarrollo de la Sociedad de la Información y del conocimiento. La Directiva sobre el comercio electrónico[2] y la Directiva sobre la privacidad y las comunicaciones electrónicas[3], ofrecen un soporte liberalizador de la Sociedad de Información. En cambio, el Convenio sobre cibercriminalidad, hecho en Budapest, 23.XI.2001, trata de poner límite a la expansión de la cibersociedad cuando detecta, anuncia y persigue las transgresiones delictivas producidas en la Sociedad de la Información.

Lejos de pretender un análisis pormenorizado del complejo fenómeno, nuestro estudio se detendrá en esa vertiente criminal de la informática y, en especial, en la que discurre a través de Internet. El derecho internacional ha de responder mediante instrumentos eficaces los vacíos normativos que se dan en la red. No en vano el Derecho de Internet ha sido comparado con el Derecho Marítimo, e Internet con el Alta Mar – High Seas –, "el territorio que atraviesa un barco y que no se sujeta a la exclusiva jurisdicción de un único estado, del mismo modo el usuario del ciberespacio atraviesa una región independiente que no está sujeta a la jurisdicción exclusiva de ningún Estado".[4] (De Azevedo Ferreira França, 1999: 28).

Internet y su faceta delictiva (el cibercrimen) provocan importantes distorsiones en las bases sobre las que se asienta la soberanía de los estados, la determinación de la

"soberanía del ciberespacio" (así llamada por la *Electronic Frontier Foundation* y la *Wired* magazine)[5] o, lo que es lo mismo, la elección de la ley penal aplicable cuando se opera en la red y de la jurisdicción que deberá resolver los conflictos planteados en el ciberespacio. El problema se multiplica porque "Internet es virtual e infinitamente expandible en tamaño"[6] (Caffarelli, 1999: 11), lo que desborda fronteras e involucra a muchas jurisdicciones.

La tendencia a la globalidad del cibercrimen fuerza a los estados a entenderse y a inventar cierta homogeneidad. El convenio y el tratado siguen siendo elementos insustituibles para lograr esa unificación de criterios, que todavía está lejos de conseguirse. Y son las organizaciones internacionales quienes alientan ese entendimiento. La Unión Europea, tímidamente, va pronunciándose sobre la cuestión y a través de sus tratados constitutivos hay cauces para legislar y desarrollar una normativa uniforme. Analizaremos los artículos en cuestión.

Este trabajo no puede olvidar los supuestos no contemplados por la normativa del ramo. Mencionaremos la compleja problemática originada por los paraísos de cibercirmen, "cybercrime havens", emporios alentados por los gobiernos para cobijar conductas antijurídicas y desde donde se atacan bienes jurídicos en estados que persiguen aquellas conductas. ¿Cómo luchar contra tales políticas? ¿Qué medidas se han adoptado hasta la fecha?

B. Presupuestos del Cibercrimen en la Red.

El cibercrimen representa el estado más sofisticado de la conducta antijurídica. Esencialmente no existe mucha diferencia entre las conductas antijurídicas y punibles tradicionales con aquellas que se cometen a través de medios informáticos. Es justamente la adjetivación del delito, "informático", la que convierte al delincuente en algo apartado de la tradición y envuelve el hecho de unas connotaciones que lo dotan de cierta autonomía conceptual. El ordenador se convierte en un instrumento del delito, no por sí solo, sino por su conexión a una red interna (intranet) o a una red externa (internet), por donde circulan usuarios, estudiantes, empresarios, profesionales, pederastas, grandes sumas de dinero encriptadas, estafadores, saboteadores, niños y terroristas.

Por la peculiaridad del fenómeno y el reto que representa para el jurista, despreciaremos en este trabajo las implicaciones del genérico delito informático y nos centraremos en el ciberdelito perpetrado en Internet.[7]

Predominantemente existen dos formas de comunicación a través de Internet: el correo electrónico[8] y la World Wide Web[9]. Simplificaremos nuestra exposición ignorando otros modos de comunicación en red que han perdido protagonismo o que poseen una importancia delictiva muy limitada, como el Bulletin Board System BBS, Internet Relay Chats (IRC), usenet, website „guest books", weblogs, File Transfer Protocol, P2P, particulares aplicaciones como Napster, Gnutella[10], sin perjuicio de que gran parte de lo dicho en estas páginas sea aplicable a dichos sistemas de comunicación. Por su parte, MORALES GARCÍA incluye, como modalidad de la WWW, el Webcasting, que define como "grupo de servicios emergentes que utilizan Internet para la entrega de contenidos a los usuarios, de una forma muy similar a los servicios de comunicación".[11]

La World Wide Web (WWW), es un sistema de hipertexto que funciona sobre Internet, a través del cual, y con la ayuda de una aplicación informática destinada al efecto, el navegador web, se extrae información (llamada "documentos" o "páginas web") y se muestra en la pantalla del usuario. Siguiendo los hiperenlaces, el usuario puede acceder a múltiples páginas, lo que se denomina "navegación". Dicha páginas se encuentran hospedadas en servidores donde se almacena la información en discos duras.

Es frecuente que los responsables de las páginas y portales Web utilicen vías distintas de acceso para transferir los contenidos. El más utilizado es el protocolo FTP.[12]

Del mismo modo que el conductor ebrio, para cometer un delito contra la seguridad del tráfico, necesita un vehículo a motor, drogas tóxicas o bebidas alcohólicas y, generalmente, una vía pública asfaltada como escenario, el ciberdelicuente requiere disponer de un terminal de ordenador (el vehículo a motor), una conexión a Internet (la vía pública) y las distintas estaciones que posibilitan la circulación: proveedores de servicios, de contenido, mirrors, proxys, etc. (el asfalto.)

Principalmente son tres o cuatro sujetos, como mínimo, los que interviene en el fenómeno del cibercrimen. El sujeto activo del delito, que inicia la conducta punible (sea enviando contenidos a un servidor, sea descargando archivos prohibidos, sea remitiendo e-mails difamatorios); los sujetos coadyuvantes sin cuya intervención el ciberdelincuente carecería de los medios técnicos necesarios para desarrollar su conducta criminal (el servidor de acceso, que posibilita la conexión a la red y el servidor de contenidos, en cuyos discos duros se alberga la información delictiva, que más tarde ofenderá o causará perjuicios); y, por último, el sujeto pasivo del delito, caracterizado en Internet por ser plural, a veces masivo, internacional y, casi siempre, indeterminado y desconocido para el delincuente. Generalmente, serán estos cuatro sujetos los protagonistas del cibercrimen, pero, en ocasiones, si el delito consiste en el envío directo de e-mails, no intervendría el servidor de contenidos, cifrándose en tres los intervinientes.

Naturalmente los sujetos, humanos o cibernéticos, se puede multiplicar por medio de mirrors[13] y proxys[14], por lo que las combinaciones del itinerario criminal aumentan considerablemente.

Características de Internet

Internet, medio donde se desenvuelve el delincuente, y que engloba el ámbito objeto de este estudio (el WWW), contiene unos elementos especialmente favorables para la comisión de delitos. Estas características representan un reto para el jurista y desafía la soberanía de los Estados, como veremos a continuación. SVANTESSON, enumera incisivamente las características más sobresalientes de Internet, a las que me referiré constantemente en el transcurso de estas páginas.

I. Entorno sin fronteras.

La red de redes supone la absoluta libertad de movimientos, la posibilidad de atravesar fronteras sin limitaciones, visados, impedimentos aduaneros. El usuario puede viajar, virtualmente, de un país a otro, adentrándose en otras jurisdicciones, incluso con absoluta ignorancia de que lo hace.[15]

II. Independencia geográfica.

Desde cualquier lugar del mundo se puede teclear en el navegador del ordenador la dirección URL deseada.[16] En una fracción de segundo, el usuario visita páginas web localizadas en distintos lugares del planeta. Si la navegación transcurre con normalidad, el internauta comprobará como, independientemente de que la página visitada se encuentre en su propio país o en las antípodas, la velocidad de conexión es prácticamente la misma (instantánea), no siendo un elemento determinante la medición tradicional de las distancias.

III. Independencia de lenguaje.

Al contrario que los sistemas de comunicación precedentes (teléfonos, radiofonía, telégrafo, etc.), la World Wide Web, por medio de una sofisticada tecnología, posibilita el acceso multilingüe a las páginas visitadas. Ello permite, a través de aplicaciones ofrecidas por diferentes operadores, que cualquier persona se incorpore a Internet sin mayores impedimentos. Se desarrolla asimismo un sistema peculiar de comunicación, una jerga propia de internautas.[17]

IV. Permite la comunicación de uno a muchos (one-to-many communications.)

Esta característica es trascendental para el jurista. El ciberdelincuente suele conocer este rasgo de la World Wide Web y utiliza la tela de araña para que los efectos de su acción se multipliquen y perjudiquen a multitud de personas. Este elemento, aleja el ciberdelito del delito tradicional, por cuanto los efectos de aquél pueden producirse, incluso simultáneamente, en una pluralidad de jurisdicciones, aunque la acción inicial partiera de un lugar muy concreto y lejano.

V. Sistema incomparable de distribución de información.

Ni la televisión ni la radio ni, por supuesto, los sistemas de comunicación predecesores poseen la fuerza distributiva de la WWW. Cualquier persona, con escasos medios técnicos y financieros, puede entrar el circuito y utilizar la red para difundir sus opiniones, investigaciones, filosofías y doctrinas. Las posibilidades de delinquir aumentan exponencialmente.

VI. Ampliamente utilizado, cada día más.

En pocos años la difusión de Internet ha llegado a casi todos los hogares de los países desarrollados.[18] En países subdesarrollados el uso se incrementa, sin que la precariedad de la economía sea un obstáculo insalvable. Países en vías de desarrollo, como India y Filipinas, se sitúan a la cabeza mundial en los avances informáticos relacionados con Internet.[19] El acceso a tal tecnología y, por consiguiente al ciberdelito, es abierta y popular. Precisamente, esta facilidad unida a la precariedad normativa en materia de persecución del cibercrimen en países subdesarrollados, hacen de éstos paraísos cibernéticos, donde los propios estados fomentan el vacío legal para atraer explotaciones que en otros estados serían ilícitas.

VII. Portabilidad.

El fenómeno de la WWW se caracteriza por la ubicuidad. La irradiación de los contenidos es altamente escurridiza, pudiendo situarse, aunque los contenidos distribuidos sean idénticos, en varios puntos del planeta. Esto obedece a diversos motivos, que pueden ser lícitos (simplemente para facilitar los accesos o la velocidad de descarga) o ilícitos (situarse fuera del alcance de la persecución policial o judicial.) Así, una página Web puede ser reflejada (por medio de *mirrors*) en un servidor localizado en cualquier otro lugar del planeta, con el simple objeto de distribuir los accesos – sin saturar las bandas – y aumentar la velocidad al usuario, que se ve, de esta forma, favorecido por un mejor servicio.

Por las mismas razones (excelencia en el servicio) es tecnológicamente posible que el texto de una página Web se aloje en un servidor y las imágenes en otro, convergiendo en el navegador del usuario textos e imágenes perfectamente editadas y maquetadas. El internauta desconoce la procedencia del contenido –tal vez de distintos Estados- pero se contenta con el acceso más veloz.

A semejanza de las antiguas *fondachi* o las alhóndigas que albergaban a los navegantes, es curioso que en ciertos aspectos –en el de la inversión de la responsabilidad, en el de la ubicación, etc.— el servidor se convierta en un establecimiento extraterritorial. Una suerte de incubadora, necesaria para la propagación de la Sociedad de Información, pero que debe involucrar al Derecho Público por ser la necesaria plataforma desde donde cometer los delitos.

Estas „alhóndigas de comerciantes" son las denominadas *server farms*, emporios cibernéticos donde las empresas alojan sus páginas Web. El *server farm*, a cambio de una retribución, provee de electricidad, de ancho de banda para conectarse y del espacio físico para alojar los contenidos (espacio en el disco duro.) Una versión del *server farm* es el *internet content host*. Este servidor, además de los servicios facilitados por el *server farm*, suministra efectivos servidores y pueden también acometer el mantenimiento eficaz de las websites. Tanto en uno como en otro caso, el sistema de websites se aloja en „barns", especie de graneros o viveros donde se hospedan billones de datos binarios y que poseen una sede física situada en un Estado determinado, que puede no coincidir –y normalmente no coinciden—con la empresa que ha contratado el servicio. Al objeto de nuestro análisis esta cuestión no es baladí pues origina conflictos de jurisdicción y competencia, como se verá más abajo.

VIII. Falta de identificadores seguros.

La carencia de identificadores seguros se manifiesta en dos sentidos, tanto desde la perspectiva del que remite la información, como desde el punto de vista de quien recibe la información. Ambos agentes de la comunicación en la WWW carecen de medios fiables para identificar a sus respectivos interlocutores.

El usuario corriente de la WWW sólo conoce, como máximo la dirección IP[20], y el nombre de dominio, conocido com DNS[21]. Algunos nombres de dominio contienen identificadores geográficos, dominios de nivel superior nacionales (ccTLD), basados en la nomenclatura ISO 3166. Sin embargo, esta nomenclatura es equívoca porque websites de un país pueden utilizar códigos de otros países[22]. Así muchos websites suecos emplean el código .nu de Niue, ya que nu significa en sueco „ahora". La identificación es aun más

difícil cuando se utilizan dominios de nivel superior genéricos (gTLDs) El problema se acentúa cuando hablamos de dominios de segundo nivel.

Si bien comienzan a desarrollarse las denominadas *geo-location tecnologies,* consistentes en medios técnicos que conectan una dirección IP con un emplazamiento físico, todavía estas tecnologías no son fiables y se hallan escasamente implantadas.[23]

Esta característica consustancial de la WWW añade el problema de las dificultades perseguibilidad (investigación cibernética) y la efectiva punición de las conductas antijurídicas.

IX. Inexistencia de una autoridad central que controle el acceso a la WWW.

Paralelamente al surgimiento de Internet, se inició un arduo debate sobre la necesidad de regulación del fenómeno. . Los ensayos normativos en nuestra legislación (tanto nacional como transnacional)[24] han merecido vehementes críticas, no sólo desde sectores *no intervencionistas* o *antiglobalización,* sino también desde posturas estrictamente técnicas[25].

En un escenario tan complejo como el de Internet, el Derecho se ve desbordado ante la celeridad tecnológica, achicando tempestades mediante tímidas respuestas, varando en instrumentos jurídicos antiguos. El acervo precedente hace que las adaptaciones sean incompletas. Realmente se ha creado una superestructura que requiere pilares y planteamientos también novedosos, sin que se encuentren absolutamente condicionados por el pasado. Los juristas se ven impotentes para comprender la problemática tecnológica y prever los avances que se avecinan. Para colmo, una vez comprendidos éstos, los instrumentos normativos se elaboran lentamente: cuando se promulgan están llamados a regir poco tiempo, pues pronto se quedan obsoletos.

La regulación de Internet, en consecuencia, siempre estará plagada de lagunas. Estas lagunas se deben llenar con autorregulación, por lo menos, en tanto que no exista una norma positiva. La costumbre, fuente del Derecho, se va a caracterizar en Internet por una rápida conformación (lo que, en cierto modo, contradice el concepto mismo de costumbre.) La introducción de nuevos elementos en la red, amparados por la libertad de prestación de servicios[26], a los que el Derecho no puede responder con la misma rapidez, fomenta el nacimiento de una costumbre "express". Los usos, que conceptual y tradicionalmente, tardaban años en gestarse, ahora tardan meses, por la propia necesidad de autorregulación.

Ante este panorama, caracterizado por una autorregulación de facto, sólo podrá existir un control meramente tecnológico y de naturaleza privada. Los ISP pueden controlar el acceso de sus usuarios, pero desde una perspectiva técnica sin que le sea permitido un juicio de contenidos, más allá de uno somero y grueso.

Algunos gobiernos podrían legislar sobre el comportamiento en Internet de sus ciudadanos, pero la contravención de tales normas difícilmente se podrían castigar, por las dificultades de investigación ya señaladas más arriba.

C. El Cibercrimen en la WWW.

a. El concepto de cibercrimen.

Las palabras "cibercrimen", "ciberdelito", "delito de la Sociedad de Información", "delito de altas tecnologías", y otros semejantes se emplean de forma genérica y a menudo sin ninguna precisión. Huyendo de discusiones terminológicas, es conveniente concretar el ámbito del ciberdelito, pues este, realmente, puede englobarse en dos grandes categorías de ofensas. En la primera, el ordenador (o el sistema informático) es el objetivo de la ofensa, atacándose la confidencialidad, la integridad y/o la disponibilidad del sistema. La otra categoría de cibercrimen no existe en puridad, pues se trata de las tradicionales ofensas (vgr. robo, fraude o falsificación) que se cometen con la asistencia o por medio de ordenadores, redes de ordenadores o con la tecnología de la información y comunicación. El ordenador, en esa segunda categoría es una mera herramienta para perpetrar el delito convencional.[27] A través de la WWW pueden cometerse, indistintamente, ambas categorías de delitos. El ciberdelincuente moderno, el *hacker*, que pretende capturar información confidencial, burlando las medidas de seguridad protectoras, convive en el ciberespacio con el estafador que persigue, a través de páginas Web engañosas, captar fondos de tarjetas de crédito de confiados usuarios.

El concepto de cibercrimen abarca desde el delito económico, como el fraude informático, el robo, la falsificación, el *computer hacking*, el espionaje informático, el sabotaje y extorsión informáticos, la piratería comercial y otros crímenes contra la propiedad intelectual, hasta la invasión de la intimidad, distribución de contenidos ilegales y dañosos, incitación a la prostitución y otros crímenes contra la moralidad, y el crimen organizado. El terrorismo utiliza asimismo el cibercrimen para dirigir ataques contra la seguridad nacional, infraestructuras esenciales y otros bienes vitales de la sociedad.[28]

Relacionando este elenco de delitos con las características propias de la WWW –apuntadas más arriba—los cibercrímenes difieren de los delitos terrestres en cuatro aspectos. 1) Se cometen fácilmente. 2) Requieren escasos recursos en relación al perjuicio causado, lo que anima a muchos individuos a adentrarse en este mundo pese a no responder al perfil sociológico del delincuente tradicional. 3) Pueden cometerse en una jurisdicción sin estar físicamente presente en el territorio sometido a la misma, como se dijo más arriba. 4) A menudo, no son claramente ilegales. Esta indefinición puede proceder del mismo hecho (actos u omisiones no claramente delictivas por no configurar los tipos enumerados en los códigos) o de la intencionada falta de regulación de ciertos conductas por parte de Estados interesados en la instalación de paraísos cibernéticos.

b. Jurisdicción y soberanía en la WWW

Uno de los problemas que plantea al jurista la WWW es la elección de la jurisdicción y la ley aplicable a los hechos – actos y omisiones –, negocios jurídicos perfeccionados en la red y, dentro de nuestro ámbito de estudio, las infracciones de naturaleza penal perpetradas en el ciberespacio.

En la comisión de un ciberdelito en la WWW intervienen numerosos agentes. De modo resumido, podríamos establecer una relación cuadrangular. (A) El sujeto de quien parte la acción –normalmente desde un ordenador situado en su ámbito doméstico o

profesional – en cuya mente se origina la idea de perpetrar una acción (rara vez una omisión) antijurídica. Por sí mismo (A) no podría acometer su proyecto delictivo. Necesita un proveedor de servicios de Internet (B) – o ISP[29] por el acrónimo inglés de *Internet Service Provider* – que conectará al usuario, a través de la línea telefónica, a Internet. Por último esa información ofensiva, dispositivo pernicioso o imagen inmoral viajarán por las autopistas virtuales y se alojarán en servidores web[30] (C), que se almacenarán en el disco duro de las plataformas a disposición de sus autores, estos servidores se denominan Web Hosts. En muchas ocasiones, las empresas (B) y (C) coinciden, siendo también frecuente que la empresa ISP sea la misma que la que ofrece el servicio telefónico doméstico. Por último, en este escenario virtual, entra en juego el sujeto pasivo del delito (D), que en su propio ordenador recibirá las ofensas o el dispositivo pernicioso – vgr. un dañino virus que destruye los datos o que reenvía información confidencial e íntima al sujeto activo del delito- o, desde ese mismo ordenador resulta estafado.[31] Este sujeto pasivo puede serlo sin necesidad de intervenir en este protocolo informático, incluso ignorando que sus imágenes o que la información confidencial que le concierne se encuentra circulando por la red.

En esta estructura simple, que bien puede remedar la de cualquier delito tradicional, adivinamos unos elementos distorsionadores. El sujeto activo (A) puede cometer el delito desde un Estado diferente al que se encuentra el sujeto pasivo (D). Puede que (A) desconozca, cuando inicia su comportamiento antijurídico, quien o quienes serán los finalmente perjudicados, o si estos serán pocos o muchos, sus nacionalidades o las jurisdicciones a las que pudieran pertenecer sus víctimas y qué consecuencias punitivas puede ocasionar su acción en cada país al que potencialmente pudiera recalar su acción (realmente todos los del globo.) Todavía cabe hacer otras reflexiones. El Web Host (C), utilizado como plataforma delictiva, puede –y es frecuente que así sea – situarse en un país distinto que el del sujeto activo, y a su vez este Web Host puede localizarse en un Estado distinto que al que pertenece el sujeto pasivo del delito (D.) Como hemos señalado más arriba, el Web Host puede auxiliarse de mirrors, lo que duplica el problema si ese servidor mirror se encuentra en un tercer Estado, y lo multiplica, si existieren varios mirrors en diversos países.

De un modo parco, esta propuesto el problema, de la jurisdicción y la ley aplicable. ¿A qué jurisdicción corresponderá el enjuiciamiento de tales delitos? ¿A la propia del sujeto activo, a la del Web Host, o a una –o a cualquiera- de las que correspondería a los perjudicados por la acción antijurídica?

c. Camino de la ciberfrontera.

En un ámbito huérfano de regulación, como el presente, las reglas sobre jurisdicción y competencia vienen dadas por los propios tribunales, a los que llegan las denuncias, las querellas y, en su caso, tratándose de asuntos civiles, las demandas.

Pocas sentencias habían levantado tanto debate doctrinal como la pronunciada por el Tribunal de Grand Instance de París, presidida por el juez Jean-Jacques Gómez, en mayo de 2000. Dicho tribunal ordenó al portal estadounidense Yahoo.com bloquear el acceso desde Francia a su Website norteamericana, a fin de impedir que los usuarios franceses participaran en subastas que tenían por objeto artículos relacionados con el nacionalsocialismo[32]. La versión francesa de Yahoo.com cumplió fielmente con la resolu-

ción. Sin embargo, al no existir semejante infracción en los Estados Unidos, la versión norteamericana de Yahoo.com se negó a ejecutar la resolución del tribunal francés.[33]

Además de la discusión jurídica que originó la cuestión – a la que nos referiremos más abajo – el asunto abrió una polémica de naturaleza tecnológica. ¿Había alcanzado el estado de la técnica un nivel de desarrollo tan avanzado que permitiera la discriminación de usuarios en sus accesos a la WWW?, o lo que es lo mismo (en lo que al Derecho Internacional se refiere), ¿sería posible la creación de ciberfronteras a semejanza de las fronteras tradicionales terrestres? Indudablemente la cuestión no es baladí. La erección de ciberfronteras tendría una importante repercusión en lo que al Derecho transnacional se refiere – el Derecho Comunitario – pues debería conjugarse con la supresión de fronteras terrestres previstas en los tratados fundacionales comunitarios. El comité de expertos nombrados *ex profeso,* se pronunció sobra la viabilidad de la resolución acordada por el Tribunal de París. Era posible que Yahoo.com implantara un sistema de identificación del origen de los usuarios, basándose en el IP de los ordenadores conectados, siempre y cuando, los usuarios franceses utilizaran en sus conexiones proveedores franceses, lo que sólo ocurriría en un 70% de los casos. Por tanto, la decisión del Tribunal de París, estaba destinada, *ab initio*, a no ejecutarse de un modo completo y fiable.[34]

La resolución del Tribunal se estrelló ante la jurisdicción estadounidense. El proveedor Yahoo.com norteamericano se personó en el Tribunal de Distrito de California – District Court of California– contra La Ligue Contre Le Racisme et L'Antisemitisme con objeto de que se declarase la decisión del tribunal francés inejecutable en Estados Unidos, y así lo estimó el basándose en que el tribunal francés no podía regular actividades de una corporación estadounidense con el único argumento de que a las mismas podían acceder usuarios desde Francia.[35]

No es objeto de este trabajo analizar las razones que apreciaron uno y otro tribunal para sostener su competencia en la cuestión planteada. Tan sólo se pretende ilustrar la laguna normativa existente en la esfera internacional sobre la jurisdicción competente en materia de cibercrímenes y, cómo las continuas disputas entre tribunales que pretenden atraer la sustanciación de las causas a sus foros, crean una patente inseguridad jurídica. El ofendido por un ciberdelito carece de instrumentos fiables para determinar *a priori* a qué jurisdicción debe someter su reclamación, a qué tribunal dentro de una jurisdicción, qué legislación criminal o civil debe invocar. Y una vez lo decida, una eventual sentencia condenatoria podría quedar inejecutada. He de resaltar que, debido a las características de la ley penal, jurisdicción y ley aplicable coinciden, pues ningún tribunal aplicaría una norma penal extranjera, cosa que puede ocurrir en materia derecho de privado.

La resolución del tribunal de París abrió el debate de la jurisdicción y ley aplicables. La naturaleza de la WWW permite la adopción de tres criterios para determinar la jurisdicción competente.[36] 1) La del país desde donde se suben los archivos ofensivos (país de emisión.) 2) La del país donde se descargan los contenidos (país de recepción.) 3) O la del país donde se encuentra el público al que se dirige la website.[37] Otras posturas jurisprudenciales más recientes, emanadas de resoluciones de tribunales estadounidenses matizan estos criterios gruesos, añadiendo los rasgos de interactividad de la websi-

te[38], de la intencionalidad manifiesta del responsable de la página Web[39], o incluso usando la doctrina del potencial efecto del delito.[40]

Los conflictos legales se agravan exponencialmente por el hecho de que muchos ordenamientos nacionales otorgan a sus propias jurisdicciones competencia sobre asuntos penales basándose en el principio de peseguibilidad universal, sin sujetarse al criterio de territorialidad. Esta distorsión sería aplicable en muchos países con respecto a asuntos relaciones con la pornografía infantil y el terrorismo.[41]

Lo expuesto pone de relieve la frágil regulación sobre jurisdicción y ley aplicable cuando tratamos con cibercrímenes. Si bien en el campo del derecho privado existe una regulación, más o menos acertada, que rige en materia de contratos, de responsabilidad extracontractual, etc.[42], el derecho penal aparece desprovisto de esa mínima solvencia, dándose la paradoja de que, precisamente por los bienes jurídicos barajados, es en el derecho público donde debería existir una mayor claridad y seguridad.

D. Unión Europea. Espacio de Libertad, Seguridad y Justicia en la Sociedad de la Información.

Las instituciones europeas han sido pioneras en la regulación de la Sociedad de la Información, pero ha eludido –porque en el campo del Derecho Penal tienen mermadas las competencias—una completa normativa sobre cibercrimen. Se ha discutido, desde la presentación del informe Sieber, *Legal Aspects of Computer-Related Crime in the Information Society – COMCRIME – Study,* preparado por encargo de la Comisión europea[43], sobre la procedencia de promulgar una normativa comunitaria que afecte, directa o indirectamente, a la esfera penal. Los instrumentos legislativos de la Comunidad Europea –reglamentos, directivas y decisiones—se han considerado insuficientes para regular delitos y penas, parcela tradicionalmente reservada a la soberanía de los Estados. El informe Sieber sostiene que, con base en los tratados fundacionales, es posible afectar al Derecho Penal, al menos de forma directriz y al objeto de lograr una normativa homogénea en el territorio de la Unión.

La lucha contra el cibercrimen ha de partir desde el derecho material, mediante normativas marco (reflejadas en convenios internacionales y, en su caso, en la legislación comunitaria) que persigan una regulación homogénea en todos los Estados (evitando en lo posible el mantenimiento y creación de paraísos cibernéticos y una diferencia punitiva de un país a otro.) De forma paralela, es necesario arbitrar mecanismos que resuelvan los conflictos de jurisdicción y reforzar los instrumentos de cooperación policial y judicial en materia de cibercrimen, reinterpretando la regulación internacional existente y, cuando ello no sea posible, elaborando nuevas disposiciones o celebrando nuevos tratados sobre la materia.

I Homogeneidad normativa. El Convenio Europeo sobre Cibercriminalidad.

La efectiva lucha contra el cibercrimen ha de partir desde planteamientos comunes en todos los estados. Sería poco eficaz castigar cierta conducta duramente en un Estado mientras que el Derecho de Penal de otros Estados mantuviera posiciones permisivas frente al cibercrimen. Quien pretenda delinquir acudirá a aquellos países cuyos ordena-

mientos amparen o, por lo menos, no persiguen tan rigurosamente el cibercrimen como en otros.

La conciencia compartida de que el cibercrimen desborda fronteras y se ha convertido, por esta razón, en un problema global ha impulsado a numerosos organismos internacionales ha plantearse la cuestión desde una perspectiva más realista y eficaz. La Organización para la Cooperación y Desarrollo Económico (OCDE), Interpol, el Consejo de Europa, la Organización de Naciones Unidas y la Unión Europea, dentro de sus ámbitos geográficos y respectivas competencias, han desarrollado verdaderas políticas de lucha coordinada contra la cibercriminalidad. En 1983 un grupo de expertos se reunió y recomendó que la OCDE tomara la iniciativa en el propósito de lograr una armonización sobre los delitos informáticos. En este marco se realizó un estudio que fructifica en el informe de 1986, "Computer-related Crime: Analysis of Legal Policy"[44], que recoge las normas penales existentes en diversos países, proponiendo reformas y recomendado un mínimo de ilícitos que debieran ser prohibidos y castigados por la ley penal. El Consejo de Europa toma el testigo y estudia la materia desde 1985 a 1989, por medio un de comité nombrado expresamente para ese propósito[45], y bosqueja la Recomendación 89(9), que se adopta definitivamente el 13 de septiembre de ese año.[46] Este parco instrumento anima a los Estados miembros del Consejo de Europa a mejorar la cooperación legal con objeto de armonizar normativas que respondan al nuevo reto emergente del cibercrimen. Coincidente con este objetivo de armonización mediante la unificación de líneas maestras uniformes y modernización de la normativa penal, en el seno de la Organización de las Naciones Unidas (Octavo Congreso sobre Prevención del Crimen y el Tratamiento de los delincuentes dirigido a los problemas legales planteados por el cibercrimen) se adopta una pionera Resolución el 14 de diciembre de 1990, que invita a los gobiernos a contemplar en sus regulaciones nacionales las resoluciones adoptadas en el Octavo Congreso.

Desde entonces se han venido sucediendo los estudios, informes, resoluciones no vinculantes, elaborados desde diversas organizaciones internacionales. Todos estos instrumentos se caracterizaban por su contenido dogmático, de escasa eficacia práctica, pues se partía del principio elemental del monopolio estatal en la promulgación de normas penales, sin embargo, paulatinamente, se va logrando el ansiado "consesus crimes", esto es, delitos caracterizados por su punibilidad en cualquier país participante en los foros mencionados. El crimen armonizado queda definitivamente plasmando en el Convenio Europeo sobre Cibercriminalidad hecho en Budapest el 23 de noviembre de 2001[47], adoptado en el seno del Consejo Europa, aunque entre su signatarios existen países no europeos, como Estados Unidos, Japón, República Sudafricana o Canadá.[48]

El Convenio no define el crimen para el que busca armonización, sino que se limita enumerar nueve categorías de ofensas y exhorta a las partes signatarias, de forma imperativa[49], a adoptar cuantas medidas legislativas o de otra naturaleza, fueran necesarias, para prever como infracción penal, conforme a su derecho interno, aquellas infracciones contempladas en el tratado. Las nueve categorías se refieren a ocho delitos contra la propiedad y a un delito que carece de esta connotación: acceso ilícito, interceptación ilícita, atentados contra la integridad de datos, atentados contra la integridad del sistema, abuso de equipos e instrumentos técnicos, falsedad informática, estafa informática, infracciones relativas a la pornografía infantil, infracciones vinculadas a los

atentados contra la propiedad intelectual y derechos afines.[50] La implementación de tales medidas legislativas implica la incorporación de nuevos tipos penales a los códigos nacionales y convertir en ilícitas conductas que, hasta entonces, se encontraban huérfanas de regulación o precariamente contempladas en los ordenamientos.

Realmente, de la enumeración de delitos *supra* mencionada, sólo los cinco primeros tienen la connotación de ser efectivamente nuevos[51], y requieren para su inclusión en el catálogo de conductas punibles proscribir, en cuanto al acceso ilegal, la intromisión electrónica, la piratería informática (*hacking*). La regulación de la interceptación ilícita requiere prohibir la invasión electrónica de la intimidad con o sin quebrantamiento de medidas de seguridad. Las disposiciones sobre los atentados contra la integridad de datos, necesitan la previa regulación de una propiedad virtual: la propiedad sobre las bases de datos. Las provisiones sobre los atentados contra la integridad del sistema han de contener particulares delitos que no guardan semejanza con los perpetrados en el medio terrestre: diseminación de virus, programas dañinos o códigos maliciosos (*debugs codes.*) La legislación penal sobre abuso de equipos e instrumentos técnicos requiere criminalizar la producción, venta, importación, distribución e, incluso, al mera tenencia de herramientas y dispositivos destinados a dicha comisión.

Los tres siguientes delitos, si bien se relacionan con los anteriores, en su marcado carácter económico —delitos contra la propiedad—, no se caracterizan por ser delitos de nueva planta. Tanto la falsedad informática, la estafa informática, como las infracciones vinculadas a los atentados contra la propiedad intelectual, actualizan los delitos convencional sobre la base de las nuevas tecnologías.

La única infracción contemplada en el tratado, ajena por completo a la protección del derecho de propiedad, es la conducta relativa a la pornografía infantil que para perseguirse eficazmente, en el contexto del ciberespacio, requiere modernizar el concepto de "producción, distribución y/o posesión de pornografía infantil".

El Convenio, en definitiva, se consagra como el instrumento más poderoso en la lucha contra el cibercrimen a nivel mundial, al no ser un instrumento exclusivamente europeo. Todos los Estados miembros de la Unión Europea han firmado el Convenio, sin embargo su eficacia está por ver ya que, hasta le fecha, pocos Estados signatarios han ratificado el tratado.

II La Unión Europea y el Cibercrimen.

Conviene, antes de continuar, exponer brevemente ciertos conceptos que se repetirán a lo largo de las líneas que siguen. A la Unión Europea se la compara gráficamente con la arquitectura de un templo griego.

El *frontispicio o frontón* comprende el Título I del Tratado de la Unión Europea (TUE), donde se encuentran los objetivos, principios y elementos constitutivos de la UE. Ese frontón está sostenido por tres grandes pilares.

El primer pilar (Títulos II al IV del TUE) alberga a las Comunidades Europeas y arrastra el articulado contenido en los Tratados Fundacionales: el Tratado de la Comunidad Europea (TCE), el Tratado de la extinta Comunidad Europea del Carbón y del Acero y el Tratado de la Comunidad Europea de la Energía Atómica.

El Título V del TUE se refiere al segundo pilar, consagrado a la Política Exterior y de Seguridad Común (PESC).

Y por último, la edificación de este templo griego culmina con el tercer pilar de la Unión: la Cooperación Policial y Judicial en Materia Penal (Título VI del TUE).

En lo que concierne al cibercrimen, el análisis emprendido se detendrá en el primer y en el tercer pilar, cuyas normativas permitirían diseñar, al menos, una embrionaria regulación marco sobre el fenómeno de la cibercriminalidad transnacional.

a. Cibercriminalidad en el marco del Primer Pilar.

Dentro de este primer pilar de la Unión Europea, existe una base jurídica para luchar, si no contra todos, sí contra algunos de los llamados cibercrímenes. Si bien es dentro del TUE, y más concretamente, en el marco de su Título VI –tercer pilar- donde habrá de articularse un coherente sistema de normas e instrumentos prevención y persecución del cibercrimen, el TCE también ofrece base jurídica para una regulación de la materia con el fin de salvaguardar los objetivos fundacionales de la Comunidad Europea. En especial, los de establecimiento de un mercado común (art. 2 TCE) que implicaría, entre otros, a tenor del artículo 3 del TCE:

> c) un mercado interior caracterizado por la supresión, entre los Estados miembros, de los obstáculos a la libre circulación de mercancías, personas, servicios y capitales;
>
> g) un régimen que garantice que la competencia no será falseada en el mercado interior;
>
> h) la aproximación de las legislaciones nacionales en la medida necesaria para el funcionamiento del mercado común;
>
> k) el fortalecimiento de la cohesión económica y social;
>
> m) el fortalecimiento de la competitividad de la industria de la Comunidad;
>
> t) una contribución al fortalecimiento de la protección de los consumidores;

Para el desarrollo de estos objetivos la Comunidad dispone de un poderoso instrumento: la posibilidad de adoptar directivas con objeto de aproximar (¿armonizar?) disposiciones legales, reglamentarias y administrativas de los Estados miembros que incidan directamente en el establecimiento o funcionamiento del mercado común (art. 94 TCE.)[52] Esta facultad corresponde al Consejo, que podrá dictar las directivas armonizadoras por unanimidad o, conforme al artículo 95.1. del TCE, por el régimen de mayoría cualificada establecido en el artículo 251 del TEC, previa consulta del Comité Económico y Social[53], cuando la materia afecte a los objetivos señalados en el artículo 14 TCE, concretados en *la creación de un espacio sin fronteras interiores, en el que la libre circulación de mercancías, personas, servicios y capitales estará garantizada de acuerdo con las disposiciones del presente Tratado.*

El número 3, del artículo 95, ofrece un marco jurídico que podría aplicarse al cibercrimen:

> La Comisión, en sus propuestas previstas en el apartado 1 referentes a la aproximación de las legislaciones en materia de salud, seguridad, protección del medio ambiente y protección de los

> consumidores, se basará en un nivel de protección elevado, teniendo en cuenta especialmente cualquier novedad basada en hechos científicos. En el marco de sus respectivas competencias, el Parlamento Europeo y el Consejo procurarán también alcanzar ese objetivo.

Este artículo debe conjugarse, coherentemente, con el artículo 153 del TCE, bajo el Título XIV, rubricado como «Protección de los consumidores». Dicho artículo, en su número 1, establece que

> Para promover los intereses y garantizarles un alto nivel de protección, la Comunidad contribuirá a proteger la salud, la seguridad y los intereses económicos de los consumidores, así como a promover su derecho a la información, a la educación y a organizarse para salvaguardar sus intereses.

El número 3 de dicho artículo 153 remite al marco regulado en el artículo 95 TCE — que ya hemos señalado más arriba — para la adopción de las medidas dirigidas a alcanzar los objetivos propuestos.

A la luz de tales preceptos surge varias preguntas: ¿existen ciberdelitos que pueden afectar al mercado interior, especialmente cuando atentan contra los derechos de los consumidores? ¿Es suficiente el marco ofrecido por los artículos TCE *supra* mencionados para que la Comunidad pueda, por medios de directivas, armonizar o aproximar las distintas legislaciones penales de los Estados miembros?

Se ha discutido arduamente sobre la posibilidad de que la Comunidad ostente competencias, si quiera tangencialmente, en materia penal. Muchos son los argumentos en contra, pero sobre todos se yerguen aquellos que defienden que la materia penal es una parcela tradicionalmente reservada a la soberanía de los Estados, ejerciendo esta competencia en régimen de monopolio infranqueable. Sólo, por medio de Tratados celebrados *ex profeso* (vgr. el ya nombrado Convenio sobre cibercriminalidad), un Estado podría obligarse a dictar normas penales sobre alguna materia, pero, en última instancia, sería el propio Estado el que mediante una acto soberano promulgara la norma penal destinada a regir en un ámbito estrictamente nacional. Las directivas comunitarias, a las que se refieren los artículos 94 y 95 del TCE, si bien no tendrían un efecto directo sobre los nacionales de los Estados miembros, sí desplegarían una obligación de trasposición sobre los Estados que entraría en conflicto con la soberanía particular de cada Estado.

Muchas competencias atribuidas a la Comunidad Europea no son exclusivas. Estas «competencias compartidas» se conjugan con el principio de «subsidiariedad», introducido por el Tratado de Maastricht, que postula que, empero haber atribuido competencias a la Comunidad en algún campo concreto, ésta sólo esta facultada para promulgar normas si los Estados miembros no han alcanzado un adecuado grado de cumplimiento de los objetivos perseguidos por la Comunidad. El principio de «subsidiariedad» persigue que acción de la Comunidad añada un valor superior que el que pudieran obtener los Estados actuando sobre la materia individualmente. La regulación de la Sociedad de la Información, tanto en su faceta civil, administrativa o penal, cumple las condiciones para la estricta aplicación del principio de subsidiariedad. Una materia que en esencia desborda las fronteras de cada estado y sólo podría normarse eficazmente desde una perspectiva transnacional o internacional.

Debemos preguntarnos si, bajo el actual marco jurídico, la Comunidad Europea podría promulgar directivas que contemplasen sanciones penales o, al menos, administra-

tivas. Una pregunta tan global y genérica como esta sólo tendría una respuesta de semejantes características: la Comunidad Europea, en principio, carece de facultades sobre la ley penal, no existiendo en el extenso articulado de los tratados fundacionales (el TUE con su frontispicio y tres pilares) mención alguna sobre una supuesta competencia de tal índole. Si descomponemos la pregunta genérica en otras más precisas, es posible que sí encontremos esa competencia, atribuida directa o indirectamente, a la Comunidad. Distinguiendo entre prohibición y sanción, **sí podemos afirmar que la Comunidad tendría facultades para establecer prohibiciones o para compeler a cumplir ciertas obligaciones o deberes**; prohibiciones u obligaciones que más tarde los Estados miembros habrían de trasponer al Ordenamiento interno y asociarles la correspondiente sanción penal o administrativa.

Sieber pone de manifiesto (1998: 214) que muchas directivas, reguladoras de muy diversas materias, establecen prohibiciones u obligaciones que deben cumplirse —que realmente constituyen los prerrequisitos de una eventual norma penal nacional—, directivas que suelen adoptarse en el marco de la armonización económica, sin llegar a regular las correspondientes sanciones detalladamente. Se aprecia esta estructura en la Directiva 2003/6/CE del Parlamento Europeo y del Consejo, de 28 de enero de 2003, sobre las operaciones con información privilegiada y la manipulación del mercado (abuso del mercado), cuando exhorta a los Estados a establecer un elenco de sanciones administrativas que castiguen las transgresiones, "sin perjuicio del derecho de los Estados miembros a imponer sanciones penales.[54] Más cercana al ámbito de nuestro estudio, la Directiva 2001/29/CE del Parlamento Europeo y del Consejo, de 22 de mayo de 2001, relativa a la armonización de determinados aspectos de los derechos de autor y derechos afines a los derechos de autor en la sociedad de la información, se pronuncia en semejantes términos. El artículo 8.1. de esta última norma establece que los

> Estados miembros establecerán las sanciones y vías de recurso adecuadas en relación con la violación de los derechos y las obligaciones previstos en la presente Directiva y adoptarán cuantas disposiciones resulten necesarias para garantizar que se apliquen tales sanciones y vías de recurso. Las sanciones deberán ser efectivas, proporcionadas y disuasorias.

Con mayor amplitud que la Directiva sobre abuso de mercado, tal vez previendo las implicaciones penales, la Directiva 2001/29/CE utiliza el término sanción, lo que, terminológicamente no excluye las sanciones criminales.[55] Es más, el segundo párrafo del mismo artículo 8, parece referirse a esta jurisdicción cuando habla de incautación del material ilícito y los dispositivos, productos o componentes, siendo que estas medidas generalmente se adoptan en el ámbito del proceso penal. La exposición de motivos de esta directiva alude específicamente al artículo 95 TCE como presupuesto jurídico de su adopción.

Según Sieber la previsión del artículo 14 TCE refuerza el principio de mercado común, cuando se habla en dicho artículo del establecimiento progresivo de un mercado interior que implicará un espacio sin fronteras interiores, en el que la libre circulación de mercancías, personas, servicios y capitales estará garantizada de acuerdo con las disposiciones del Tratado.

A la luz de los artículos mencionados es evidente el espíritu del Tratado. Se pretende la creación de un mercado interior — o común — donde no se falsee la competencia

(art. 81 TCE), donde las empresas establecidas libremente (art. 43 TCE) queden sometidas a normas restrictivas semejantes — como son aquellas que castigarían los cibercrímenes — pues de lo contrario se patrocinaría una migración empresarial hacia los Estados miembros que no contemplasen tales infracciones o que asociasen a las mismas sanciones más leves. En virtud del principio de subsidiariedad, la Comunidad encuentra en la Directiva un instrumento adecuado — aunque no suficiente, como más adelante veremos — para establecer una mínima estructura para luchar eficazmente contra aquellos cibercrímenes de claro contenido económico, logrando la armonización de legislaciones. La pasividad comunitaria en este campo afectaría indiscutiblemente al mercado común.

Naturalmente, las previsiones del TCE no podrían aplicarse a todos los ciberdelitos. Tan sólo comprendería aquellos con un claro contenido económico o que atenten contra los derechos difusos de una pluralidad de personas — por ejemplo, los consumidores —. SIEBER enumera gruesamente tres tipos de acciones sobre las que podría recaer una eventual política armonizadora de la Comunidad: delitos económicos, contenidos ilícitos o dañosos y la debatida cuestión de la responsabilidad de proveedores de acceso y de servicios Web.

El evidente que el mercado común puede verse seriamente comprometido por el desarrollo de delitos económicos. En lo que se refiere a delitos económicos cometidos a través de la WWW, baste citar el fraude informático, el robo, el falsificación, el computer hacking, el espionaje informático, el sabotaje y extorsión informáticos, la piratería comercial y otros crímenes contra la propiedad intelectual afectan al mercado común de una manera creciente, pues el número de transacciones *online* aumenta de forma exponencial debido al acceso a las nuevas tecnologías de todos los sectores de la población. La existencia de paraísos del cibercrimen en el ámbito comunitario — Estados con escaso nivel de protección — destruye la competencia perfecta y coloca a unos Estados en un grado de productividad superior (así, por ejemplo, los servidores situados en paraísos cibernéticos no deberían adoptan grandes medidas de seguridad, lo que reduciría sus costes de explotación.) Es lógico pues que la Comunidad deba tomar partido adoptando medidas protectoras sobre las redes informáticas, estableciendo una regulación precisa sobre la firma digital y un estándar de seguridad mínimo que proteja las redes instaladas en el territorio de la Unión Europea.

Más lejana queda la competencia comunitaria de establecer prohibiciones sobre contenidos ilícitos o perjudiciales sobre la base del mercado común. Sin embargo, a poco que razonemos al respecto podemos hallar fundados puntos de conexión cuando la distribución de tales contenidos — generalmente imágenes pornográficas en forma de fotografías y películas autorreproducibles o textos difamatorios — se realice de forma remunerada a través de cualquier sistema de pago aplicable a la WWW (especialmente, mediante pago con tarjeta de crédito o débito.) Estas actividades caen dentro del concepto amplio de prestación de servicios, contemplada en el art. 49, y cualquier limitación a las mismas, basada en normativas nacionales reguladores de la moral o la protección a la infancia, que no se viera reproducida de forma semejante en todos los Estados miembros, forzaría la migración de tales proveedores a Estados con regulación más liviana, no lográndose el efecto prohibitorio pretendido, distorsionando gravemente la competencia. Hemos de decir que este negocio, lejos de se residual, mueve una in-

gente cantidad de dinero y se ha propagado vertiginosamente en el favorable entorno de Internet. La información fluida proporcionada por la WWW puede hacer que, a pesar de que en el Estado origen de los contenidos no exista prohibición ni sanción, su accesibilidad desde otros Estados menos permisivos puede producir importante conflictos de jurisdicción: el Estado receptor siempre intentará aplicar su norma, administrativa o penal, a lo que él considera una infracción. La eventual persecución criminal de los administradores de tales compañías que desde la perspectiva de los Estados receptores ofrecen servicios ilegalmente, pero legalmente en el Estado de establecimiento, genera incertidumbre y la consiguiente reducción de intercambios comerciales online ante la posibilidad de ser sancionado dentro de la Unión Europea. Situación que afecta indudablemente a la fortaleza del mercado interior.

Ha sido una espinosa cuestión la regulación de la responsabilidad, tanto civil como criminal, de los proveedores de servicios de acceso a Internet y de espacio para desplegar contenidos (generalmente en forma de páginas Web.) El desarrollo de Internet se enfrentó con una disyuntiva inquietante: propagación de la Sociedad de Información velozmente, dejando la normativa a expensas de la autorregulación que hicieran los operadores del mercado o establecer desde el principio una regulación muy severa sobre los operadores con objeto de prevenir hipotéticos delitos que necesariamente se cometerían. Son obvias las consecuencias de la elección de una u otra opción. La primera propiciaría una deseable implantación de la Sociedad de Información en escaso lapso de tiempo, mientras que la segunda la ahogaría, pues pocas empresas tecnológicas se convertirían en proveedores dentro de un régimen muy restrictivo. Determinar la responsabilidad de los operadores por los contenidos ilícitos o dañinos que transportan o albergan no es cuestión baladí. Significaría convertir a tales empresarios en guardianes de la honestidad, impidiendo el acceso de contenidos a sus sistemas basándose en su particular concepción de la moralidad, de las buenas costumbres o de la protección a la juventud y la infancia. Reservándose un derecho de admisión, se podrían conculcar elementales derechos constitucionales como el de la libertad de expresión, de enseñanza, de acceso a la cultura, y otros. Atenta pues al mercado común la existencia de diferentes legislaciones al respecto, cuando unas son más rigurosas que otras, pues por los mismos y repetidos motivos *supra* mencionados se distorsionaría la competencia. En este caso, la armonización auspiciada por la Comunidad se ha dirigido a liberar de responsabilidad a los operadores, tal como recomendó Sieber en su renombrado trabajo (1998 : 226), no respondiendo de los contenidos ilícitos o dañosos provenientes de los usuarios. Residualmente sólo responderían por sus propios contenidos o cuando los albergaran o dieran acceso contraviniendo órdenes de autoridades. La *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 (Directiva sobre el comercio electrónico)* recoge estos principios y constituye la piedra angular de la exención de responsabilidad — al menos en el ámbito de la Unión Europea — de los proveedores de servicios en Internet.[56]

De lo expuesto más arriba podemos identificar una efectiva competencia comunitaria para determinar prohibiciones, independientemente de que a éstas de les asocie una sanción penal o administrativa. **Pero conviene referirnos, como lógica continua-**

ción a lo dicho, a la posibilidad de que la Comunidad pueda establecer verdaderas sanciones por sí misma, aunque sólo sean de índole administrativa o, dicho de otro modo, analizar si las Comunidades Europeas podrían promulgar sanciones penales o, al menos, administrativas?

Sobre esto la doctrina jurídica comunitaria no es pacífica. El principio general "nullum crimen sine lege" ha sido un poderoso argumento en contra del reconocimiento de esta competencia comunitaria por la vía del **Reglamento.** El establecimiento de normas criminales supone un intrusión severa en los derechos fundamentales y las libertades públicas, por lo que la limitación que entrañan sobre tales derechos debe venir amparada por órganos democráticos, y ni el Consejo de Ministros ni la Comisión, principales artífices de las normas comunitarias, se encuentran revestidos de origen indiscutiblemente democrático[57] Parece una cuestión pacífica el que la esfera criminal no ha sido conferida a los órganos transnacionales y se mantiene irrevocablemente en poder de los Estados miembros. No obstante se observan decididos avances que acercan a los órganos comunitarios a la categoría de creadores de leyes penales. En este sentido cabe señalar que el Tratado de Ámsterdam supone la creación de un tímido marco, desde el propio tratado constitutivo, sobre el que adoptar medidas penales, pero sólo contra actuaciones que supongan un fraude o actividad ilegal y que afecten a los intereses financieros de la Comunidad (art. 280.) «Estas medidas deberán tener un efecto disuasorio y ser capaces de ofrecer una protección eficaz en los Estados miembros». Para esta lucha los Estados miembros adoptarán las mismas medidas que para combatir el fraude que afecte a sus propios intereses financieros.[58] Puede constituir un plan aceptable y abra una puerta a una mayor competencia en materia criminal (y por ende a la armonización y a la eficacia). Pero hasta ahora las previsiones sólo son predicables cuando los ataques afecten a los intereses financieros de la Comunidad y no se confiere expresamente facultad normativa en materia criminal, lo que nos sigue colocando en el terreno de la indefinición.[59]

Dicho esto, por el momento, se descarta la facultad de la Comunidad de establecer sanciones penales mediante el instrumento normativo del Reglamento. Cosa distinta es la posibilidad de establecer sanciones administrativas mediante dicho instrumento. A este respecto sí existen previsiones en el TCE aunque circunscritas a ámbitos muy concretos. En el terreno de la libre competencia, el artículo 83 faculta al Consejo para adoptar, por mayoría cualificada y a través de reglamentos y directivas, medidas contra acciones empresariales que atenten contra el mercado común[60], incluyendo "el establecimiento de multas y multas coercitivas". Con base en dicho artículo se han promulgado Reglamentos, que han sancionado las prácticas prohibida mediante multas[61], pero la cuestión radica en si esta facultad puede extenderse a otras materias. Para SIEBER, la disputa no es jurídica si no de naturaleza meramente política[62] y, no parece que por ahora, salvo en los casos expresamente establecidos, los Estados consientan en despojarse de sus atributos sancionadores, propios de su soberanía; cosa que no ocurriría tan rigurosamente si la participación de las instituciones comunitarias se hiciera por medio de directivas, ya que en última instancia serían los propios estados quienes deberían implementar las sanciones en su ordenamiento interno (y a través de los cauces constitucionales domésticos).

En este último supuesto, ¿sería factible la promulgación de directivas comunitarias que establecieran verdaderas sanciones, criminales? La pregunta puede formularse en otros términos. ¿**Puede la Comunidad Europea exigir, mediante una directiva, a sus Estados miembros, la adopción de sanciones penales en sus territorios para conductas que la propia Comunidad ha prohibido, en función de su intervención armonizadora?**

Es notable el influjo que ejercen las normas comunitarias sobre la legislación criminal de cada país, si bien este vínculo no aparece siempre como visible. Así, corrientes proteccionistas, o defensoras de los derechos humanos, que se han originado en el seno de las Comunidades han tenido repercusión en la normativa penal de los Estados miembros, pero de un modo indirecto y voluntario (sin existir un mandato de trasposición de una sanción prevista en la directiva.)[63] Sin embargo, lo que pretenden estas líneas es abordar la cuestión de si la Comunidad puede imponer a sus miembros la obligación jurídica de sancionar una conducta prohibida. Desde la perspectiva del derecho interno la adopción de sanciones criminales, en este contexto, no contravendría la Constitución doméstica, pues en último término sería el propio Estado, a través del mecanismo constitucional pertinente, quien elaboraría y promulgaría la norma. Y en cuanto al derecho comunitario, no existe obstáculo que lo impida.

Como siempre, el TJCE, ha llenado de contenido el silencio que reside en el TCE sobre la cuestión. En la sentencia de 12 de septiembre de 1989, asunto 68/88 , el TJCE sobre la base el artículo 10 (entonces artículo 5) condenó a la República Helénica por no haber promulgado las normas sancionadoras apropiadas, aun cuando la norma originaria no compeliera expresamente al establecimiento de las mismas.

> En su considerando 23º, el Tribunal destaca que, cuando una normativa comunitaria no contenga disposición específica alguna que prevea una sanción en caso de infracción o cuando remita en este aspecto, a las disposiciones legales, reglamentarias y administrativas nacionales, el artículo 5 del Tratado exige de los Estados miembros la adopción de todas las medidas apropiadas para asegurar el alcance y la eficacia del Derecho comunitario.
>
> Para ello (considerando 24º), aun conservando la elección de las sanciones, los Estados miembros deben procurar, en particular, que las infracciones del Derecho comunitario sean sancionadas en condiciones análogas de fondo y de procedimiento a las aplicables a las infracciones del Derecho nacional cuando tengan una índole y una importancia similares y que, en todo caso, confieran un carácter efectivo, proporcionado y disuasorio a la sanción.
>
> Además, en relación con las infracciones del Derecho comunitario, las autoridades nacionales deben proceder con la misma diligencia que utilizan para la aplicación de las respectivas legislaciones nacionales (considerando 25º)

Es de señalar que a lo largo de la sentencia, el TJCE emplea la expresión "procedimientos penales o disciplinarios", asumiendo pues que la facultad de elección de los Estados miembros de la sanción alcanza a la criminal.

Podemos concluir que bajo los principios consagrados en el artículo 5 TCE[64], de efecto útil y proporcionalidad, las Comunidades serían competentes para, por medio de directivas, requerir a los Estados miembros la adopción de sanciones criminales pero sólo contra infracciones armonizadas por la propia Comunidad, como más arriba he expuesto, y sólo en esos casos, y en la medida en que esa previsión vaya encaminada a

asegurar el cumplimiento último de las previsiones impuestas por el TCE (por ejemplo el art. 95) en las que se base la directiva.

Pese a esta posibilidad, hasta el de hoy no se ha promulgado directiva alguna que contemple la explícita obligación de imponer sanciones penales por los Estados miembros. Esta facultad atribuida a las Comunidades sólo se ha ceñido al establecimiento de sanciones administrativas. Además de las directivas más arriba citadas (que también prevén sanciones sin adjetivarlas), tampoco la Directiva 91/308/CEE sobre la prevención del blanqueo de capitales, contempla la imposición de sanciones específicamente penales, sino sólo sanciones genéricas.[65]

b. El cibercrimen dentro del Tercer Pilar.

La Unión Europea ha apostado decididamente por la Sociedad de la Información y del Conocimiento a través de grandes iniciativas, como el reciente programa *e*Europe 2002[66] y su normativa de implementación[67], o su sucesor *e*Europe 2005[68], que pretendían propagar la Tecnología de la Información y del Conocimiento a una velocidad vertiginosa. No cabe duda de que la evolución era necesaria pero la rápida implantación no vino acompañada de medidas que impidieran la cibercriminalidad en ciernes, sino que estas medidas se fueron adoptando después de que se constataran los resultados criminales. En abril de 1998, la Comisión alertó al Consejo, mediante un estudio sobre delincuencia informática (llamado estudio 'COMCRIME')[69]. En la Cumbre de Tampere, celebrada en octubre de 1999, el Consejo Europeo concluye que la labor para acordar definiciones y sanciones comunes debe incluir la delincuencia de alta tecnología. Semejante impulso vino de parte del Parlamento Europeo y del Consejo. Este último mediante la Posición común 1999/364/JAI *relativa a las negociaciones relativas al proyecto de convenio sobre criminalidad en el ciberespacio que se celebran en el Consejo de Europa*[70], reunió algunos de los elementos definitorios, de lo que más tarde sería el propio Convenio, como parte de su estrategia dirigida a combatir el cibercrimen.

No obstante estos esfuerzos, debe resaltarse que el Tratado de la Unión Europea (TUE)[71], no contiene mención explícita del cibercrimen, sin embargo, puede ofrecer un marco jurídico suficiente para regular el fenómeno, a través de posiciones comunes, decisiones marco, decisiones, o la celebración de convenios, actuaciones, todas ellas, que puede adoptar el Consejo de acuerdo a los límites y procedimientos establecidos en el Título VI del TUE.

Dentro del Título I «Disposiciones comunes» del TUE, el artículo 2 establece como objetivo de la Unión

> mantener y desarrollar la Unión como un espacio de libertad, seguridad y justicia, en el que esté garantizada la libre circulación de personas conjuntamente con medidas adecuadas respecto al control de las fronteras exteriores, el asilo, la inmigración y la prevención y la lucha contra la delincuencia.

La prevención y la lucha contra la delincuencia estarían incompletas si la Unión no desarrollara políticas de lucha contra el cibercrimen. El Título VI TUE, que lleva por rúbrica «Disposiciones relativas a la cooperación policial y judicial en materia penal», contiene varias previsiones que afectan a la prevención y lucha contra la ciberdelincuencia. El artículo 29 establece que

> Sin perjuicio de las competencias de la Comunidad Europea, el objetivo de la Unión será ofrecer a los ciudadanos un alto grado de seguridad dentro de un espacio de libertad, seguridad y justicia elaborando una acción en común entre los Estados miembros en los ámbitos de la cooperación policial y judicial en materia penal y mediante la prevención y la lucha contra el racismo y la xenofobia.
>
> Este objetivo habrá de lograrse mediante la prevención y la lucha contra la delincuencia, organizada o no, en particular el terrorismo, la trata de seres humanos y los delitos contra los niños, el tráfico ilícito de drogas y de armas, la corrupción y el fraude, a través de:
>
> -una mayor cooperación entre las fuerzas policiales, las autoridades aduaneras y otras autoridades competentes de los Estados miembros, ya sea directamente o a través de la Oficina Europea de Policía (Europol), de conformidad con lo dispuesto en los artículos 30 y 32,
>
> -una mayor cooperación entre las autoridades judiciales y otras autoridades competentes de los Estados miembros, también mediante la Unidad Europea de Cooperación Judicial (Eurojust), de conformidad con lo dispuesto en los artículos 31 y 32,
>
> -la aproximación, cuando proceda, de las normas de los Estados miembros en materia penal, de conformidad con lo dispuesto en la letra e) del artículo 31.

El ansiado «Espacio de libertad, seguridad y justicia», conforme a dicho artículo y en lo que atañe a la cibercriminalidad, sólo podrá alcanzarse mediante la elaboración de una acción común entre los Estados miembros en los ámbitos de la cooperación policial y judicial en materia penal, y la prevención y la lucha de la delincuencia, organizada o no, los delitos contra los niños (vgr. delitos relacionados con la pornografía infantil cometidos a través de Internet) y el fraude (entre estos, figuraría la estafa informática.) Las herramientas de las que dispone la Unión para la consecución de estos objetivos son la cooperación entre autoridades judiciales, aduaneras, o de cualquier otra clase y, por supuesto, fuerzas policiales y la aproximación, cuando proceda, de las normas de los Estados miembros en material penal. Respondiendo al primero de los propósitos, el artículo 30 contiene un mandato para desarrollar esta cooperación en el seno de la Oficina Europea de Policía (Europol)[72] así como por medio de Eurojust[73] y la colaboración de este último organismo con la Red Judicial Europea[74]. Con carácter general, el actual artículo 30, letra a), consagra la cooperación operativa entre las autoridades competentes, incluidos los servicios de policía, de aduanas y otros servicios especializados de los Estados miembros con funciones coercitivas, en relación con la prevención, localización e investigación de hechos delictivos.

Hemos de señalar que el artículo 4 de la Decisión del Consejo por la que se crea Eurojust[75] atribuye a este órgano competencias específicas sobre delincuencia informática.

La aproximación de legislaciones penales de los Estados miembros, contemplada en los artículos 29 *in fine* y 31, letra c) TUE, facilita, aunque no suficientemente, la necesaria armonización de tipos penales para la lucha contra la cibercriminalidad y previene los conflictos jurisdicción tan abundantes en la cibercriminalidad. En este sentido, constituyen acertadas previsiones la de la letra d) del artículo 31, cuando señala que la acción en común sobre cooperación judicial en materia penal, incluirá entre otras:

> c) la consecución de la compatibilidad de las normas aplicables en los Estados miembros, en la medida necesaria para mejorar dicha cooperación;
>
> d) la prevención de conflictos de jurisdicción entre los Estados miembros;

> e) la adopción progresiva de medidas que establezcan normas mínimas relativas a los elementos constitutivos de los delitos y a las penas en los ámbitos de la delincuencia organizada, el terrorismo y el tráfico ilícito de drogas.

En el desarrollo y cumplimiento de tales objetivos (reflejados en los arts. 30 y 31), el TUE prevé la actuación de autoridades de un Estado en otro, en colaboración y de acuerdo con las autoridades de este último, correspondiendo al Consejo establecer las condiciones y límites de la intervención (art. 32)

Las características del cibercrimen, *supra* descritas, requiere una armonización más amplia, no ceñida exclusivamente, como se deriva de la letra e) del articulo 31 TUE, a la delincuencia organizada (en nuestro caso, operativa a través de Internet) y al terrorismo (ciberterrorismo, en su faceta informática.)

Siguiendo a MANGAS MARTÍN y LIÑÁN NOGUERAS (2005: 386-388) los actos que puede adoptar la Unión Europea, por medio del Consejo, en el marco de la Cooperación en Asuntos de Justicia e Interior (CAJI) son cinco:

a) Las posiciones comunes, que definen el enfoque de la Unión sobre una asunto concreto [art. 34.2.a) TUE]

b) Las decisiones marco, que tendrán por objeto la aproximación de las disposiciones legales y reglamentarias de los Estados Miembros. Obligan a los Estados miembros en cuanto a los resultados, dejando a las Autoridades nacionales la elección de la forma y los medios [art. 34.2.b) TUE.][76]

c) Las decisiones que, al igual que las disposiciones precedentes, serán obligatorias y no tendrán efecto directo. Tienen un ámbito más amplio que las decisiones marco no pudiendo regular asuntos que caen bajo la competencia de estas. El art. 34.2.c) TUE contempla que las decisiones irán acompañadas de medidas (cuya forma no se precisa ni en el Tratado ni habitualmente en la práctica) que el Consejo adoptará para su aplicación.

d) Los convenios complementarios [art. 34.2.d) TUE] constituyen una fórmula que ha producido interesantes resultados en materia de cooperación penal. Mediante este instrumento jurídico, el Consejo celebra convenios (al que pueden acompañar medidas de aplicación) y recomienda su adopción a los Estados miembros según sus particulares sistemas constitucionales, abriéndose un periodo de ratificación. Se les denomina "Actos del Consejo por el que se establece el Convenio...".[77]

e) Por extensión del artículo 24 TUE, ubicado en el Título V (Disposiciones relativas a la política exterior y en seguridad común), se aplican los acuerdos con terceros propios de dicho Título al ámbito de la Cooperación Policial y Judicial en materia penal. Por vía de los acuerdos con terceros se podría luchar contra los paraísos cibernéticos, pero la instrumentación deja abierta muchas incógnitas por cuanto que es discutida la personalidad jurídica internacional de la Unión Europea.[78]

Por tanto, en lo que se refiere al cibercrimen, y de conformidad con el marco legal más arriba expuesto, el Consejo, por medio de acciones conjuntas, decisiones marco y convenios, puede regular una porción importante de la materia, activando los instrumentos y suministrando las competencias, para la persecución de los delitos informáti-

cos, especialmente aquéllos que se cometan a través de red, caracterizados por la transnacionalidad.

SIEBER (1998: 237, 238) se refiere, en concreto, a:

- Creación de unas mínimas reglas de derecho penal que establezcan estándares sobre los que armonizar la lucha contra el crimen informático, especialmente el que se produce en redes internacionales (o lo que es lo mismo, en la WWW.)

- Recomendación de adopción de medidas e instrumentos tecnológicamente apropiados para enfrentarse con la investigación del cibercrimen operado en redes internacionales (especialmente dificultosa cuando los datos viajan encriptados.)

- Abordar las investigaciones transfronterizas cuando los delitos se perpetran a través de red.

- Establecer un marco que impida que se originen conflictos de jurisdicción, tan frecuentes en el cibercrimen.

c. Derecho derivado en el marco de la Cooperación Policial y Judicial en materia penal.

I. Derecho sustantivo derivado.

Los actos adoptados en virtud del Título VI del TUE han proliferando en los últimos años al compás del desarrollo tecnológico. Al contrario de la normativa nacida del TCE, que, como se mostró más arriba, no se adentra en el castigo penal, dejando a discreción de los Estados la elección de sanciones para aplicar a las conductas prohibidos, el derecho derivado del Título VI TUE no se detiene en la sanción administrativa e impone con frecuencia la imposición de penas.

La Decisión 2000/375/JAI del Consejo, de 29 de mayo de 2000, relativa a la lucha contra la pornografía infantil en Internet[79]

La Decisión 2000/375/JAI, se enfrentaba al cibercrimen, relacionado con la pornografía infantil, de un modo programático y enunciativo. A lo largo de sus ocho artículos, establece una serie de medidas útiles pero insuficientes. De este modo, se contemplan medidas de participación ciudadana en la lucha contra la pornografía infantil, exhortando a los Estados a habilitar instrumentos de concienciación social y denuncia; a la actuación policial rápida; a la cooperación entre los Estados miembros para la facilitar la investigación y persecución de tan execrables delitos a través de puntos de contacto que funcionen 24 horas al día; la información puntual a Europol de los casos detectados. Se pretende la colaboración de los proveedores de servicios, para la cual los Estados deberán establecer las medidas y los cauces necesarios. Se insta a que se implementen los avances tecnológicos, a medida que progrese el estado del técnico, para desarrollar filtros de acceso de la pornografía y sistemas de detección. El plazo de trasposición al derecho interno finalizó el 31 de diciembre del año 2000.

La Decisión Marco 2005/222/JAI del Consejo, de 24 de febrero de 2005, relativa a los ataques contra los sistemas de información[80]

La Decisión Marco 2005/222/JAI, aborda, categóricamente pero con simpleza (en sólo trece artículos), los grandes problemas que atañen a la lucha contra el cibercrimen: la armonización normativa que, esta decisión, abraza a la materia penal y, por fin, se enfrenta a la transcendental cuestión de la competencia. Si bien la Decisión no

comprende todos los delitos informáticos, en cuanto a los demás, marca el camino a seguir por futuros instrumentos normativos. [81]

Cada Estado adoptará las medidas necesarias para que sean castigadas como infracción penal, el acceso intencionado sin autorización a sistemas de información (art. 2); la intromisión intencionada, y no autorizada, en sistemas de información a fin de de obstaculizar o interrumpir de manera significativa el funcionamiento de los mismos (art. 3); la intromisión intencionada y no autorizada en datos informáticos contenidos en sistemas de información que produzcan el efecto de de borrarlos, dañarlos, deteriorarlos, alterarlos, suprimirlos o hacerlos inaccesibles (art. 4); serán sancionadas, asimismo, otras formas de participación como la inducción, la complicidad y la tentativa (dejando a discreción del Estada contemplarla en la infracción referida en el art. 2).

En su empeño armonizador, la Decisión no sólo proclama que las sanciones penales habrán de ser efectivas, proporcionadas y disuasorias, sino que las sanciones aplicables a las conductas referidas en los artículos 3 y 4 —las más graves—, estarán comprendidas entre uno a tres años de prisión como mínimo en su grado máximo.[82] Reduce significativamente la autonomía de los Estados, ciñéndola a este confuso margen y a la infracción establecida en el artículo 2 (cuya amplitud sancionadora queda a discreción de los Estados.) La sanción será de dos a cinco años de prisión como mínimo en su grado máximo cuando se cometan en el marco de una organización delictiva tal como la define la Acción Común 98/733/JAI[83], con independencia del nivel de sanción mencionado en dicha Acción Común. Esta circunstancia agravante podrán contemplarla los Estados miembros (discrecionalmente) si la infracción hubiera ocasionado graves daños o afectado a intereses esenciales. Cuando el delincuente sea una persona jurídica, y con independencia de la sanción que corresponda a las personas físicas que la administren, podrán imponerse contra aquélla sanciones, penales o administrativas, de naturaleza económica o incluso la vigilancia de las actividades (art. 9).

Lo más interesante, sin duda, es que se afronta, aunque de manera muy somera, el problema de la jurisdicción aplicable al cibercrimen (de forma impropia la decisión habla de "competencia"). El artículo 10 sienta las bases de más de una controversia, pues la jurisdicción, sobre las infracciones mencionadas en la Decisión, se atribuye:

a) Al Estado en cuyo territorio se haya cometido, total o parcialmente la infracción, que comprende tanto el caso en que el infractor se encuentre físicamente en ese Estado aunque el ataque se produzca en sistemas informáticos situados en otro país, como el supuesto inverso, es decir, cuando el autor se halle físicamente en otro país pero la infracción se cometa en sistemas informáticos situados en el Estado de que se trate.

b) También tendrá jurisdicción cualquier Estado de la UE para conocer del asunto cuando la infracción la hubiese cometido uno de sus nacionales y, asimismo

c) El Estado en cuyo territorio tenga su domicilio social la persona jurídica en cuyo beneficio se comete la infracción.

A tenor de esta redacción, y puesto que los sistemas informáticos se hallan, a menudo, interconectados por redes transfronterizas se adivinan importantes puntos de fricción. Así, bastaría la comisión parcial del delito para que un Estado aplicara su jurisdicción, siendo frecuentes los multiataques informáticos que producirían la potencial

actuación de muchas jurisdicciones. Los Estados que persiguiesen a sus nacionales podrían colisionar con la jurisdicción de aquellos en cuyo territorio se ha cometido el delito o en cuyo territorio se domiciliase la persona jurídica administrada por el nacional perseguido por su propio país. Otras muchas combinaciones podrían darse, lo que convierte a esta regla más que en una regla de conflicto, en una regla conflictiva.

En previsión de los conflictos que se avecinarán, el mismo artículo, en su apartado cuarto, contempla el supuesto de la pluralidad de competencia, disponiendo que

> cuando una infracción sea competencia de más de un Estado miembro y cualquiera de estos Estados pueda legítimamente iniciar acciones judiciales por los mismos hechos, **los Estados miembros de que se trate colaborarán para decidir cuál de ellos iniciará acciones judiciales contra los autores de la infracción, con el objetivo de centralizar, *en la medida de lo posible,* dichas acciones en un solo Estado miembro.** Con este fin, los Estados miembros *podrán* recurrir a cualquier órgano o mecanismo creado en el marco de la Unión Europea para facilitar la cooperación entre sus autoridades judiciales y la coordinación de sus actuaciones.

Para dilucidar a qué Estado corresponderá finalmente el ejercicio de la jurisdicción, *se podrán* tener en cuenta los siguientes criterios por orden consecutivo:

1) El Estado miembro en cuyo territorio se hayan cometido las infracciones.[84]

2) El Estado miembro del que sea nacional el autor.

3) El Estado miembro en el que se haya encontrado al autor.

Analizando el este apartado, podría conceptuarse como una declaración de intenciones de escasa relevancia teórica, pues a la vez que proclama soluciones, estas quedan a la buena voluntad del Estados que mantengan algún punto de conexión con la infracción, puesta que la prelación de jurisdicciones no obliga a los Estados involucrados.

Si bien la regulación contenida en la Decisión no es compacta, si supone un paso adelante en la lucha contra el cibercrimen, puesto que identifica de forma taxativa los dos grandes obstáculos que dificultan esta lucha: la disparidad normativa y la jurisdicción aplicable. Su eficacia debe comprobarse empíricamente, luego que quede transpuesta al derecho interno en el plazo establecido al afecto (hasta el 16 de marzo de 2007) y comience a rodar en forma de normas internas.

II. Derecho procesal derivado.

Faltan disposiciones específicas que regulen la investigación (policial y judicial) y el tratamiento de procesal penal del cibercrimen. Por ello debe recurrirse a las normas sobre asistencia judicial penal en la Unión Europea y las que regulan las actuaciones conjuntas entre fuerzas de seguridad de varios Estados. Lo cierto es que las menciones específicas del cibercrimen son escasas y su inclusión en las actuaciones policiales y judiciales reguladas en tales normas suele encontrar algún amparo genérico y, por tanto, sujeto a diversas interpretaciones. Conviene pues referirnos a algunas de estas referencias, si bien de un modo muy breve.

El Convenio relativo a asistencia judicial en materia penal entre los Estados miembros de la Unión Europea[85] resulta de aplicación al cibercrimen. De conformidad con su preámbulo, el Convenio no se establece como una célula autónoma y única reguladora de la asistencia judicial y policial, sino que ha de complementarse con los instrumentos

internacionales y transnacionales existentes hasta la fecha o se promulguen en el futuro. El Convenio pretende, en síntesis, activar la ayuda mutua entre autoridades judiciales, policiales y aduaneras de los Estados miembros, completando y facilitando la aplicación del Convenio de 1959 del Consejo de Europa sobre ayuda mutua en materia penal y de su protocolo de 1978, del Convenio de aplicación del Acuerdo de Schengen de 1990 y del Tratado Benelux de 1962, de forma compatible con los principios fundamentales de sus perspectivos Derechos internos, respetando los derechos individuales y los principios contenidos en el Convenio europeo para la protección de los derechos humanos y de las libertades fundamentales, firmado en Roma el 4 de noviembre de 1950.[86]

El Convenio de 2000 establece un variado conjunto de medidas y de prácticas que permiten la agilización de los procedimiento, suprimiendo, o rebajando, los inconvenientes burocráticas que tradicionalmente afectaba a la cooperación internacional en materia judicial. Así, salvo casos específicos en la que intermedia una autoridad central, las solicitudes de asistencia mutua y las comunicaciones serán transmitidas y ejecutadas directamente por las autoridades judiciales territorialmente, pudiendo darse el intercambio espontáneo de información (sin solicitud previa) sobre hechos penalmente sancionables y sobre infracciones administrativas entre esas mismas autoridades.

Las formas de asistencia previstas en el Convenio son muy variadas y habrán de afectar en los procesos penales, tanto el la fase de juicio oral como en la instructora, y por extensión a las actuaciones desempeñadas por la policía judicial de los países cooperantes. Los delitos cibernéticos y, en especial, los que se cometen a través de la WWW, pese a sus características individidualizadoras, no dejan de ser delitos que caen dentro del ámbito de aplicación del Convenio, máxime cuando una de esas características que distingue al ciberdelito, como he señalado más arriba, es la transgresión de fronteras y, como consecuencia, la ubicuidad jurisdiccional.

El Convenio contempla, bajo ciertas condiciones, el traslado temporal de detenidos; la intervención de testigos o peritos a través de videoconferencia en procedimientos incoados en otros Estados miembros; la creación de equipos comunes de investigación entre dos o más estados miembros; las investigaciones encubiertas, mediante la intervención de agentes que utilicen una identidad secreta o ficticia; y la interceptación de telecomunicaciones.

Sin obviar la importancia de estos instrumentos procesales, revisten especial relevancia para nuestro objeto de estudio, la previsión de creación de equipos comunes de investigación y la interceptación de telecomunicaciones.

Creación de equipos comunes de investigación.-

El artículo 13, apartado 1, del Convenio contempla la creación de equipos comunes de investigación mediante decisión de las autoridades competentes de dos o más estados, con un fin determinado y por un periodo limitado que podrá ampliarse con el consentimiento de todas las partes, para llevar a cabo investigaciones penales en uno o más de los Estados miembros que hayan creado el equipo.

Podrán crearse equipos conjuntos de investigación, en particular, en los casos siguientes:

a) cuando la investigación de infracciones penales en un Estado miembro requiera investigaciones difíciles que impliquen la movilización de medios considerables y afecten también a otros Estados miembros;

b) cuando varios Estados miembros realicen investigaciones sobre infracciones penales que, debido a las circunstancias del caso, requieran una actuación coordinada y concertada de los Estados miembros afectados (art. 13.1. *in fine*.)

El mismo artículo, a lo largo de su redacción, ofrece las pautas y condiciones para la creación de los equipos comunes, su constitución, la dirección (que recaerá en una autoridad competente del país en el que actúe el equipo), el alcance de la intervención de los "destinados" extranjeros en el país donde actúe el equipo, que será máxima salvo que existan límites en la legislación del Estado donde actúa el equipo. Excepcionalmente se prevé la posibilidad de que tomen parte en los equipos funcionarios de organismos creados de conformidad con el Tratado de la Unión Europea, en la medida en que lo permitan la legislación de los Estados miembros interesados o las disposiciones de todo instrumento jurídico aplicable entre ellos (apartado 12, del artículo 13).[87] [88]

Sin duda ayudará a la persecución del cibercrimen la previsión del apartado 8 del artículo 13, que establece la posibilidad de que el equipo creado pueda solicitar ayuda a un Estado miembro no participante en el equipo por medio de las autoridades competentes del Estado donde actúe el equipo. El apartado 9, dentro de ciertos límites, contempla la posibilidad de intercambio de información entre los miembros del equipo de las que tengan conocimiento en sus países de origen.

La información obtenida legalmente (apartado 10) en el curso de la investigación de un equipo común, tanto por un miembro nacional del Estado donde actúe el equipo como por un miembro destinado al mismo mientras forme parte de un equipo conjunto de investigación y a la que no tengan acceso de otro modo las autoridades competentes de los Estados miembros afectados podrá utilizarse para los siguientes fines:

a) para los fines para los que se haya creado el equipo;

b) condicionada a la autorización previa del Estado miembro en que se haya obtenido la información, para descubrir, investigar y enjuiciar otras infracciones penales. Si bien esta autorización sólo podrá denegarse en los casos en que esta utilización ponga en peligro las investigaciones penales en el Estado miembro de que se trate o en que dicho Estado miembro pueda denegar la asistencia judicial;

c) para evitar una amenaza inmediata y grave para la seguridad pública, y sin perjuicio de lo dispuesto en la letra b) si ulteriormente se iniciara una investigación penal;

d) para otros fines, siempre y cuando hayan convenido en ello los Estados miembros que crearon el equipo.

Pese a su generalidad y a que parece referirse constantemente a la delincuencia terrestre (cuando diferencia el Convenio entre Estados donde actúa el equipo y otro Estados), la creación de equipos conjuntos para la investigación, persecución y represión del cibercrimen se antoja indispensable, pues habrá muchos supuestos en los que se haya producido una pluralidad de damnificados de distintas nacionalidades o, dada la facilidad que ofrece el medio virtual, que el delito se haya perpetrado mediante una organización o simple reunión plurinacional de delincuentes. El Convenio, que simplifica burocráticamente la cooperación transnacional, acompañado de la adecuada diligencia policial y judicial, podría constituir un válido instrumento para responder a la delincuencia infor-

mática, *donde el carácter transnacional de las conductas hace muy difícil no ya su descubrimiento, sino su castigo, siendo frecuentes los problemas de jurisdicción competente, así como el hecho de es verdaderamente difícil determinar la identidad de los delincuentes.*[89] La rapidez que se imprima a la cooperación internacional asegurará la efectividad del ordenamiento jurídico represor.

Resalta LOURIDO RICO (2004: 164) la importancia que ha tenido en el ámbito del establecimiento de equipos comunes, la Decisión Marco del Consejo, de 13 de junio de 2002, sobre equipos conjuntos de investigación[90], a iniciativa de Bélgica, Francia, España y Reino Unido, que aceleraba la implantación de esta técnica sin aguardar a la entrada en vigor del Convenio de 2000, que de conformidad al art. 27 del mismo habría de producirse transcurridos 90 días desde que el octavo país hubiera notificado al Secretario General del Consejo de la Unión Europea la ratificación del Convenio conforme a su normativa constitucional doméstica. La entrada en vigor del Convenio se ha producido recientemente, el 23 de agosto de 2005, mientras que el plazo máximo para la trasposición previsto en la Decisión Marco, expiraba el 1 de enero de 2003, por lo que ésta significó un significativo progreso en la lucha transnacional contra el crimen.

En mi opinión, los equipos conjuntos de investigación ofrecen una ventaja añadida. La participación de autoridades judiciales de varios Estados en la fase instructora del procedimiento, provee de una valiosa información a fin delimitar, sobre los hechos delictivos investigados, la jurisdicción, e incluso la competencia objetiva, funcional y territorial, dentro de cada Estado. Podría darse el caso de que inicialmente los hechos pudieran indicar una concreta jurisdicción competente pero, en el curso de las investigaciones, resultar otra. Los datos suministrados por los equipos comunes servirían de base jurídica a los jueces para reclamar su competencia o para inhibirse de la misma.

Interceptación de las comunicaciones.-

Los artículos 17 al 22 (la totalidad del Título III) regulan la intervención de las comunicaciones en el marco del Convenio. Aunque una primera lectura puede inducir a pensar que el Convenio circunscribe la intervención a las comunicaciones a distancia tradicionales, al emplear la fórmula abierta de "intervención en las telecomunicaciones" sin definir el concepto de "telecomunicación" colegida con el art. 1.1. del Convenio de 1959 que obliga a las partes contratantes a "prestarse la asistencia judicial más amplia posible", permiten contemplar la intervención en los términos amplios, que incluiría el teléfono móvil, el fax y el correo electrónico.[91]

Sin embargo, los artículos mencionados, no establecen mecanismos para la intervención en las telecomunicaciones operadas a través de las TICs, resultando muy dudoso que el concepto de "proveedor de servicio" referido en el artículo 19 comprenda al *proveedor a acceso a Internet* o al *proveedor de contenidos.* El término *pasarela* que se emplea en dicho artículo no parece incluir a los operadores de la WWW, aunque da lugar a una interpretación amplia.

> En particular, el artículo 19 establece que "los Estados miembros garantizarán que los sistemas de servicios de telecomunicaciones que operen a través de una pasarela en su territorio y a los que no pueda accederse directamente desde otro Estado miembro a efectos de intervención legal de las comunicaciones de una persona que se halle en el territorio de este último, puedan hacerse

directamente accesibles para la intervención legal por parte de dicho Estado miembro, por mediación de un proveedor de servicios designado que se encuentre en el territorio de éste.

Tal vez por esta causa, el artículo 22 deja la puerta abierta a la innovación tecnológica, al disponer que ninguna de las disposiciones del título constituirá un obstáculo para posibles acuerdos bilaterales o multilaterales entre los Estados miembros, destinados a facilitar la explotación de las posibilidades técnicas actuales y futuras en lo que respecta a la intervención legal de telecomunicaciones.

E. Conclusiones.

La evolución normativa, tanto a nivel nacional como transnacional, en materia de cibercrimen, se ha generado con base a unos tratados que, tal vez, no hubieran contemplado el cibercrimen como una amenaza inminente, lo que, desde el punto de vista sistemático suele producir la impresión de parcheo y, hasta de improvisación. Lo cierto, es que la regulación de la UE sobre la cibercriminalidad, tanto del primer como del tercer pilar, ha aparecido y ha empezado a enfrentarse con temas tan espinosos como la responsabilidad de los proveedores de acceso y de contenido, el establecimiento de márgenes penales para delitos estrictamente informáticos y, por primera vez, se ha abordado, con escasa resolución, el problema de la jurisdicción en el ciberespacio, que más que establecer reglas de conflicto, parece que sólo se ha pretendido proclamar expresamente la existencia del conflicto para que sean legisladores futuros quienes lo solucionen.

Ese futuro, todavía incierto, ya está escrito. El Tratado por el que se establece una Constitución para Europa, en su art. III-271, contempla la posibilidad de que, por medio de leyes marco europeas, se establezcan normas mínimas relativas a la definición de las infracciones penales y de las sanciones en ámbitos delictivos que sean de especial gravedad y tengan una dimensión transfronteriza derivada del carácter o de las repercusiones de dichas infracciones o de una necesidad particular de combatirlas según criterios comunes. Entre los ámbitos delictivos enumerados, destaca la delincuencia informática.

Una vez alcanzada la cohesión normativa (armonizada) de puertas adentro, la UE podrá abordar la lucha contra la ciberdelincuencia en paraísos cibernéticos, asunto que merecería un análisis independiente.

BIBLIOGRAFÍA

ALVAREZ VIZCAYA, Maite. "Consideraciones político criminales sobre la delincuencia informática: el papel del derecho penal en la red". En: LOPEZ ORTEGA, Juan José. Internet y Derecho Penal. 1ª edición. Madrid: Consejo General del Poder Judicial, 2001. p. 257-279.

ANARTE BORRALLO, Enrique. "Sobre los límites de la protección penal de datos personales". *Derecho y Conocimiento. Anuario jurídico sobre la Sociedad de la Información y del Conocimiento*, *Facultad de Derecho Universidad de Huelva,* 2004, vol.2, ISSN 1578-8202.

BENSOUSSAN, Alain. "Loi appliquable et juridictions competentes pour les sites Internet. Ordonnance de référé du TGI de Paris du 22 mai 2000 sur la vente d'objets nazis sur le site Yahoo" [en línea]. Marzo de 2000. Disponible en http://www.journaldunet.com/juridique/juridique15yahoo.shtml. [Consulta: 9 de agosto de 2006].

CALVO CARAVACA, Alfonso Luis y CARRASCOSA GONZÁLEZ, Javier. *Conflictos de Leyes y Conflictos de Jurisdicción en Internet.* Primera edición. Madrid: Colex, 2001. 172 págs. ISBN: 84-7879-636-3.

CASTILLO JIMÉNEZ, Cinta. "La sociedad de la información y los derechos fundamentales". *Derecho y Conocimiento. Anuario jurídico sobre la Sociedad de la Información y del Conocimiento*, *Facultad de Derecho Universidad de Huelva,* 2004 vol.2, ISSN 1578-8202.

CLIMENT BARBERÁ, Juan. "La Justicia Penal en Internet. Territorialidad y competencias penales". En: LOPEZ ORTEGA, Juan José. Internet y Derecho Penal. 1ª edición. Madrid: Consejo General del Poder Judicial, 2001. p. 647-663.

DIERKS, Michael P. "Computer network abuse". *Harvard Journal of Law & Technology*, 1993, (Volume 6, Spring Issue)

ECHEVERRÍA, Javier. "Nuevas tecnologías, sociedad y democracia". *Instituto de Filosofía, CSIC.* (Vitoria-Gazteiz, HEGOA, 18 de noviembre de 2004.)

EVANS, James. "'Love Bug' Suspect Charged". *PC WORLD* [en línea]. 25 de junio de 2000. Disponible en http://www.pcworld.com/article/id,17497-page,1/article.html. [Consulta: 9 de agosto de 2006].

FISCHER-HÜBNER, Simone. "Privacy in the Global Information Society". *Lecture Notes in Computer Science, Volume 1958,* (Junio, 2001).

GOODMAN, Marc y BRENNER Susan. "The emerging consensus on criminal conduct in cyberspace". *International Journal of Law and Information Technology*, 2002, vol. 10, núm. 2. p. 139-223.

HESS ARAYA, Christian. "El nombre de dominio, ¿una nueva forma de propiedad?". Publicación electrónica disponible en http://www.hess-cr.com/secciones/dere-info/dnspropiedad.shtml, visitado el día 11 de noviembre del 2005. San José de Costa Rica, 2002.

HESS ARAYA, Christian. *"TLC, ALCA e Internet "*. Publicación electrónica disponible en http://www.hess-cr.com/secciones/dere-info/nacion-040310tlc-udrp.shtml, visitado el día 11 de noviembre del 2005. San José de Costa Rica, 2004.

LEZERTÚA, Manuel. "El Proyecto de Convenio sobre el Cybercrimen del Consejo de Europa". En: LOPEZ ORTEGA, Juan José. Internet y Derecho Penal. 1ª edición. Madrid: Consejo General del Poder Judicial, 2001. p. 17-61.

LOPEZ MORENO, Juana y FERNÁNDEZ GARCÍA, Emilio. "La Word Wide Web como vehiculo de delincuencia: supuestos frecuentes". En: LOPEZ ORTEGA, Juan José. Internet y Derecho Penal. 1ª edición. Madrid: Consejo General del Poder Judicial, 2001. p. 401-456.

LOURIDO RICO, Ana María. *La Asistencia Judicial Penal en la Unión Europea.* Primera edición. Valencia: Tirant Lo Blanch, 2004. 237 págs. ISBN: 84-8442-931-8.

MANGAS, Araceli, y LIÑAN, Diego. *Instituciones y Derecho de la Unión Europea*. Quinta edición. Madrid: Tecnos (Grupo Anaya S.A.), 2005. 771 págs. ISBN: 84-309-4299-8.

MANOLOPOULOS, Andreas. "Raising Cyber-Borders: The interaction between Law and Technology". *International Journal of Law and Information Technology*, 2003, Vol. 11 No. 1. p. 40-58.

MOLES PLAZA, Ramón J. *Derecho y control en Internet.* Primera edición. Barcelona: Ariel Derecho, 2004. 164 págs. ISBN: 84-344-3237-4.

MORALES GARCÍA, Óscar. "Apuntes de política criminal en el contexto tecnológico. Una aproximación a la Convención del Consejo de Europa sobre Cyber-crime". En: MORALES GARCÍA, Oscar. Delincuencia Informática. Problemas de responsabilidad. 1ª edición. Madrid: Consejo General del Poder Judicial, 2002. p. 13-33.

MORALES GARCÍA, Óscar. "Criterios de atribución de responsabilidad penal a los prestadores de servicios e intermediarios de la sociedad de la información". En: MORALES GARCÍA, Oscar. Delincuencia Informática. Problemas de responsabilidad. 1ª edición. Madrid: Consejo General del Poder Judicial, 2002. p. 181-239.

MORALES PRATS, Fermín. "Internet: Riesgos para la intimidad". En: LOPEZ ORTEGA, Juan José. Internet y Derecho Penal. 1ª edición. Madrid: Consejo General del Poder Judicial, 2001. p. 65-81.

SANCHEZ ALMEIDA, Carlos. (2004, Marzo). Ponencia presentada en el XIII Congreso de Responsabilidad Civil, organizado por la Comisión de Abogados de Entidades Aseguradoras y Responsabilidad Civil del Ilustre Colegio de Abogados de Barcelona. *República Internet.* Consultada el 29 de septiembre de 2005, http://www.tercerarepublica.com/articulo.php?id=25.

SANTOS GARCÍA, Daniel. *Nociones Generales de la Ley Orgánica de Protección de Datos,* 2005. Madrid: Tecnos.

SIEBER, Ulrich. *Legal Aspects of Computer-Related Crime in the Information Society – COMCRIME – Study.*1 de junio de 1998. Versión 1.0. 240 págs.

SILVA SÁNCHEZ, Jesús. "La Responsabilidad Penal de las Personas Jurídicas en el Convenio del Consejo de Europa sobre Cibercriminalidad". En: MORALES GARCÍA, Oscar. Delincuencia Informática. Problemas de responsabilidad. 1ª edición. Madrid: Consejo General del Poder Judicial, 2002. p. 115-141.

SVANTESSON, Dan Jerker. "The characteristics making Internet communication challenge traditional models of regulation - What every international jurist should know about the Internet". *International Journal of Law and Information Technology,* 2005, vol. 13, núm. 1. p. 39-69.

WU, Timothy. "Cyberspace Sovereignty? - The Internet and the International System". *Harvard Journal of Law & Technology*. 1997, vol 10, núm. 3, summer issue.

---

[1] Incluso las Ciencias Sociales más adustas han visto alteradas sus primitivas concepciones. La Historia, vgr., ha comenzado a remover sus cimientos y a interesarse no sólo por el pasado remoto sino por el más reciente, naciendo una nueva disciplina: La Historia del Tiempo Presente. Cuesta, Josefina (1993) *Historia del Presente*. Madrid: Eudema.

[2] 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. DO L 178 de 17.7.2000, p. 1/16

[3] 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 electrónicas. DO L 201 de 31.7.2002, p. 37/47

[4] "Just as the territory a ship traverses is not subject to any one state's exclusive jurisdiction, so too the user in cyberspace traverses a sovereignless region that is not subject to any state's exclusive jurisdiction." Traducción del autor de este trabajo.

[5] WU, TIMOTHY S. (1997). Cyberspace Sovereignty? -- The Internet and the International System. *Harvard Journal of Law & Technology*, (Volume 10, Number 3 Summer Issue), 648.

[6] "Internet is virtually infinitely expandable in size". Traducción propia del autor de este trabajo.

[7] Internet es *una red de redes* a escala mundial de millones de computadoras interconectadas con un conjunto de protocolos, el más destacado, el TCP/IP. También se usa este nombre como sustantivo común y por tanto en minúsculas para designar a cualquier red de redes que use las mismas tecnologías que Internet, independientemente de su extensión o de que sea pública o privada.
Cuando se dice red de redes se hace referencia a que es una red formada por la interconexión de otras redes menores.
Al contrario de lo que se piensa comúnmente, Internet no es sinónimo de World Wide Web. Ésta es parte de aquella, siendo la World Wide Web uno de los muchos servicios ofertados en la red Internet. La Web es un sistema de información mucho más reciente (1995) que emplea Internet como medio de transmisión.
Algunos de los servicios disponibles en Internet aparte de la Web son el acceso remoto a otras máquinas (SSH y telnet), transferencia de archivos (FTP), correo electrónico (SMTP), boletines electrónicos (news o grupos de noticias), conversaciones en línea (IRC y chats), mensajería instantánea (MSN Messenger, ICQ, YIM, AOL, Jabber), transmisión de archivos (P2P, P2M, Descarga Directa), etcétera. Para mayor información puede consultarse: http://es.wikipedia.org/wiki/Internet. [Consulta: 1 de septiembre de 2006]

[8] Correo electrónico, o en inglés e-mail, es un servicio de red para permitir a los usuarios enviar y recibir mensajes mediante sistemas de comunicación electrónicos (normalmente por Internet). Esto lo hace muy útil comparado con el

correo ordinario, pues es más barato y rápido. Junto con los mensajes también pueden ser enviados ficheros como paquetes adjuntos. Vid. http://es.wikipedia.org/wiki/Correo_electr%C3%B3nico. [Consulta: 1 de septiembre de 2006]

[9] La World Wide Web (del inglés, Telaraña Mundial), la Web o WWW, es un sistema de hipertexto que funciona sobre Internet. Para ver la información se utiliza una aplicación llamada navegador web para extraer elementos de información (llamados "documentos" o "páginas web") de los servidores web (o "sitios") y mostrarlos en la pantalla del usuario. El usuario puede entonces seguir hiperenlaces que hay en la página a otros documentos o incluso enviar información al servidor para interactuar con él. A la acción de seguir hiperenlaces se le suele llamar "navegar" por la Web o "explorar" la Web. No se debe confundir la Web con Internet, que es la red física mundial sobre la que circula la información.
Del mismo modo que se puede distinguir entre "una intranet" (una inter-red) y "la Internet", uno puede referirse a "un(a) web" como una página, sitio o conjunto de sitios que proveen información por los medios descritos, y "la Web", que es la enorme e interconectada web disponible prácticamente en todos los sitios de Internet. Para mayor información puede consultarse:
http://es.wikipedia.org/wiki/World_Wide_Web. [Consulta: 1 de septiembre de 2006]

[10] SVANTESSON, DAN JERKER B. (2005) The characteristics making Internet communication challenge traditional models of regulation — What every international jurist should know about the Internet. *International Journal of Law and Information Technology* (Vol. 13 No. 1, pag 39-69), pag 42-43.

[11] MORALES GARCÍA, Óscar. "Criterios de atribución de responsabilidad penal a los prestadores de servicios e intermediarios de la sociedad de la información". En: MORALES GARCÍA, Oscar. Delincuencia Informática. Problemas de responsabilidad. 1ª edición. Madrid: Consejo General del Poder Judicial, 2002. p. 204-205. El autor añade que la especialidad del Webcasting (también denominado *multidifusión*, *multicasting* o *Broadcast*) radica en el hecho de la información no es buscada por el usuario, sino que ésta es puesta a su disposición. Programas tan populares como el Realaudio o Realplayer utilizan el sistema para la reproducción de la información que viaja en *multicasting*.

[12] FTP es uno de los diversos protocolos de la red Internet, concretamente significa File Transfer Protocol (Protocolo de Transferencia de Ficheros) y es el ideal para transferir grandes bloques de datos por la red. Su comportamiento está definido por la recomendación RFC 959. Se precisa de un Servidor FTP y un cliente FTP, puede darse el caso de que los servidores sean de libre acceso para todo el mundo y entonces estamos hablando de login anónimo o FTP anónimo. **La mayoría de las páginas web a nivel mundial son subidas a los respectivos servidores mediante este protocolo.** Para mayor detalle puede consultarse http://es.wikipedia.org/wiki/Ftp. [Consulta: 1 de septiembre de 2006]

[13] El concepto de Proxy o servidor de Proxy es un concepto amplio que hace referencia a un intermediario. Una situación frecuente, sobre todo en pequeñas organizaciones, es disponer de una única dirección de IP (el identificativo de cada terminal informático cuando accede a la red) y varios ordenadores que no puede acceder simultáneamente a Internet (al disponer de un único IP.) El servidor de Proxy actúa de intermediario para los ordenadores de la organización, almacena páginas visitadas por otros ordenadores del grupo —en la caché—, por lo que la velocidad de acceso a esas páginas aumenta notablemente, pues ya se encuentran a disposición de los ordenadores interconectados. En la ciberdelincuencia el servidor Proxy podría albergar contenidos delictivos, pues puede utilizarse, según los casos, por el sujeto activo y pasivo de los cibercrímenes. Vid. http://www.webopedia.com/TERM/p/proxy_server.html. [Consulta: 1 de septiembre de 2006]

[14] Se denomina mirror o espejo, a la copia idéntica que tiene un servidor de Internet de la información de otro. Se utiliza para evitar aglomeraciones cuando la página es muy frecuentada y para que la carga de la página o archivos sea más rápida. En lo que respecta al cibercrimen el mirror puede albergar la misma información delictiva que el servidor original. Vid.
http://www.webopedia.com/TERM/m/mirror_site.html. [Consulta: 1 de septiembre de 2006]

[15] SVANTESSON, Dan Jerker., op. cit., pág 45. El autor señala un caso de control de acceso a Internet. En ciertos países con regímenes autoritarios, el acceso a la red se ve intermediado por un proveedor estatal de comunicaciones, al objeto de censurar, previamente, los contenidos que pueden visitar sus ciudadanos. La República Popular China, considerando el peligro que representaba Internet se anticipó dictando las *Provisonal Regulations of the People's Republic of China for the Administration of International Connections to Computer Infomration Networks (1997)*

[16] URL significa Uniform Resource Locator, es decir, localizador uniforme de recurso. Es una secuencia de caracteres, de acuerdo a un formato estándar, que se usa para nombrar recursos, como documentos e imágenes en Internet, por su localización.
Las URL fueron una innovación fundamental en la historia de Internet. Fueron usadas por primera vez por Tim Berners-Lee en 1991, para permitir a los autores de documentos establecer hiperenlaces en la World Wide Web (WWW o Web). Desde 1994, en los estándares de Internet, el concepto de URL ha sido incorporado dentro del más general de URI (Uniform Resource Identifier - Identificador Uniforme de

Recurso), pero el término URL aún se utiliza ampliamente. www.webopedia.com/TERM/U/URL.html y http://es.wikipedia.org/wiki/URL. [Consulta: 1 de septiembre de 2006]

[17] Consultada la vigésima segunda edición del Diccionario de la Real Academia de la Lengua (2001) (http://www.rae.es) se define la página web como "Documento situado en una red informática, al que se accede mediante enlaces de hipertexto." Nuestro diccionario todavía no ha incorporado palabras como internauta, ciberdelito, cibercrimen, ciberdelincuente, website y otras que, nosotros, por necesidades explicativas habremos de utilizar frecuentemente. [Consulta: 1 de septiembre de 2006]

[18] El número de personas que han utilizado Internet en España en los últimos tres meses del año, ha pasado de 13.534.664 en el año 2004 a 15.131.420 en el año 2005. Fuentes: Asociación Española de Usuarios de Internet. Disponible en: http://www.fundacionauna.org/areas/25_publicaciones/eEspana_2006.pdf. [Consulta: 4 de septiembre de 2006]

[19] Precisamente países como Filipinas o India suelen ser el origen de perniciosos virus, sorprendiendo a las propias autoridades que no encontrar fundamento legal alguno para entablar acciones criminales contra sus autores. Puede destacarse el virus "I Love You" programado por el estudiante filipino Onel de Guzmán que fue desatado el 4 de mayo de 2000 causando daños por unos 8.7 billones de dólares. Vid. EVANS, James. "'Love Bug' Suspect Charged". *PC WORLD* [en línea]. 25 de junio de 2000. Disponible en http://www.pcworld.com/article/id,17497-page,1/article.html. [Consulta: 9 de agosto de 2006].

[20] Una dirección IP es un número que identifica de manera lógica y jerárquicamente a una interfaz de un dispositivo (habitualmente una computadora) dentro de una red que utilice el protocolo IP (Internet Protocol), que corresponde al nivel de red o nivel 3 del modelo de referencia OSI. Dicho número no se ha de confundir con la dirección MAC que es un número físico que es asignado a la tarjeta o dispositivo de red (viene impuesta por el fabricante), mientras que la dirección IP se puede cambiar. Vid. http://www.webopedia.com/TERM/I/IP.html y http://es.wikipedia.org/wiki/Ip. [Consulta: 25 de julio de 2006]

[21] El DNS se traduce en una base de datos jerárquica, en cuyo vértice figura el dominio raíz ".", a partir del cual brotan una serie de dominios de nivel superior (TLDs). Éstos se dividen, a su vez, en genéricos y nacionales. Los primeros (gTLD) incluyen tanto las extensiones tradi-cionales como .com, .net, .org, así como las más recientemente aprobadas por la ICANN, como .name, .biz o .pro. Por su parte, los segundos (ccTLD), hacen alusión a los dominios asociados a países específicos, como .fr (Francia), .br (Brasil) o .cr (Costa Rica), representados por dos caracteres correspondientes al código ISO-3166 de cada nación. Clara explicación ofrecida por HESS ARAYA, Christian. "El nombre de dominio, ¿una nueva forma de propiedad?". Publicación electrónica disponible en http://www.hess-cr.com/secciones/dere-info/dnspropiedad.shtml, visitado el día 11 de noviembre del 2005. San José de Costa Rica, 2002.

[22] SVANTESSON, Dan Jerker., op. cit., pág 55.

[23] Su implantación definitiva originará la eterna controversia seguridad versus intimidad, que animará encendidos debates que no son objeto de este trabajo.

[24] En especial, la Ley 34/2002, de 11 de julio, sobre servicios de la sociedad de la información y de comercio electrónico, que traspone al ordenamiento jurídico interno la 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 (Directiva sobre el comercio electrónico.)

[25] Sánchez Almeida, Carlos. (2004, Marzo). Ponencia presentada en el XIII Congreso de Responsabilidad Civil, organizado por la Comisión de Abogados de Entidades Aseguradoras y Responsabilidad Civil del Ilustre Colegio de Abogados de Barcelona. *República Internet.* Consultada el 29 de septiembre de 2005, http://www.tercerarepublica.com/articulo.php?id=25

[26] El marco normativo proclama el principio de la no sujeción a autorización previa para la prestación de servicios en la Sociedad de la Información, salvo ciertos supuestos (véase el art. 6 de la Ley 34/2002, de 11 de julio, sobre servicios de la sociedad de la información y de comercio electrónico.)

[27] GOODMAN, Marc y BRENNER Susan. "The emerging consensus on criminal conduct in cyberspace". *International Journal of Law and Information Technology*, 2002, vol. 10, núm. 2. p. 155.

[28] GOODMAN, Marc y BRENNER Susan., op. cit., p. 145.

[29] Un proveedor de servicios de Internet (o ISP por el acrónimo inglés de Internet Service Provider) es una empresa dedicada a conectar a Internet la línea telefónica de los usuarios o las distintas redes que tengan, y dar el mantenimiento necesario para que el acceso funcione correctamente. También ofrecen servicios relacionados, como alojamiento web, registro de dominios, y otros más específicos. Vid. http://es.wikipedia.org/wiki/ISP. y http://www.webopedia.com/TERM/I/ISP.html. [Consulta: 4 de septiembre de 2006]

Todo usuario de Internet tiene algún proveedor de acceso a Internet contratado. Muchas veces son las mismas compañías encargadas de dar el servicio telefónico.

[30] El alojamiento web (en inglés web hosting) es el servicio que provee a los usuarios de Internet un sistema para poder almacenar información, imágenes, vídeo, o cualquier contenido accesible vía Web. Los Web Host son

compañías que proporcionan espacio de un servidor a sus clientes. Vid. http://www.webopedia.com/TERM/H/Hosting_Services_Provider.html y http://es.wikipedia.org/wiki/Web_hosting. [Consulta: 15 de julio de 2006]

[31] En otros ejemplos (vgr. en los delitos relacionados con la pornografía infantil o difamación) el sujeto pasivo no interviene para nada en el proceso informático.

[32] El simple acto de exponer tales objetos en Francia constituye una violación del artículo R 645-1del Código Penal Francés. Asimismo, la exposición con el propósito de venta constituye contravención del artículo R 645-2 de ese mismo código.

[33] MANOLOPOULOS, Andreas. "Raising Cyber-Borders: The interaction between Law and Technology". *International Journal of Law and Information Technology*, 2003, Vol. 11 No. 1. p. 42.

[34] Finalmente, la solución adoptada por el Tribunal de Grand Instance París, fue jurídicamente ambigua e insegura. El tribunal decidió imponer el sistema de filtrado IP (inaplicable al 30% de los usuarios franceses) y fórmulas residuales, como declaraciones juradas de los usuarios sobre su nacionalidad (fácilmente manipulables), o impedir el acceso cuando el usuario introduce en motor de búsqueda palabras como "nazi".

[35] Yahoo A, Inc v la Ligue Contre Le Racisme et L'Antisemitisme 169 F, Supp, 2d 1181, N.D. Cal., 2001, Nov. 7, 2001.

[36] BENSOUSSAN, Alain. "Loi appliquable et juridictions competentes pour les sites Internet. Ordonnance de référé du TGI de Paris du 22 mai 2000 sur la vente d'objets nazis sur le site Yahoo" [en línea]. Marzo de 2000. Disponible en http://www.journaldunet.com/juridique/juridique15yahoo.shtml. [Consulta: 9 de agosto de 2006].

[37] MANOLOPOULOS, Andreas., op. cit., p. 48. El tribunal francés entendió que Yahoo se dirigía a Francia, a través de sus banners escritos en francés.

[38] A partir del caso Zippo Mfg. Co v Zippo Dot Com, Inc, se clasifican tres niveles de interactividad de webs.

1. Sitios activos donde usuarios hacen contratos, y el sitio realiza repetidas transacciones. En este caso, el tribunal competente fue el de Zippo Dot Com, Inc.
2. Sitios activos, donde se ofrece información sin transacciones.
3. Sitios activos/pasivos según los casos: intercambio de información con el computador host. Será activo si existe un elevado nivel de interactividad o es clara su naturaleza comercial. Vid. MANOLOPOULOS, Andreas., op. cit., p. 52. Para este autor, este criterio es inseguro porque los criterios de interactividad pueden variar, citando como argumento la resolución 952 F. Supp. 1119 (W.D. Pa. 1997) Vid. MANOLOPOULOS, Andreas., op. cit., p. 53.

[39] El Tribunal Supremo de EE.UU. en Calder v Jones se inclina por ejercer la jurisdicción si el demandado tuvo intención dañosa dirigida al estado del foro. Resolución 456 US 783 (1984). Vid. MANOLOPOULOS, Andreas., op. cit., p. 55

[40] Una aplicación consecuente de esta doctrina del efecto potencial del delito conduciría al resultado de que los Proveedores de Servicios Europeos (ISP) estarían sujetos a la Ley Islámica si sus contenidos fueran accesibles, por ejemplo, desde Irán. Vid. SIEBER, Ulrich. *Legal Aspects of Computer-Related Crime in the Information Society – COMCRIME – Study.*1 de junio de 1998. Versión 1.0. p. 131.

[41] Puede observarse esta previsión, vg., en la Seccion 6 No. 6 del Código Penal Alemán, así como en la Sección 64 (I) No. 4a del Código Penal Austriaco. En el Ordenamiento español encontramos una regulación semejante en el artículo 23.4. de la Ley Orgánica del Poder Judicial, estableciendo que Igualmente será competente la jurisdicción española para conocer de los hechos cometidos por españoles o extranjeros fuera del territorio nacional susceptibles de tipificarse, según la ley penal española, como alguno de los siguientes delitos:

a) Genocidio.
b) Terrorismo.
c) Piratería y apoderamiento ilícito de aeronaves.
d) Falsificación de moneda extranjera.
e) Los delitos relativos a la prostitución y los de corrupción de menores o incapaces.
f) Tráfico ilegal de drogas psicotrópicas, tóxicas y estupefacientes.
g) Los relativos a la mutilación genital femenina, siempre que los responsables se encuentren en España.
h) Y cualquier otro que, según los tratados o convenios internacionales, deba ser perseguido en España.

Tanto el terrorismo (ciberterrorismo) y los delitos relativos a la prostitución y los de corrupción de menores o incapaces (pornografía infantil) son susceptibles de persecución por la jurisdicción española, agravando los conflictos jurisdiccionales propios de la cibercriminalidad. La letra h) de este artículo habilita a la jurisdicción española, por medio de un tratado o convenio internacional, a perseguir un *numerus apertus* de delitos. Entre ellos podrían estar los ciberdelitos.

[42] Las normas existentes al respecto (Convenio de Bruselas sobre competencia judicial y ejecución de resoluciones judiciales en materia civil y mercantil del 27 de septiembre de 1968; Convenio de Lugano de1988; y el Reglamento 44/2001 del Consejo, del 22 de diciembre del 2000, referente a la competencia judicial, el reconocimiento y la eje-cución de resoluciones judiciales en materia civil y mercantil) sólo circunscriben su aplicación al ámbito de la U.E. y al de la A.E.L.C. (Asociación Europea de Libre Cambio) y pueden ser insuficientes para responder a las exigencias del hombre cotidiano (en el E3 cualquier persona, desde su casa, se convierte en exportador, importador, sujeto activo en las relaciones jurídicas internacionales y, sin embargo, no podría litigar ni ser parte en los procesos con la misma facilidad, pues estos serán costosos y, tal vez, se desarrollen a miles de kilómetros de distancia.) Internet genera una gran inseguridad procesal que debe resolverse en futuro.

[43] SIEBER, Ulrich. *Legal Aspects of Computer-Related Crime in the Information Society – COMCRIME – Study.*1 de junio de 1998. Versión 1.0. 240 págs.

[44] Informe sieber.

[45] Select Comité of Experts on Computer-Related Crime of the Council of Europe.

[46] Ver Consejo de Europa, Recomendación Nº. 4 (89) 9 del Comité de Ministros a los Estados Miembros sobre crímenes relacionados con la informática. Disponible en http://cm.coe.int/ta/rec/1989/89r9.htm, página visitada el 15-6-2006.

[47] Disponible en http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=185&CM=8&DF=6/16/2006&CL=ENG, página visitada el 16-6-2006

[48] A fecha de de 16 de junio de 2006, según se comprueba en la página mantenida al efecto por el Consejo de Europa (http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=8&DF=6/16/2006&CL=ENG), han firmado el Convenio todos los países del Consejo de Europa menos Andorra, Azerbaijan, Georgia, Liechtenstein, Mónaco, Rusia, San Marino, Turquía. Igualmente han firmado el Convenio Canadá, Japón, Sudáfrica y Estados Unidos. A fecha de hoy, sin embargo, una pequeña parte de los países signatarios han ratificado el Convenio, teniendo, por tanto, una eficacia muy limitada. Concretamente, sólo Albania, Bosnia y Herzegovina, Bulgaria, Croacia, Chipre, Dinamarca, Estonia, Francia, Hungría, Lituania, Rumanía, Eslovenia, Ex República Yugoslava de Macedonia y Ucrania.

[49] El texto utiliza la expresión, "las partes adoptarán…", apartándose de la mera declaración de intenciones propia de documentos precedentes.

[50] Vid. GOODMAN, Marc y BRENNER Susan. "The emerging consensus on criminal conduct in cyberspace". *International Journal of Law and Information Technology*, 2002, vol. 10, núm. 2. p. 189.

[51] Ibid.

[52] El artículo 94 del TCE establece: «El Consejo adoptará por unanimidad, a propuesta de la Comisión y previa consulta al Parlamento Europeo y al Comité Económico y Social, directivas para la aproximación de las disposiciones legales, reglamentarias y administrativas de los Estados miembros que incidan directamente en el establecimiento o funcionamiento del mercado común».

[53] El artículo 95.1. del TEC establece: «No obstante lo dispuesto en el artículo 94 y salvo que el presente Tratado disponga otra cosa, se aplicarán las disposiciones siguientes para la consecución de los objetivos enunciados en el artículo 14. El Consejo, con arreglo al procedimiento previsto en el artículo 251 y previa consulta al Comité Económico y Social, adoptará las medidas relativas a la aproximación de las disposiciones legales, reglamentarias y administrativas de los Estados miembros que tengan por objeto el establecimiento y el funcionamiento del mercado interior».

[54] Puede mostrarse como ejemplo, dentro del marco de la protección del mercado interior, la Directiva 2003/6/CE del Parlamento Europeo y del Consejo, de 28 de enero de 2003, sobre las operaciones con información privilegiada y la manipulación del mercado (abuso del mercado), que en su artículo 5 establece «Los Estados miembros prohibirán a cualquier persona efectuar prácticas de manipulación del mercado». Artículo 14.1. establece que «Sin perjuicio del derecho de los Estados miembros a imponer sanciones penales los Estados miembros garantizarán, de conformidad con su Derecho nacional, que se tomen las medidas administrativas apropiadas, o que se impongan sanciones administrativas contra las personas responsables cuando no se hayan cumplido las disposiciones adoptadas con arreglo a la presente Directiva. Los Estados miembros se asegurarán de que estas medidas tienen un carácter efectivo, proporcionado y disuasorio».

[55] El artículo 8 de la Directiva 2001/29/CE del Parlamento Europeo y del Consejo, de 22 de mayo de 2001, relativa a la armonización de determinados aspectos de los derechos de autor y derechos afines a los derechos de autor en la sociedad de la información, dispone, en tres párrafos, lo siguiente:
1. Los Estados miembros establecerán las sanciones y vías de recurso adecuadas en relación con la violación de los derechos y las obligaciones previstos en la presente Directiva y adoptarán cuantas

disposiciones resulten necesarias para garantizar que se apliquen tales sanciones y vías de recurso. Las sanciones deberán ser efectivas, proporcionadas y disuasorias.
2. Cada uno de los Estados miembros adoptará las medidas necesarias para garantizar que los titulares de los derechos cuyos intereses se vean perjudicados por una actividad ilícita llevada a cabo en su territorio puedan interponer una acción de resarcimiento de daños y perjuicios y/o solicitar medidas cautelares y, en su caso, que se incaute el material ilícito y los dispositivos, productos o componentes a que se refiere el apartado 2 del artículo 6.
3. Los Estados miembros velarán por que los titulares de los derechos estén en condiciones de solicitar medidas cautelares contra los intermediarios a cuyos servicios recurra un tercero para infringir un derecho de autor o un derecho afín a los derechos de autor.

[56] La 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 (Directiva sobre el comercio electrónico) regula en su Sección 4 la «Responsabilidad de los prestadores de servicios intermediarios». El Artículo 12 establece garantías para los servicios que consistan en transmitir en una red de comunicaciones, datos facilitados por el destinatario del servicio o en facilitar acceso a una red de comunicaciones. No se puede considerarse al prestador de servicios de este tipo responsable de los datos transmitidos. El artículo 13 establece semejante exención para el prestador de servicios consistentes en el almacenamiento automático, provisional y temporal de esta información, realizado con la única finalidad de hacer más eficaz la transmisión ulterior de la información a otros destinatarios del servicio. El artículo 14 también libera de responsabilidad al prestador de servicio consistente en almacenar datos facilitados por el destinatario del servicio. Por su parte el artículo 15 declara la «inexistencia de obligación general de supervisión» por parte de los prestadores de servicios de los datos que transmitan o almacenen, ni una obligación general de realizar búsquedas activas de hechos o circunstancias que indiquen actividades ilícitas, respecto de los servicios contemplados en los artículos 12, 13 y 14. En todos los artículos existe una cláusula de responsabilidad sólo cuando un tribunal o una autoridad administrativa, de conformidad con los sistemas jurídicos de los Estados miembros, exija al prestador de servicios que ponga fin a una infracción o que la impida.

[57] Si bien el Parlamento Europeo, desde el Tratado de Maastricht, ha cobrado mayor protagonismo en la creación de las normas comunitarias, no ostenta, a semejanza de los parlamentos nacionales, plena competencia para la elaboración de leyes, por lo que su intervención no reviste a la norma de un origen incontrovertiblemente democrático. En concreto, el artículo 249 (antiguo 189), que fue introducido por el Tratado de Maastricht, convertía al Parlamento Europeo en codecisor junto al Consejo, conforme al procedimiento establecido en el artículo 251, pero sólo en las materias expresamente mencionadas en el TCE. Aparte de esa intervención, el Parlamento Europeo también participa en el proceso normativo evacuando consultas y dictámenes (artículos 252 y 253) con una activa participación en procedimiento establecido en el artículo 252.

[58] El artículo 208 A es reformado en virtud el Tratado de Ámsterdam (Diario Oficial n° C 340 de 10 de noviembre de 1997) y reenumerado según el mismo — pasando a ser el actual 280 —. Este artículo ha tenido una rápida acogida en los Códigos Penales nacionales aún antes de su consagración comunitaria. Sin ir más lejos, nuestro Código Penal vigente castiga en los artículos 305 y ss. a los que defrauden a la Hacienda de la Comunidad Europea (art. 305.3), defrauden a los presupuestos generales de la Comunidad Europea (art. 306), obtengan indebidamente fondos de los presupuestos generales de la Comunidad Europea u otros administrados por ésta (art. 309). En todos los casos se fija el límite mínimo de la defraudación, a partir del cual la infracción es delictiva, en 50.000 euros.

[59] Esta cuestión abriría multitud de interrogantes que no están resueltos por la redacción de la norma. El artículo 280 TCE da similares competencias a la Comunidad y a los Estados miembros en materia sancionadora, habiendo éstos criminalizado las conductas de fraude contra los intereses de la Comunidad en la legislación penal nacional. Sería contradictorio, puesto que los Estados ya han establecido sanciones para esas conductas, que la Comunidad hiciera lo mismo. Habría duplicidad de normas sancionadoras para las mismas infracciones lo que llevaría a la inaplicabilidad automática de una de aquéllas, en virtud del principio, común a todos los Estados miembros, de “non bis in idem”. Lo que nos induce a pensar, que el espíritu del artículo 280 no persigue la elaboración de normas penales, aunque deja la puerta abierta por el mero hecho de no impedirlo.

[60] Enumeradas en los artículo 81 y 82 del TCE.

[61] Por ejemplo, el Reglamento (CE) n° 1/2003 del Consejo, de 16 de diciembre de 2002, relativo a la aplicación de las normas sobre competencia previstas en los artículos 81 y 82 del Tratado (Texto pertinente a efectos del EEE). Diario Oficial n° L 001 de 04/01/2003 p. 0001 – 0025. El artículo 23 faculta a la Comisión para la imposición de multas sancionadoras de hasta un 1 % del volumen de negocios total realizado durante el ejercicio social anterior. Asimismo el articulo 24 faculta a la Comisión

para imponer a las empresas y asociaciones de empresas multas coercitivas de hasta un 5 % del volumen de negocios medio diario realizado durante el ejercicio social anterior por cada día de retraso contado a partir de la fecha que fije en su decisión.

[62] SIEBER, Ulrich., op., cit., p. 230.

[63] Ello se observaría, vgr. en el caso de España, en la introducción de artículos en el Código Penal que persiguen los delitos ambientales. Como se sabe, la mayoría de los tipos penales relativos a la protección del medio ambiente son tipos penales en blanco, en los que existe una remisión a normas extrapenales cuya contravención debe verificarse para incurrir en la infracción. Los capítulos III (De los Delitos contra los Recursos Naturales y el Medio Ambiente) y IV (De los Delitos relativos a la Protección de la Flora, Fauna y Animales Domésticos) del Título XVI, Libro II, contiene varios tipos en blanco, referidos a normas administrativas que, tratándose de naturaleza ambiental, son en un 80% trasposición de directivas comunitarias.

[64] El artículo 5 TCE establece que "la Comunidad actuará dentro de los límites de las competencias que le atribuye el presente Tratado y de los objetivos que éste le asigna.
En los ámbitos que no sean de su competencia exclusiva, la Comunidad intervendrá, conforme al principio de subsidiariedad, sólo en la medida en que los objetivos de la acción pretendida no puedan ser alcanzados de manera suficiente por los Estados miembros, y, por consiguiente, puedan lograrse mejor, debido a la dimensión o a los efectos de la acción contemplada, a nivel comunitario.
Ninguna acción de la Comunidad excederá de lo necesario para alcanzar los objetivos del presente Tratado."

[65] Directiva del Consejo 91/303/CEE, de 10 de junio de 1991, relativa a la prevención de la utilización del sistema financiero para el blanqueo de capitales. (DO L 166 de 28.6.1991, p. 77).

[66] Comunicación de la Comisión, de 13 de marzo de 2001: «eEurope 2002 - Impacto y prioridades». Comunicación preparada para el Consejo Europeo de Estocolmo el 23 y 24 de marzo de 2001 [COM (2001) 140 final - sin publicar en el Diario Oficial].

[67] 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 electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas) [Diario Oficial L 201 de 31 de julio de 2002]. Reglamento (CE) n° 876/2002 del Consejo, de 21 de mayo de 2002, por el que se crea la Empresa Común Galileo [Diario Oficial L 138 de 28 de mayo de 2002]. Reglamento (CE) n° 733/2002 del Parlamento Europeo y del Consejo, de 22 de abril de 2002, relativo a la aplicación del dominio de primer nivel «.eu» [Diario Oficial L 113 de 30 de abril de 2002]. Comunicación de la Comisión, de 28 de mayo de 2002, al Consejo, al Parlamento Europeo, al Comité Económico y Social y al Comité de las Regiones - eEurope 2005: Una sociedad de la información para todos - Plan de acción [COM(2002) 263 final - no publicada en el Diario Oficial]. Directiva 2002/38/CE del Consejo, de 7 de mayo de 2002, por la que se modifica y se modifica temporalmente la Directiva 77/388/CEE respecto del régimen del impuesto sobre el valor añadido aplicable a los servicios de radiodifusión y de televisión y a algunos servicios prestados por vía electrónica [Diario Oficial L 128 de 15 de mayo de 2002]. Directiva 2002/21/CE del Parlamento Europeo y del Consejo, de 7 de marzo de 2002, relativa a un marco regulador común de las redes y los servicios de comunicaciones electrónicas (Directiva marco) [Diario Oficial L 108 de 24 de abril de 2002]. Directiva 2002/19/CE del Parlamento Europeo y del Consejo, de 7 de marzo de 2002, relativa al acceso a las redes de comunicaciones electrónicas y recursos asociados, y a su interconexión (Directiva acceso) [Diario Oficial L 108 de 24 de abril de 2002]. Directiva 2002/20/CE del Parlamento Europeo y del Consejo, de 7 de marzo de 2002, relativa a la autorización de redes y servicios de comunicaciones electrónicas (Directiva autorización) [Diario Oficial L 108 de 24 de abril de 2002]. Directiva 2002/22/CE del Parlamento Europeo y del Consejo, de 7 de marzo de 2002, relativa al servicio universal y los derechos de los usuarios en relación con las redes y los servicios de comunicaciones electrónicas (Directiva servicio universal) [Diario Oficial L 108 de 24 de abril de 2002]. Comunicación de la Comisión al Consejo, al Parlamento Europeo, al Comité Económico y Social y al Comité de las Regiones de 26 de enero de 2001 - Creación de una sociedad de la información más segura mediante la mejora de la seguridad de las infraestructuras de información y la lucha contra los delitos informáticos - eEurope 2002 [COM (2000) 890 final - no publicada en el Diario Oficial]. Decisión 2001/48/ CE del Consejo, de 22 de diciembre de 2000, por la que se adopta un programa plurianual comunitario de estímulo al desarrollo y el uso de contenidos digitales europeos en las redes mundiales y de fomento de la diversidad lingüística en la sociedad de la información [Diario Oficial L 14 de 18 de enero de 2001]. Reglamento (CE) nº 2887/2000 del Parlamento Europeo y del Consejo, de 18 de diciembre de 2000, sobre el acceso desagregado al bucle local [Diario Oficial L 336 de 30 de diciembre de 2000].

[68] Comunicación de la Comisión, de 28 mayo 2002, al Consejo, al Parlamento Europeo, al Comité Económico y Social Europeo y al Comité de las Regiones - Plan de acción eEurope 2005: una sociedad de la información para todos [Comunicación COM (2002) 263 final - no publicada en el Diario Oficial].
[69] El ya renombrado informe elaborado por: SIEBER, Ulrich. *Legal Aspects of Computer-Related Crime in the Information Society – COMCRIME – Study.*1 de junio de 1998. Versión 1.0. 240 págs.
[70] Posición Común 1999/364/JAI, de 27 de mayo de 1999, adoptada por el Consejo sobre la base del artículo 34 del Tratado de la Unión Europea, relativa a las negociaciones del proyecto de Convenio sobre delincuencia en el ciberespacio celebradas en el Consejo de Europa. DOUE L 142/1 de 5. 6. 1999.
[71] Diario Oficial n° C325 de 24 diciembre 2002 (versión consolidada.)
[72] Si bien el origen de Europol lo encontramos en el Acto del Consejo, de 26 de julio de 1995, relativo al establecimiento del Convenio por el que se crea una Oficina Europea de Policía, (DO C 316 de 27.11.1995), el denominado Convenio Europol, la institución ha ido llenándose progresivamente de competencias y recursos a través de actos y decisiones del Consejo, que pueden hallarse en http://europa.eu/scadplus/leg/es/lvb/l14005b.htm (página visitada el 18 de junio de 2006). El Tratado de Amsterdam modifica el artículo K.2 (hoy artículo 30) con el objeto de canalizar la cooperación a través de Europol.
[73] Eurojust se constituye como órgano de la Unión dotado con personalidad jurídica propia. es competente por lo que se refiere a las investigaciones y las actuaciones (en relación con al menos dos Estados miembros) relativas a las formas graves de delincuencia para promover la coordinación entre las autoridades competentes de los distintos Estados miembros y facilitar la aplicación de la cooperación judicial internacional y la ejecución de las solicitudes de extradición. Entre otras cosas, la competencia de Eurojust cubre los tipos de delincuencia y las infracciones de los que es competente Europol (por ej.: terrorismo, tráfico ilícito de estupefacientes, trata de seres humanos, falsificación de monedas, blanqueo de dinero), la ciberdelincuencia, el fraude y la corrupción, el blanqueo de los productos del crimen, la participación en una organización criminal. Eurojust se crea mediante Decisión del Consejo, de 28 de febrero de 2002 (DO L 63 de 6.3.2002), con el objeto de reforzar la lucha contra las formas graves de delincuencia. La decisión debió ser traspuesta a los Ordenamientos Nacionales el 6.9.2003 a más tardar. El informe de la Comisión de 6 de julio de 2004, sobre la transposición a los ordenamientos jurídicos nacionales de la Decisión que creaba Eurojust [COM (2004) 457 final - no publicado en el Diario Oficial], mostraba un balance decepcionante. Más información puede encontrarse en http://europa.eu/scadplus/leg/es/lvb/l33188.htm (página visitada el 18 de junio de 2006.)
[74] La Red Judicial Europea tiene por objeto mejorar desde el punto de vista jurídico y práctico la ayuda judicial mutua entre los Estados miembros de la Unión Europea, en particular para luchar contra las formas de delincuencia grave (delincuencia organizada, corrupción, narcotráfico y terrorismo.) Se crea mediante la Acción común 98/428/JAI, de 29 junio 1998, adoptada por el Consejo sobre la base del artículo K.3 del Tratado de la Unión Europea (actual artículo 31), relativa a la creación de una red judicial europea [Diario Oficial L 191 de 7.7.1998].
[75] Decisión del Consejo, de 28 de febrero de 2002 (DO L 63 de 6.3.2002), con el objeto de reforzar la lucha contra las formas graves de delincuencia. Disponible en: http://eur-lex.europa.eu/LexUriServ/site/es/oj/2002/l_063/l_06320020306es00010013.pdf.
[76] Si bien, aparentan gran similitud con las tradicionales directivas, se apartan de éstas en que las decisiones jamás pueden gozar del efecto directo cuando no se trasponen en plazo o cuando se trasponen precariamente sin contemplar el contenido con plenitud.
[77] Mediante este instrumento se han adoptado varios actos de gran relevancia para la lucha contra el cibercrimen. Por ejemplo, el Acto del Consejo de 16 de octubre de 2001, por el que se celebra el Protocolo del Convenio relativo a la asistencia judicial en materia penal entre los Estados miembros de la Unión Europea. DO n.º C 326, de 21.11.2001.
[78] Este asunto está resuelto en el Tratado por el que se establece una Constitución para Europa, que consagra, en el art. I-7 la personalidad jurídica de la Unión.
[79] DOUE L 138/1 de 9.6.2000.
[80] DO L 69 de 16. 3. 2005.
[81] La Decisión no alude expresamente a la Convención sobre cibercriminalidad hecha en Budapest, sin embargo su espíritu se encuentra presente en aquélla, por cuanto los delitos relacionados son un trasunto de los enumerados en la Convención. La no alusión sería debida a que en la actualidad el estado del proceso de ratificación va muy retrasado.
[82] La expresión produce ciertos equívocos, pues puede interpretarse de dos formas: a) o bien que los márgenes sólo son preceptivos en los grados máximos de las penas, por tanto el grado inferior podría consistir en una pena no privativa de libertad, lo que daría lugar a cierta disparidad entre las legislaciones penales de los Estados miembros; b) o bien entenderse que el grado máximo son los tres años, como mínimo. De cualquier modo, es evidente que la redacción se presta a muchos equívocos, teniendo que la legislación penal de los Estados miembros está todavía muy lejos de una unificación terminológica.

[83] Acción Común 98/733/JAI, de 21 de diciembre de 1998, relativa a la tipificación penal de la participación en una organización delictiva en los Estados miembros de la Unión Europea. DO L 351 de 29.12.1998, p. 1.
[84] De acuerdo con los apartados 1, letra a), y 2 del artículo 10.
[85] Acto del Consejo, del 29 de mayo del 2000, DO C 197 de 12.7.2000.
[86] Véase preámbulo del Convenio.
[87] Esta previsión final del artículo, contempla embrionariamente la posibilidad de se incorporen a dichos equipos miembros de Europol, Eurojust o de otros organismos que se pudieran poner en práctica en el futuro.
[88] LOURIDO RICO indica un supuesto en que se hace explícita referencia a estas actuaciones "externas". En la Recomendación de 30 de noviembre de 2000 que dirige el Consejo a los Estados miembros relativa al apoyo de Europol a los equipos conjuntos de investigación creados por los Estados miembros, [DOCE C357 de 13-12-2000, págs. 7 y 8], se recomienda a los Estados miembros que utilicen en sus equipos conjuntos de investigación a miembros de Europol, cuya intervención consistirá fundamentalmente en poner a disposición de los equipos la información de que disponga, apoyar en la coordinación centralizada de sus operaciones y prestarles asesoramiento técnico. Vid. LOURIDO RICO, Ana María. *La Asistencia Judicial Penal en la Unión Europea.* Primera edición. Valencia: Tirant Lo Blanch, 2004. p. 163-164.
[89] LOPEZ MORENO, Juana y FERNÁNDEZ GARCÍA, Emilio. "La Word Wide Web como vehiculo de delincuencia: supuestos frecuentes". En: LOPEZ ORTEGA, Juan José. Internet y Derecho Penal. 1ª edición. Madrid: Consejo General del Poder Judicial, 2001. p. 409. Los autores continúan diciendo: "Internet presenta una capacidad ilimitada para ser un medio y vehículo de delincuencia, mientras que la capacidad de los Estados es infinitamente menor, y se halla limitada por las fronteras exteriores, que no existen en Internet."
[90] D.O.C.E. L162, de 20-6-2002, págs. 1-3.
[91] LOURIDO RICO, Ana María., op. cit., p. 181.