El cibercrimen en el ámbito económico y patrimonial

Prof. Dr. iur Dr. med. Carlos María Romeo Casabona
Prof. Dr. Iñigo de Miguel Beriain

Tema 2º

Los criterios de intervención del Derecho Penal frente al ciberdelito
Los sujetos del ciberdelito
La aplicabilidad efectiva de la ley penal

4. LOS CRITERIOS DE INTERVENCIÓN DEL DERECHO PENAL FRENTE AL CIBERCRIMEN

Son varios los aspectos que se plantean en relación con las tomas de decisión político-criminales de configurar delitos relacionados con el ciberespacio. En primer lugar, decidir cuándo deberá intervenir el Derecho Penal, y bajo qué criterios. En segundo lugar, establecer cuál será la técnica legislativa más apropiada en cada caso para configurar nuevos delitos relacionados con el cibercrimen.

También afectan a decisiones de política legislativa, normalmente no penal, sino procesal penal o internacional, los aspectos

relativos a la aplicación de la ley penal en el espacio, la determinación de la jurisdicción competente, etc.

5. EL DERECHO PENAL COMO *ULTIMA RATIO*

No siempre es necesario el recurso al Derecho, y en particular al Derecho Penal, para lograr los propósitos de protección de los bienes jurídicos vinculados con los ataques relacionados con las TIC (sistemas y redes informáticos). El Derecho debe quedar reservado a cuando otros instrumentos no jurídicos no sean suficientes para conseguir tales objetivos; y al Derecho Penal en concreto debe acudirse únicamente cuando otros sectores del ordenamiento jurídico (p. ej., el Derecho Administrativo), hayan fracasado en sus cometidos de protección. Quiere así significarse que no puede pretenderse que la ordenación jurídica de la redes descanse exclusiva o fundamentalmente en el sistema penal, sino que debe orientarse en primer lugar a la adopción de acciones y medidas extrajurídicas como las ya aludidas, además de a otras jurídicas no penales (*ultima ratio*).

En efecto, no hay que olvidar una importante, frecuente y conocida reflexión, a saber: los instrumentos jurídicos son una vía para la protección de los bienes jurídicos, pero no la única ni probablemente la más eficaz. Para prevenir estas conductas parece más conveniente apostar, en primer lugar, por la adopción de medidas de seguridad y de protección de naturaleza diversa: físicas, tecnológicas (valiéndose de procedimientos informáticos) y laborales, en su caso; y deberán aplicarse con una intensidad proporcional al valor intrínseco de los sistemas informáticos que se posean y de su importancia operativa para la persona, empresa, entidad o administración pública afectadas. Así, la restricción de acceso a los locales en los cuales se encuentran sistemas informáticos con datos de trascendencia cuya integridad hay que salvaguardar; el establecimiento de claves de acceso con distintos niveles de accesibilidad a los trabajadores en función de su categoría, función y responsabilidad; la autentificación de la identidad de los comunicantes o de las partes de un negocio jurídico celebrado a través de la red (firma electrónica), etc.

Algunas de estas materias han sido reguladas normativamente con el fin de imponer a los distintos agentes que intervienen en la red la adopción de las medidas físicas o lógicas de seguridad y de protección que sean adecuadas. Así, la Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y del Comercio

Electrónico (LSSI), parcialmente derogada por la Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones; o los Reales Decretos 994/1999, de 11 de junio, por el que se aprueba el Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal, y 195/2000, de 11 de febrero, por el que se establece el plazo de implantación de las medidas de seguridad en tres niveles diferentes, en función de la naturaleza de los datos (básico, medio y alto, arts. 3 y 4 del RD 994/1999, siendo el primero de ellos el mínimo exigible).

Acotado lo anterior, y una vez traspasada la barrera del Derecho, decidir cuándo otros sectores del ordenamiento jurídico son insuficientes y cuándo actualizar la función del Derecho Penal como *ultima ratio*, dependerá de cada contexto ilícito concreto. Sin embargo, aunque someramente ya se han señalado algunas de las características de las TIC más susceptibles de entrar en el marco resolutorio del Derecho Penal: pueden verse afectados bienes jurídicos personales fundamentales o supraindividuales de especial interés social; la capacidad lesiva de dichos bienes a través de las TIC es potencialmente muy elevada, a la vista de su vulnerabilidad, de su capacidad repetitiva de los hechos ilícitos, de su repercusión a una pluralidad muy elevada de sujetos pasivos (víctimas); desde el punto de vista jurisdiccional y procesal son mayores las dificultades de aportar medios de prueba suficientes para sustentar una condena, determinar la ley penal aplicable y lograr que ésta recaiga con sus consecuencias jurídicas sobre los culpables de los hechos incriminados.

Este conjunto de circunstancias no sólo podrá justificar decisiones incriminadoras por parte del legislador, sino también la agravación de las penas de algunos delitos.

6. LA INCRIMINACIÓN DEL CIBERCRIMEN: PRINCIPIO DE LEGALIDAD Y TÉCNICAS LEGISLATIVAS

Una política legislativa en materia penal frente a los ciberdelitos no puede desconocer los aspectos técnicos relacionados con estos delitos, pues si el legislador se limita a la introducción de los delitos que haya considerado necesarios desde una perspectiva político-criminal, puede frustrar la eficacia punitiva. Tanto los

instrumentos y categorías jurídicas de la parte especial (las figuras delictivas contenidas en la ley penal en particular) como de la parte general del delito (los elementos comunes de todos los delitos) deberán ser analizados y, en su caso, adaptados normativamente a los requerimientos que planteen estos delitos, teniendo al mismo tiempo sumo cuidado de que el texto legal no sea servil en exceso, precisamente respecto a esas características técnicas.

Una muy trascendente cuestión jurídica que se plantea con el cibercrimen consiste en si los tipos penales tradicionales vigentes de un sistema jurídico dado permiten ser interpretados de forma extensiva, basada en una visión evolutiva o progresiva de los mismos, de forma que las conductas a las que dedicamos nuestra atención queden abarcadas por esos tipos delictivos, o, si por el contrario, estamos incurriendo en analogía perjudicial para el reo, contraria a uno de los basamentos irrenunciables del Estado de Derecho, como es el principio de legalidad de los delitos, si se tratase efectivamente tan sólo de 'hechos semejantes', pero no idénticos, al menos desde una perspectiva teleológica.

La necesidad de proteger los datos almacenados y archivados en sistemas informáticos o durante el curso de su circulación por la red, así como ésta misma y los propios sistemas informáticos, han dado lugar a que en derecho comparado encontremos numerosos ejemplos legislativos de esta preocupación, habiendo creado, por diversas técnicas legislativas, las figuras delictivas oportunas. Desde esta vertiente jurídico-penal, que es la que interesa aquí, el principio de legalidad (con sus consecuentes prohibición de la analogía y el requerimiento de taxatividad de la ley penal, esto es, de concreción suficiente de la descripción de las conductas prohibidas por la ley), así como los de mínima intervención y *ultima ratio* –ya mencionado- del Derecho Penal, se configuran como ejes fundamentales que ha de observar irrenunciablemente el legislador.

Las reformas legales realizadas a lo largo de los dos últimos decenios en los diversos sistemas jurídicos revelan la creciente preocupación porque las conductas dolosas que hemos agrupado en torno a las agresiones más graves realizadas contra medios o sistemas informáticos o a través de los mismos queden cubiertas por la ley penal sin ninguna concesión a posibles lagunas punitivas. Diversos organismos internacionales han recomendado en este sentido el aseguramiento de la punición, incluso por

medio de nuevas iniciativas legislativas, de la mayor parte de las conductas que hemos agrupado en este trabajo como delitos informáticos y ciberdelitos. Algunos países han incorporado nuevos tipos penales específicamente referidos a conductas relacionadas con agresiones en conexión con sistemas informáticos, lo que abunda en la idea de que los tipos penales tradicionales relacionados con aquéllas no satisfacían plenamente las exigencias político-criminales para lograr una protección adecuada de los bienes jurídicos afectados.

Las diversas reformas se podrían agrupar en dos modelos principales sobre la técnica legislativa más conveniente, según se expone a continuación.

6.1. La configuración de tipos de equivalencia

El primer modelo consiste, en efecto, en la creación de 'tipos de equivalencia', es decir, introducción de nuevos tipos penales que complementen a los ya existentes, corrigiendo o sustituyendo, en la descripción de la nueva acción típica, las carencias detectadas en aquéllos (p. ej., en lo relativo a los modos o formas de realización de la acción típica y al objeto material de la misma). O bien, en introducir figuras delictivas nuevas en aquellos casos respecto a los cuales así lo justifiquen las necesidades punitivas, siempre que el tipo correspondiente aparezca descrito teleológicamente orientado a un bien jurídico específico identificable.

Este modelo presenta la ventaja de concreción del tipo y de vinculación a bienes jurídicos merecedores de protección penal por lo general muy bien perfilados, lo que permite una mejor adaptación a las exigencias de la seguridad jurídica. Su contrapartida radica en que es relativamente fácil incurrir en excesivo casuismo o prolijidad, a la vez que se corre el riesgo de dejar sin cobertura determinadas conductas dignas de la intervención penal y otras nuevas que se pongan en práctica al hilo de los constantes avances tecnológicos en este sector. En particular este riesgo puede manifestarse si la descripción de la acción típica es excesivamente servil y rígidamente tributaria de la descripción de técnicas o procedimientos vinculados con aquéllas, pues unos y otros pueden quedar rápidamente anticuados. No obstante, estos riesgos son evitables, si se consigue depurar suficientemente el ámbito típico del delito.

6.2. La tipificación de conductas peligrosas

El otro modelo legislativo consiste básicamente en la descripción de conductas normalmente peligrosas para el correcto funcionamiento de los sistemas informáticos y sus diversos componentes, así como de la información que procesan y albergan, esto es, se protege aquél y éstos en cuanto tales por la potencialidad de producir una lesión a ciertos, diversos y no necesariamente determinados bienes jurídicos. Serían una variante de los llamados delitos de acción peligrosa, en los cuales ésta ha de presentar una peligrosidad real para el bien jurídico *ex ante*, es decir, en el momento del inicio de la acción, aunque al concluir ésta dicho bien no haya padecido peligro alguno (pues sería entonces un delito de peligro concreto).

Junto con la ventaja de asegurar una amplia cobertura penal frente a conductas indeseables por su potencialidad lesiva, presenta varios inconvenientes nada despreciables: abuso del recurso a la estructura de los delitos de peligro abstracto (o de peligrosidad) y de peligro abstracto-concreto (o de acción peligrosa); pérdida de perspectiva de los bienes jurídicos que se desean proteger; intervención penal tal vez excesiva en este campo, al adelantar la misma sin exigir el peligro concreto o la lesión del bien jurídico. Estas deficiencias comportan riesgos para la seguridad jurídica y de sobrepasar el principio de intervención penal mínima, pues puede adelantarse de forma considerable la intervención del Derecho Penal sin el referente preciso de bienes jurídicos suficientemente delimitados y sin que sea exigida por el delito su real puesta en peligro (principio de ofensividad).

El Convenio sobre Cibercrimen cuenta con ejemplos de ambos modelos, probablemente con una mayor presencia del segundo de los dos mencionados, pero con la llamativa peculiaridad de que acaba corrigiéndose al aceptar que los Estados Parte puedan introducir alguna restricción (por supuesto, también prevista en el propio Convenio) que aluda a la necesidad de que con la realización del hecho penado se persiga un fin determinado, finalidad subjetiva por lo general orientada a la lesión de un bien jurídico más explícito. Así, en relación con la falsificación de datos informatizados:

> *"Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno, cuando se cometa de forma deliberada e ilegítima, la*

> *introducción, alteración, borrado o supresión de datos informáticos que dé lugar a datos no auténticos, con la intención de que sean tenidos en cuenta o utilizados a efectos legales como si se tratara de datos auténticos, con independencia de que los datos sean o no directamente legibles e inteligibles. Cualquier Parte podrá exigir que exista una intención fraudulenta o una intención delictiva similar para que se considere que existe responsabilidad penal"* (art. 7º; subrayado añadido).

En este ejemplo no se logra en realidad apuntar hacia un bien o bienes jurídicos más definidos. En todo caso, los Estados Parte tendrán que afinar la concreta configuración de los tipos delictivos correspondientes, por medio de las iniciativas legislativas oportunas, dada la vigencia del principio de legalidad.

Una reforma penal en relación con la delincuencia vinculada a las TIC debería tener en cuenta las anteriores observaciones sobre los respectivos modelos, sin perjuicio de que parece más adecuado el primero de ellos como referente político-criminal.

6.3. El referente del Derecho positivo interno

Por lo que se refiere al Derecho español y a los problemas de tipicidad que puede suscitar la incriminación de algunas conductas y, en consecuencia, la escrupulosa observancia del principio de legalidad penal y la correlativa exclusión de la aplicación analógica de la ley penal cuando es contraria al procesado, debemos distinguir la situación hasta que concluyó la vigencia del CP 1973 y la generada a partir de la entrada en vigor de su sucesor, el CP 1995. Por otro lado, y en relación con las perspectivas de reforma del CP sobre esta materia, la Ley Orgánica 5/2010, de 22 de junio, por la que se modifica el Código Penal, introdujo algunos delitos nuevos.

En efecto, con anterioridad a la incorporación a las leyes penales de las figuras delictivas destinadas a la incriminación de alguna de las conductas señaladas más arriba existían en los diversos sistemas penales del derecho comparado e, indudablemente, también en el español, graves dificultades para la subsunción legal de aquéllas. En efecto, en relación con el CP 1973 el principal problema que se planteaba era el de averiguar si tales conductas resultaban punibles conforme al mismo. En muchos casos la punibilidad era cuando menos dudosa sin caer al mismo tiempo

en interpretaciones analógicas –no meramente extensivas- de la ley penal y poner de este modo en peligro el principio de legalidad de los delitos en relación con ciertos comportamientos que, sin embargo, sí debían ser punibles desde una perspectiva político-criminal.

La situación cambia de forma sustancial con el CP 1995, pues la introducción y expansión de la informática en la vida cotidiana, especialmente en la laboral y de servicios, así como las críticas doctrinales respecto a tales lagunas punitivas indeseables, despertaron la atención del legislador español, de modo que introdujo numerosas figuras delictivas en el CP 1995. Con ellas el legislador quiso colmar tales lagunas o despejar las importantes dudas se habían suscitado en torno a su sanción penal con el CP anterior.

Sin perjuicio de la valoración individual que pueda merecer cada una de las figuras delictivas específicas incorporadas al ordenamiento jurídico, debe acogerse favorablemente la *metodología adoptada* por el legislador español en el nuevo CP, consistente en la creación de figuras delictivas en atención al respectivo bien jurídico protegido y, a partir de éste, a la forma de ataque al mismo. Con tal propósito ha recurrido en ocasiones a la que hemos denominado más arriba como "técnica de equivalencia", sustituyendo algunos elementos del tipo por otros adaptados a las formas comisivas vinculadas o dependientes de las características de los sistemas informáticos (p. ej., el fraude o estafa informática, art. 248.2 del CP español).

En otros casos, la ley se ha centrado en asegurar una más firme protección penal de determinados bienes jurídicos que carecían de ella o lo era de forma muy desafortunada, a causa, la mayor parte de las veces, de la inadaptación de una legislación antigua y anticuada para las necesidades político-criminales de los nuevos tiempos (así, la protección de la intimidad y de los datos de carácter personal, art. 197 del CP; la capacidad competitiva de la empresa: secreto industrial, art. 278). Asimismo, se han acuñado conceptos jurídicos adaptados a estas tecnologías; así, la definición de documento, art. 26 del CP:

> *"A los efectos de este Código se considera documento todo soporte material que exprese o incorpore datos, hechos o narraciones con eficacia probatoria o cualquier otro tipo de relevancia jurídica".*

Por lo que se refiere a los hechos que se realizan a través de los medios informáticos, siendo éstos el simple medio de expresión o de comisión específico (que podríamos denominar "delitos de expresión", p. ej., difusión de pornografía, especialmente infantil, provocación al odio, a la xenofobia o a la discriminación por motivos racistas, apología del terrorismo, injurias o calumnias, publicidad engañosa, etc., a través de las redes telemáticas), no plantean -o no deberían plantear- ningún problema diferencial de tipicidad, si el hecho en sí es ya previamente punible con independencia de su comisión a través de las TIC. No obstante, es cierto que en ocasiones tales problemas llegan a producirse, probablemente debido entonces a deficiencias o inadaptaciones de técnica legislativa, aunque también a criterios político-criminales cambiantes: así sucede con la pornografía infantil (art. 189.1, b y 7 del CP), pues parece una reforma insuficiente si se pretendía reprimir penalmente y con amplio alcance las conductas relacionadas con ella perpetradas en la red, sin perjuicio de que sea discutible esa misma pretensión de incriminación tan extensa.

Como ya se indicó más arriba, la **LO 5/2010 de modificación del CP** ha introducido la tipificación como delito de algunas conductas relacionadas con las TIC, como son:

- ✓ ***los accesos no autorizados a datos o programas informáticos contenidos en un sistema informático o en parte del mismo o mantenerse en él contra la voluntad de la persona que tenga el legítimo derecho para excluirlo, vulnerando las medias de seguridad para impedirlo (art. 197.3),***
- ✓ ***el uso de tarjetas ajenas o cheques de viaje o sus datos (art. 248.2, c),***
- ✓ ***la distinción de las conductas típicas de dañar (y varias conductas más) y de obstaculizar o interrumpir el acceso a datos en relación con el delito de daños (art. 264),***
- ✓ ***la falsificación de tarjetas ("clonación" de tarjetas) (art. 399 bis),***
- ✓ ***delitos relacionados con la pornografía infantil (art. 189), respecto a la cual –y los demás delitos relacionados- se retoca la circunstancia agravante de reincidencia internacional (art. 190),***
- ✓ ***la agravación de algunos de estos delitos si se cometen por medio de una organización criminal (art. 197.8 y 264.3, 1º) y***
- ✓ ***responsabilidad penal específica cuando los autores de algunos de estos delitos lo sean personas jurídicas (así, arts. 189 bis, 399 bis. 1, párr. 2º).***

7. LOS SUJETOS DEL DELITO DE CIBERCRIMEN

En general es irrelevante para el Derecho Penal quiénes sean los sujetos activo y pasivo del delito, esto es, quiénes cometan el hecho y quiénes sean sus víctimas, respectivamente. Sin embargo, en algunas ocasiones sí puede ser relevante, al menos de forma indirecta. Esto ocurre en algunos casos con los delitos informáticos y en particular con los ciberdelitos.

7.1. Los sujetos activos: los prestadores de servicios en la red

En cuanto a los sujetos activos de estos delitos, esto es, las personas que han cometido el delito o han contribuido a su comisión, debería mencionarse en primer lugar a los operadores de redes y servicios de comunicaciones electrónicas, los proveedores de acceso a redes de telecomunicaciones y los prestadores de servicios de alojamiento de datos en la red, que son quienes prestan el acceso de sus clientes a la red y facilitan el alojamiento o almacenamiento de datos puestos a disposición de la red por parte de aquéllos.

El Convenio sobre Cibercrimen proporciona una definición sobre estos profesionales:

> *"Por proveedor de servicios se entenderá:*
>
> *i) toda entidad pública o privada que ofrezca a los usuarios de sus servicios la posibilidad de comunicar por medio de un sistema informático, y*
>
> *ii) cualquier otra entidad que procese o almacene datos informáticos para dicho servicio de comunicación o para los usuarios de ese servicio" (art. 1º, c).*

La primera cuestión que se plantea es que al incumbirles, como se verá más abajo, determinados deberes, entre ellos de vigilancia y de control, y en su caso bloqueo, de los contenidos de la información que contribuyen a acceder, difundir y distribuir entre los usuarios de la red. Sin embargo, al manejar ingentes volúmenes de información es prácticamente imposible desde un punto de vista técnico, y se recuerda que jurídicamente tampoco es deseable, pues llevaría a extender los mecanismos de control incluso a las comunicaciones reservadas. La segunda cuestión que deberá dejarse al menos apuntada es la relativa a la responsabilidad de las personas jurídicas en cuyo seno se cometen los delitos cibernéticos, pues en la definición de proveedor de servicios que acabamos de citar aquél puede serlo

una "entidad pública o privada" o "cualquier otra entidad", es decir, que ni siquiera llegue al rango de persona jurídica.

Aparte de estas reflexiones quedan los problemas particulares que pueden surgir sobre la identificación del autor o los autores de los ciberdelitos (especialmente en relación con los llamados *hackers*, *cyberpunks*, *crackers* y *sniffers*, entre otros). También deben quedar únicamente mencionados en este lugar la frecuencia de la aparición del *error iuris* en este ámbito, tanto en forma de error sobre los elementos normativos del tipo, como de error de prohibición (art. 14 CP), en particular cuando surge la cuestión de la relevancia penal del hecho a la luz de normas jurídicas extrapenales. Probablemente no sería inadecuado plantearse en estas circunstancias la posibilidad de trasladar aquí de algún modo las construcciones elaboradas en torno al error de prohibición condicionado culturalmente.

7.1.1. Responsabilidad penal de las personas físicas

Si bien los prestadores de servicios no suelen ser mencionados explícitamente en los tipos penales correspondientes, sí que les incumben determinadas obligaciones que les puede llegar a acreditar como garantes de un bien jurídico determinado (posición de garante) y por ello susceptibles de responder penalmente por un delito de comisión por omisión (v. art. 11, párr. 2º, letra a, del CP en relación con la LSSI) o variantes omisivas de garante, si no dan cumplidamente satisfacción a dichas obligaciones legales. Pero lo realmente cuestionable es si estas personas tienen realmente una posición de garante, o bajo qué circunstancias podría aceptarse ésta.

Conforme a la normativa vigente, estas obligaciones consisten en deberes de vigilancia y en la interrupción de la prestación de un servicio, en la retirada de determinados contenidos (art. 11 de la Ley de servicios de la sociedad de la información y de comercio electrónico, LSSI) y en la retención de los datos de conexión y tráfico originados por las comunicaciones establecidas por los clientes (art. 2º de la LSSI). Por otro lado, la legislación vigente establece asimismo la responsabilidad de los diversos proveedores de acceso a la red y prestadores de los diversos servicios, señalando los supuestos legales de exclusión de responsabilidad y, a su vez, las excepciones a dicha exclusión (véanse los arts. 13 a 17 de la LSSI). Estas últimas se basan en general en que el profesional, en primer lugar, haya tenido

determinados conocimientos de las actividades realizadas por el cliente (p. ej., mediante denuncia), en particular de la ilicitud de las mismas; y, en segundo lugar, en la no actuación con la diligencia debida para retirar los datos o impedir el acceso a los mismos, suprimir o inutilizar el enlace correspondiente.

Por consiguiente, la cuestión de la responsabilidad penal de estos profesionales se relaciona más inmediatamente con los actos de acceso, transferencia y difusión en la red de determinados contenidos en si mismos ya ilícitos, por parte de la persona o personas que realizan dichos actos de difusión, en relación con los deberes de bloquear o suprimir los enlaces de cuyo conocimiento ilícito haya tenido conocimiento. Otras obligaciones vienen a traducirse en formas de cooperación en la investigación criminal.

> El Tribunal Supremo ha aceptado que estas personas no son responsables penalmente por la información que se aloja y se difunde a través de sus recursos cuando, de acuerdo con la LSSI: a) No tengan conocimiento efectivo de que la actividad o la información almacenada es ilícita o de que lesiona bienes o derechos de un tercero susceptibles de indemnización, o b) si lo tienen, actúen con diligencia para retirar los datos o hacer imposible el acceso a ellos (sentencia TS de 18 de mayo de 2010).

De todos modos, es preciso plantear algunas reservas frente a la hipótesis de que por el mero hecho de ser tributarios de una posición de garante basada en presupuestos formales (en obligaciones de carácter legal, en este caso) hayan de ser responsables penalmente como consecuencia de cualquier omisión de control de sus clientes o de retirada de los contenidos puestos en circulación por éstos últimos, en concreto cuando éstos han cometido un delito a través de la red (p. ej., por acceder a información prohibida o por introducir en aquélla información ilícita). La estructura de la autoría y la participación (en general y en relación con los medios o soportes de difusión mecánicos en particular; recuérdese que el CP español establece una particular, limitada y subsidiaria forma de responsabilidad de los autores y partícipes de estos delitos, conocida como responsabilidad en cascada [art. 30]; la doctrina está dividida sobre si esta forma de responsabilidad es o no aplicable al asunto que nos ocupa) y de los delitos de comisión por omisión, por un lado, así como algunos principios fundamentales del Derecho Penal, como son los de legalidad y de culpabilidad, por otro, hacen más que

dudosa que la responsabilidad penal de los operadores y de los prestadores de servicios pueda llegar a sustanciarse en un buen número de las hipótesis imaginables.

Por consiguiente, una concepción material de la posición de garante reduce el alcance de ésta a los supuestos en los que realmente el prestador de servicios tiene el dominio fáctico sobre la fuente de peligro, condición irrenunciable para poder afirmar la equivalencia con la forma activa del delito de que se trate, y aquélla hemos visto que es relativa, dada la limitada capacidad de vigilancia y control de los accesos que canaliza o los servicios que presta, y siendo necesario, como se indicaba más arriba, que el sujeto sea consciente (que omita dolosamente) de la situación típica, tal conciencia no existirá en muchas ocasiones.

Finalmente, si aceptamos que la mayor parte de los delitos referidos a la difusión de contenidos en la red no son de resultado material, difícilmente podrá imputarse en relación con ellos un resultado al autor, por lo que por esta razón y otras de semejante entidad la estructura real de estos delitos cometidos por los proveedores y los prestadores de servicios no podrá ser la de comisión por omisión en sentido estricto, sino alguna otra forma omisiva, planteándose, a su vez, la cuestión de la punibilidad de las diversas formas intermedias de omisión, empezando por la previsible ausencia de tipicidad respecto a las mismas.

Aspectos relativos al conocimiento del contenido ilícito de la información pueden llegar a situar la cuestión, más allá de la comprobación de la concurrencia del tipo correspondiente, en torno a la conciencia de la antijuricidad de la conducta (error de prohibición) por parte del prestador de servicios en la red, pero, además, la delimitación de si sus obligaciones alcanzan –evidentemente, no- a la difusión de contenidos ilícitos en terceros países, pero no en el que radica el proveedor.

7.1.2. ¿Responsabilidad penal de las propias personas jurídicas?

Las personas jurídicas (empresas, sociedades, entidades, asociaciones, fundaciones, etc.) no podrían ser sujetos activos del delito de acuerdo con el viejo principio *societas delinquere non potest*, que todavía inspira la legislación de muchos países, (incluida hasta hace poco tiempo la española), por lo que si bajo tal régimen de no sanción penal de las mismas se comete algún delito a través de ellas, la entidad en cuanto tal no podrá ser

castigada penalmente (aunque sí ser sancionada por la Administración como consecuencia de la comisión de una infracción administrativa, cuando y según esté previsto legalmente). Sin embargo, sí podrán ser imputadas como autoras de ese delito las personas físicas que se hayan valido de aquélla para cometerlo, actuando en su nombre o representación (o mejor: en su lugar), esto es, que hayan realizado por si mismas, personalmente, la conducta típica punible, incluso en aquellas situaciones en las que la persona física que actuó no reúna las características exigidas por el tipo para poder ser sujeto activo del delito, sino tan solo la empresa o entidad en cuyo nombre o representación realizó la acción (p. ej., el empleado informático de una empresa que figura legalmente como prestadora de servicios en la red).

La antigua discusión sobre si las personas jurídicas también han de caer dentro de la esfera de la responsabilidad penal se ha extendido a este ámbito de las TIC, dado que el paso del tiempo ha puesto de manifiesto con mayor intensidad que la solución de la sola responsabilidad de las personas físicas no es suficiente, incluso, podría añadirse, aunque se prevean consecuencias accesorias aplicables a las personas jurídicas (art. 129 del CP), dada la estrecha dependencia de aquellas en relación con éstas. El Convenio sobre Cibercrimen apunta en esta dirección, si bien deja a la discreción de los Estados que son parte en él que dicha responsabilidad pueda ser de naturaleza civil, administrativa o penal (art. 12 del Convenio). En relación con ésta última, no cabe duda de que sería posible, aunque laborioso, resolver dogmáticamente la imputación de responsabilidad directa de las personas jurídicas, es decir, no teniendo que ser subsidiaria de la concreta substanciación de responsabilidad en una persona física. Cierto que esta vía acabaría conduciendo a la necesidad de construir un Derecho Penal específico para las mismas, al menos parcialmente, aunque se inspirase –como así debiera, con las adaptaciones oportunas-, en las grandes categorías doctrinales concebidas para la responsabilidad penal de las personas físicas.

En este estado de cosas, hay que mencionar que la Ley Orgánica 10/2010, de 22 de junio, de modificación del CP, ha zanjado esta discusión en España, al haber establecido la responsabilidad penal directa de las personas jurídicas, lo que constituye una de las novedades más significativas de esta reforma (art. 31 bis):

> *"1. En los supuestos previstos en este Código, las personas jurídicas serán penalmente responsables de los delitos cometidos en nombre o por cuenta de las mismas, y en su provecho, por sus representantes legales y los administradores de hecho o de derecho.*
>
> *En los mismos supuestos, las personas jurídicas serán también penalmente responsables de los delitos cometidos, en el ejercicio de actividades sociales y por cuenta y en provecho de las mismas, por quienes, estando sometidos a la autoridad de las personas físicas mencionadas en el párrafo anterior, han podido realizar los hechos por no haberse ejercido sobre ellos el debido control atendidas las concretas circunstancias del caso.*
>
> *2. La responsabilidad penal de las personas jurídicas será exigible siempre que se constate la comisión de un delito que haya tenido que cometerse por quien ostente los cargos o funciones aludidas en el apartado anterior, aun cuando la concreta persona física responsable no haya sido individualizada o no haya sido posible dirigir el procedimiento contra ella. Cuando como consecuencia de los mismos hechos se impusiere a ambas la pena de multa, los Jueces o Tribunales modularán las respectivas cuantías, de modo que la suma resultante no sea desproporcionada en relación con la gravedad de aquéllos.*
>
> *3. La concurrencia, en las personas que materialmente hayan realizado los hechos o en las que los hubiesen hecho posibles por no haber ejercido el debido control, de circunstancias que afecten a la culpabilidad del acusado o agraven su responsabilidad, o el hecho de que dichas personas hayan fallecido o se hubieren sustraído a la acción de la justicia, no excluirá ni modificará la responsabilidad penal de las personas jurídicas, sin perjuicio de lo que se dispone en el apartado siguiente." (…).*

El art. 33.7 del CP ha introducido un catálogo de penas específicas para los delitos cometidos por las personas jurídicas, algunas de las cuales encuentran su origen en las consecuencias accesorias que preveía el art. 129 CP hasta su modificación por la misma Ley citada.

Aunque esta cuestión ha sido objeto de gran debate, y en particular el modelo de incriminación de las personas jurídicas adoptado por el legislador español, no es éste el lugar para su discusión, sino para dar únicamente cuenta de la vigencia de este sistema en nuestro ordenamiento jurídico.

7.2. El sujeto pasivo: el sujeto pasivo masa, el menor y otros sujetos vulnerables

Por lo que se refiere al sujeto pasivo, es decir, la víctima del delito, es frecuente que en estos delitos aquél no sea singular. Al contrario, las propias características multiplicadoras del delito de las TIC ponen de manifiesto la facilidad con que la acción delictiva puede recaer sobre una pluralidad de víctimas, en muchas ocasiones en número muy elevado y frecuentemente con indeterminación de su cuantía e identidad.

Sujeto pasivo masa. Por consiguiente, la conocida construcción dogmática del "sujeto pasivo masa" se revela como casi una constante en estos delitos, mediante la cual la responsabilidad se fija en atención del total de la lesión producida, aunque afecte a titulares del bien jurídico atacado distintos; así, se impondrá la pena prevista para el delito más grave; y si se trata de delitos contra el patrimonio, se atenderá para determinar la figura aplicable al total del perjuicio ocasionado, pudiendo llegarse a penas muy elevadas (pena superior en uno o dos grados a la inicialmente prevista para el delito) por otros mecanismos de agravación previstos (art. 74.1 y 2 del CP). La duda que surgía en el pasado sobre si la respuesta penal frente al delito masa es suficiente a la vista de la enorme capacidad lesiva que presentan estos procedimientos técnicos desde el punto de vista de los sujetos pasivos queda resuelta en sentido afirmativo. De todos modos, queda abierta la reflexión sobre si esta construcción del CP debería prever la posibilidad de una ulterior agravación de la pena cuando el número de víctimas y/o el perjuicio causado sean extraordinariamente elevados y el delito se ha cometido en conexión con las TIC.

El recurso a procedimientos de las TIC automatizados para lograr ese efecto multiplicador respecto a los sujetos pasivos no se ve obstaculizado por la exigencia legal de un elemento subjetivo específico ("en ejecución de un plan preconcebido o aprovechando idéntica ocasión", art. 74.1), pues el sujeto es consciente y quiere aprovecharse precisamente de tales recursos repetitivos automatizados (dolo). Es más, precisamente estas características comisivas del hecho anudan y fortalecen la cualidad indiciaria de la concurrencia del elemento subjetivo legalmente requerido, así como la identidad –más que semejanza- del precepto infringido.

Menores. En otro orden de ideas, pero igualmente relacionado con el sujeto pasivo, conviene tener presente que los sistemas informáticos han puesto en evidencia la vulnerabilidad que pueden comportar para los menores, por los contenidos inapropiados para ellos que pueden difundirse a través de la red y cuyo acceso es relativamente fácil de conseguir por cualquier usuario, incluidos aquéllos. No interesa en este lugar despejar la cuestión del castigo penal de los autores de aquellos contenidos o de quienes los han introducido en la red, sin perjuicio de que en la mayor parte de los casos su intención no es tener como destinatarios de los mismos a los menores. Lo que quiere subrayarse de nuevo ahora es que existen otros tipos de medidas, que no son jurídicas, sino de seguridad física y lógica, a las que me refería más arriba, que han sido concebidas para impedir accesos no deseados realizados por menores. En primer lugar, cabe que el autor o difusor de los contenidos inapropiados incluya en la página inicial advertencias sobre su contenido y sobre la no autorización de acceso a menores, lo que constituye una mera advertencia, desde luego significativa, pero no puede ser calificada en realidad como una barrera u obstáculo de acceso. Existen, asimismo, procedimientos de accesos reservados (p. ej., disposición de códigos de acceso), medida que puede ser más efectiva. En segundo lugar, las medidas de control podrían establecerse en los terminales a través de los cuales suele o puede acceder con más facilidad el menor (terminales de centros educativos o culturales, equipos domésticos, cibercafés o servicios similares, etc.).

De nuevo debe evitarse también aquí la intervención del Derecho Penal, si lo que se pretende es únicamente hacer frente a que el menor pueda acceder a determinados contenidos. En otros ámbitos cibernéticos, sin embargo, su vulnerabilidad es muy elevada y loa respuesta penal podría ser más severa.

8. LA APLICABILIDAD EFECTIVA DE LA LEY PENAL

La comisión de delitos a través o en conexión con las TIC suele generar dificultades específicas para la determinación del lugar de comisión del delito. En último extremo, la cuestión gira en torno a la determinación del juez competente para conocer y juzgar los hechos. Si en la comisión del delito se hallan implicados los territorios de varios Estados, habrá que despejar cuál es la ley

aplicable, pues el juez, dado el principio de soberanía, sólo tiene jurisdicción para aplicar las leyes de su propio Estado, sin perjuicio de las excepciones de extraterritorialidad que pueda contemplar la ley.

Por otro lado, los diversos principios para la aplicación de la ley de un determinado Estado plantean con frecuencia nuevos y complejos problemas jurídicos. Así, se aprecian graves insuficiencias si se procede con estricta vinculación al principio de territorialidad, pero no son de menor entidad los excesos a los que puede conducir la búsqueda de otros principios de aplicación extraterritorial de la ley penal.

8.1. La determinación de la jurisdicción competente

Algunos ejemplos servirán para ilustrar los diversos problemas subyacentes. Piénsese, por ejemplo, si A, que reside en Madrid, vende o cede pornografía infantil a través de la red a B, residente en San Sebastián. O si X introduce en la red un virus informático muy destructivo desde un equipo terminal situado en Tailandia, produciendo sus efectos devastadores en sistemas o equipos informáticos de Filipinas, Japón, España, Francia, Estados Unidos, Canadá, etc. La cuestión que habrá que dilucidar es qué juez es competente para juzgar a A en el primer ejemplo, ¿el de Madrid, lugar donde se introdujo el material pornográfico en la red, o el de San Sebastián, que es donde se accedió a dicho material? En el otro ejemplo, la cuestión se complica, por varios motivos: supongamos que X no causó daño alguno con el virus introducido a ningún usuario de su país: ¿deberán perseguirle los tribunales de justicia de Tailandia? Por el contrario, ¿pueden considerarse competentes para juzgar a X los tribunales de los diversos países en los que se ha producido el daño, aplicando para ello su ley respectiva? ¿Cuál de ellos tendrá preferencia? ¿Cómo se hará efectivo el procesamiento y juicio de X si no se encuentra en ninguno de dichos países? ¿Y si en la legislación penal de alguno de estos países –incluido el país desde el que se introdujo el virus en la red- el hecho realizado por X no está castigado como delito?

En resumen, el problema más acentuado que plantea la efectividad de la persecución penal de los hechos cometidos a través de la red consiste en la determinación del lugar y tiempo de comisión del delito (*locus tempusque delicti commissi*), pues la respuesta a este interrogante permitirá a su vez determinar cuál

es el juez competente para el conocimiento de tales hechos, así como la ley penal aplicable. En efecto, la sociedad de la información, caracterizada muy marcadamente por la ausencia de fronteras y por la inmaterialidad de la comunicación, ha conducido en el ámbito del Derecho a la irrelevancia de los límites temporales y espaciales que han constituido el límite tradicional de aquél.

No cabe duda de que cuando la acción se realiza y el resultado se produce en el territorio de un mismo Estado es aplicable la ley de ese Estado, la ley del lugar donde se cometió el delito (principio de territorialidad). En esta hipótesis la respuesta del Derecho español es semejante: se aplica la ley española y son competentes para juzgar los jueces españoles (Cfr. el art. 23.1 de la Ley Orgánica del Poder Judicial, LOPJ). Una cuestión distinta es determinar cuál es el juez competente, dentro de un solo Estado, para conocer de los hechos. La respuesta variará de un sistema jurídico a otro, pero dado que gran parte de estos delitos no son de resultado material (por tanto, no responderán por lo general a la estructura de los delitos a distancia), habrá que referirse, en principio, al lugar en el cual se realizó la acción.

Por lo demás, éste es el criterio adoptado por el Derecho español (Cfr. art. 14 de la Ley de Enjuiciamiento Criminal, LECri). En su defecto, lo será el Juzgado que incoó en primer lugar las diligencias (Cfr. art. 15 de LECri). En este sentido se ha pronunciado el Tribunal Supremo en su auto de 26 de marzo de 1998. No obstante, ocasionalmente se ha admitido alguna excepción, sin perder de vista que se trataba de un delito de resultado material. Así, en relación con el delito de estafa y su comisión por medio de las TIC (fraude informático) se ha estimado competente el Juzgado del lugar en donde se produce la consumación de delito, es decir, donde se produce el efectivo desplazamiento patrimonial (auto del Tribunal Supremo de 27 de octubre de 1998: estafa en una transacción realizada por el procedimiento de televenta).

8.2. Las limitaciones de la aplicación del principio de territorialidad

La cuestión es más problemática cuando los hechos guardan relación con más de un Estado, por ejemplo, si el acceso ilegal se realiza desde el territorio de un Estado, pero se hace efectivo en un sistema informático o archivo situados en otro Estado, o si el

acceso a los datos o la comunicación privada se realizan atravesando varios Estados (delito en tránsito). El punto de partida ha de ser de nuevo el principio de territorialidad, pero teniendo presente que en este caso todos los lugares de tránsito han de considerarse irrelevantes para este asunto, como también lo es el lugar en donde radica el proveedor de acceso a la red o el prestador de servicios, dado que ni la acción ni el resultado –de producirse- recae en ninguno de ellos, a salvo de que esté en juego determinar una posible responsabilidad de dicho proveedor. Con todo, se plantea también aquí la cuestión de la determinación del lugar de la comisión del delito con el fin ya señalado de poder establecer cuál será el juez competente para conocer de los hechos y en consecuencia determinar también la ley que resulte aplicable, pues el principio de territorialidad no suele aportar soluciones satisfactorias, cualquiera que sea la teoría del *locus commissi delicti* que se adopte (teoría de la acción, teoría del resultado y teoría de la ubicuidad o mixta).

Conforme a la teoría de la acción para los delitos que nos ocupan aquí el lugar –y momento- relevante lo será aquél desde el que se realizó el acceso, la introducción de los contenidos ilícitos o la alteración ilícita de los datos. Esta teoría presenta la ventaja en relación con estos delitos de que será más fácil la persecución y procesamiento del autor de los hechos, al encontrarse más probablemente en el lugar donde los cometió.

No obstante, pueden presentarse algunas circunstancias en la aparición del delito que requieren alguna aclaración o discusión. Así, en los supuestos de omisión se propone que se tenga en cuenta el lugar en el que se encontraba el sujeto cuando omitió la acción que estaba obligado a realizar. Este podría ser el caso del proveedor de acceso a la red que no cancela dicho acceso y las páginas introducidas en aquélla por un cliente teniendo un contenido ilícito (p. ej., difusión de pornografía infantil, incitación a la xenofobia, etc.), siempre que esté obligado a ello por la ley, pues en este caso podría ostentar la llamada posición de garante, condición necesaria, como se ha visto, para poder ser sujeto de un delito de comisión por omisión. De todos modos, en el caso de la omisión siempre queda pendiente la cuestión de determinar el momento en el que se entiende realizada aquélla.

En principio, el lugar de la acción en relación con los actos de difusión de contenidos ilícitos lo será aquél desde donde se introducen los datos, voz, sonido o imagen en la red o desde

donde se incorpora a ésta un mensaje de correo electrónico. Por lo que se refiere a los delitos contra sistemas informáticos o contra la integridad (p. ej., delitos de daños) y confidencialidad de la información lo será el lugar desde el que se introduce el virus informático o se produce el acceso o entrada ilegal a dichos sistemas o archivos.

También se ha propuesto y discutido la oportunidad de la aplicación de la teoría del resultado, pues serán las autoridades judiciales y policiales del lugar donde se produjo la lesión del bien jurídico, el resultado dañoso para el mismo, las que tengan mayor interés en la persecución de los responsables de los hechos causantes de dicha lesión. El hecho de que el autor o los autores se encuentren en el territorio de otro Estado (p. ej., en el que se perpetró la acción delictiva) podría resolverse acudiendo a varios procedimientos de entreayuda judicial, en particular a la extradición, aunque ésta se encuentra a su vez sometida a varias limitaciones jurídicas, como la de no entrega de los nacionales.

Los problemas surgen en otro ámbito, vinculado con las características que presentan algunos delitos respecto al resultado. Es sabido que existe un grupo de delitos cuya estructura no requiere el acaecimiento de ningún resultado material (llamados por ello también delitos de simple actividad: delitos de peligrosidad –o de peligro abstracto- y de acción peligrosa –o de peligro abstracto-concreto), por lo que en relación con ellos esta teoría del resultado sería inaplicable y habría que acudir indefectiblemente a la teoría de la acción. Así, puede ser problemático decidir cuál es la jurisdicción competente en los casos de accesos ilegales a bases de datos o a sistemas informáticos situados en un Estado diferente al del lugar desde el que se realizó dicho acceso, sobre todo si no se ha irrogado ningún daño material a los mismos, si bien podría argumentarse a favor del lugar en el que se sustanció dicho acceso, es decir, en el que se encontraba el sistema invadido. Aquí podrían entrar en juego los delitos de descubrimiento y revelación de secretos en relación con los datos personales, o bien el delito de espionaje industrial, si el acceso afecta a información de interés económico. Véase en relación con el Derecho español los arts. 197.3, que recoge el delito de acceso no autorizado, vulnerando las medidas de seguridad establecidas para impedirlo, a datos o programas informáticos contenidos en un sistema informático ajeno (según la reforma de la LO 5/2010), y 278.1 del CP, respectivamente. V.

también el delito del art. 197.2, bien es cierto que exige que se actúe con la intención de perjudicar a un tercero o al titular de los datos ("en perjuicio de tercero").

Algo semejante ocurre si se ponen en circulación determinados contenidos ilícitos, p. e.j., de incitación al racismo, a la xenofobia, o se difunde pornografía prohibida. En estos delitos, en sentido estricto, es problemático identificar un resultado material.

Para intentar resolver estas limitaciones se ha llegado a proponer algún criterio extensivo respecto a la noción de resultado que, en conclusión, comporta la aceptación de que el resultado lo es en todo caso el efecto de la acción descrito en el tipo penal, o de que todos los delitos informáticos conllevan un resultado material. Lo cierto es que ninguno de estos criterios se concilia bien con las construcciones dogmáticas que se han elaborado sobre estos delitos, esto es, identificar –o, tal vez mejor, confundir- el resultado material, característico de algunos delitos, con el resultado de lesión del bien jurídico protegido en relación con cada figura delictiva, cuando en realidad son dos conceptos diferentes, pues en el último supuesto coincide con el lugar de la acción.

Frente a éstas y otras propuestas que conducen a una aplicación extensiva de la ley penal se han opuesto diversos criterios limitativos, con el fin de reducir el ámbito de punibilidad de los delitos cometidos a través de la red, conteniendo así los efectos hipertróficos no deseables a los que podrían aquellos criterios. Unos son de carácter subjetivo, y atienden a que el autor se haya representado o no el lugar del resultado, esto es, supone exigir al autor una especie de dolo respecto al lugar del resultado. Pero es cierto que tal propuesta no es viable, tanto porque sería de difícil prueba tal extremo, cuanto que, en realidad, las reglas sobre la aplicación de la ley en el espacio no forman parte del tipo de la figura delictiva cometida y por ello no tienen que ser abarcadas por el dolo del autor, pues aquél, el dolo, se limita a la conciencia y voluntad de la realización de los elementos objetivos del tipo, los cuales sólo de forma excepcional mencionan el lugar o el tiempo del delito.

Otros criterios de carácter restrictivo que se han propuesto pretenden situarse en un plano objetivo y consisten en exigir un punto de conexión con el país –o países- en el que supuestamente se habría producido el resultado, el cual sería de carácter

territorial (p. ej., el idioma en el que está escrito el mensaje o documento); o en aplicar el principio de oportunidad, conforme al cual en estos casos no debería ejercitarse la acción penal si el hecho ya fue juzgado y castigado penalmente en otro país, pero asumiendo la persecución penal si el hecho es atípico en el lugar de su comisión o de residencia del autor. Por el contrario, algunos autores propugnan la aplicación del principio de doble incriminación, es decir, que el hecho constituya delito tanto en el Estado de realización de la acción como de producción del resultado, con el fin de mantener las pretensiones expansionistas de algunos Estados dentro de unos límites razonables.

Por otro lado, existen riesgos expansivos de otra índole, como la incriminación de algunas conductas realizadas a través de la red, en concreto, aquéllas que consisten en la introducción y difusión de determinados contenidos que pueden ser lícitos en el Estado desde el que se introducen o difunden (lugar de la acción), por estar amparados en el ejercicio de la libertad de expresión, pero que en otro pueden ser delictivos (lugar de recepción o del resultado, en su caso), por enfrentarse a las creencias religiosas, concepciones culturales, ético-sociales, etc., protegidas penalmente. Así, es posible que algunas expresiones, imágenes o manifestaciones puedan ser calificadas como delito de blasfemia, contra la religión, apología del nazismo, pornografía, etc., de acuerdo con la ley del Estado receptor. De este modo se corre el riesgo de que un Estado pretenda convertirse en una suerte de guardián moral de la red (En cierto sentido, la sentencia del Tribunal Supremo Federal Alemán de 12.12.2000 (BGHSt 46, 212, caso Toeben) parece apuntar en esta dirección, al considerar que es aplicable el parágr. 130 I y III a la difusión a través de Internet (www) de contenidos de odio introducidos por un extranjero en un servidor extranjero que sean accesibles desde la R. F. Alemana), o de que simplemente persiga cualquier información circulante contraria a los intereses de sus dirigentes (los medios de comunicación han dado cuenta de que como consecuencia de esta actitud algunos proveedores de servicios -Microsoft, Yahoo y Google- en determinado momento cedieron a las presiones de las autoridades chinas y han retirado de la red algunos contenidos considerados políticamente inadecuados.), lo que podría derivar en gravísimas restricciones para la libertad de expresión cibernética, aparte de su dudosa eficacia. Sin perjuicio de que en estos casos puede excluirse la responsabilidad penal por ausencia de dolo en el autor o por haber incurrido en un error de

prohibición, pues el usuario no siempre tendrá conciencia de que el hecho realizado constituye un ilícito penal en un tercer país, sobre todo si no lo es en el suyo propio, es preferible buscar otras soluciones más seguras, que pasan necesariamente por una regulación en el Derecho Internacional, como se dirá más abajo.

En términos generales parece más aconsejable partir de la teoría de la ubicuidad, esto es, aceptar para la determinación de la ley aplicable tanto el momento y lugar de realización de la acción como los de la producción del resultado (de existir éste). En cualquier caso, hay que asumir que en no pocas ocasiones las soluciones que se obtengan con la aplicación de esta construcción tampoco serán satisfactorias, por ejemplo cuando no se haya podido determinar con precisión el lugar de comisión de los hechos. En este sentido, pero en relación con un presunto delito contra la propiedad intelectual cometido a través de Internet, el Auto de la Audiencia Provincial de Barcelona de 25 de abril de 2002 ha establecido que aun habiendo sido cometido el hecho a través de un servidor bajo dominio de los EEUU, no puede descartarse que haya podido cometerse en territorio español, por lo que en virtud de los arts. 23.1 de la LOPJ y 14 y 15 de la LECri considera que los hechos caen bajo la competencia de los órganos jurisdiccionales españoles.

También debe tenerse en cuenta cuando no haya un resultado material, como hemos visto más arriba que suele ocurrir en los delitos contra la intimidad y contra los datos de carácter personal, circunstancia de la que se deriva el riesgo de impunidad del autor en el Estado de realización de la acción cuando el hecho no es punible en él por razones ético-culturales u otras. Por otro lado, como se dirá a continuación, será necesario tener presentes otros criterios complementarios.

En resumen, las reflexiones precedentes nos sitúan ante una peculiar paradoja, si se pretende resolver los problemas de persecución eficaz de los ciberdelitos por medio de las construcciones jurídico-penales tradicionales analizadas más arriba, que fueron concebidas en realidad para una dinámica delictiva sustancialmente diferente de la que caracteriza a los ciberdelitos. La paradoja radica, por un lado, en la dificultad, por un motivo u otro, de perseguir estos delitos y, por otro, en el efecto contrario que puede dar lugar a una criminalización y persecución expansivas de los mismos, tampoco satisfactorias. A este respecto, el principio de doble incriminación (esto es, que el

hecho constituya delito tanto en el país donde se cometió el hecho como en el que el autor está a disposición de los tribunales de justicia para ser juzgado) presenta una doble vertiente, también paradójica. Por un lado, su exigencia permitiría contener los excesos a los que podría conducir una desmedida intromisión por parte de un Estado como consecuencia del ejercicio de la libertad de expresión frente a una máxima protección penal de determinados valores socio-culturales; pero, por otro, podría ser una legitimación de impunidad consecuente a la situación de los ordenamientos jurídicos poco sensibles a la persecución penal y, por ello, tipificación de los delitos cibernéticos (paraísos Informáticos).

9. PROCEDIMIENTOS DE ENTREAYUDA JUDICIAL: LA EXTRADICIÓN

La extradición consiste en la entrega de un delincuente por parte del Estado en cuyo territorio se ha refugiado a aquél que es competente para juzgarle o para imponer la pena (o la medida) impuesta.

La extradición constituye uno de los instrumentos jurídicos más importantes hasta el momento de cooperación entre los Estados para asegurar que los autores de delitos graves serán juzgados por los tribunales competentes, a pesar de que se encuentren en el territorio de otro estado.

La extradición presupone: i) que los jueces españoles son competentes para conocer del caso, que la ley española resulta aplicable al delito en cuestión, y el mismo presupuesto s aplicable cuando es un tercer Estado el que solicita la extradición; ii) que el presunto autor del hecho se encuentra fuera del territorio jurídico del Estado, por lo que no puede ser juzgado o no se puede ejecutar, en su caso, la pena.

En este lugar vamos a centrarnos, por su mayor interés para esta exposición, en la llamada extradición activa, que concurre cuando un Estado solicita a otro la entrega de un imputado que se encuentra en el territorio de éste último (la pasiva consiste en la entrega del delincuente al Estado que solicita la entrega, la cual se rige por unas reglas jurídicas diferentes). La extradición activa se encuentra regulada en el Derecho español en la LECri (arts. 824 y ss.). En ella se establecen una serie de requisitos para que el Estado español pueda solicitar la extradición de un justiciable a otro Estado, de los cuales destacamos aquí los siguientes:

El principio identidad o de doble incriminación: comporta que el hecho perseguido constituya delito tanto conforme a la legislación española como a la del Estado requerido. Es imaginable que, conforme se apuntó más arriba, este principio falle en alguna ocasión por la existencia de diferencias culturales entre los dos Estados afectados, o por la carencia de una legislación penal suficiente en el Estado requerido (paraísos jurídicos). No obstante, la LOPJ ha modificado este requisito sobre la competencia de los jueces españoles para conocer de delitos cometidos en el extranjero por españoles o extranjeros que hayan adquirido la nacionalidad española: "Que el hecho sea punible en el lugar de ejecución, salvo que, en virtud de un Tratado internacional o de un acto normativo de una Organización internacional de la que España sea parte, no resulte necesario dicho requisito" (art. 23.2, a).

El principio de *ne bis in idem*: no se puede castigar a una persona dos veces por el mismo hecho con el mismo fundamento, lo que significa que si ha sido ya juzgada (absuelta o condenada) o ha cumplido la pena (al menos parcialmente) no podrá solicitarse la extradición (o no será concedida) al menos por ese mismo hecho.

Principio de gravedad del delito imputado: dada la complejidad que implica la extradición, suele exigirse que el hecho por el que se solicita la extradición constituya un delito de cierta gravedad. Esta condición suele darse, no obstante, en gran parte de los delitos informáticos sancionados en la actualidad.

Por su interés, recogemos a continuación las reglas que prevé el Convenio sobre Cibercrimen para la extradición (art. 24):

> *"1. a) El presente artículo se aplicará a la extradición entre las Partes por los delitos establecidos en los artículos 2 a 11 del presente Convenio, siempre que estén castigados en la legislación de las dos Partes implicadas con una pena privativa de libertad de una duración máxima de como mínimo un año, o con una pena más grave.*
>
> *b) Cuando deba aplicarse una pena mínima diferente en virtud de un acuerdo basado en legislación uniforme o recíproca o de un tratado de extradición aplicable entre dos o más Partes, incluido el Convenio Europeo de Extradición (STE nº 24), se aplicará la pena mínima establecida en virtud de dicho acuerdo o tratado.*

2. Se considerará que los delitos mencionados en el apartado 1 del presente artículo están incluidos entre los delitos que dan lugar a extradición en cualquier tratado de extradición vigente entre las Partes. Las Partes se comprometen a incluir dichos delitos entre los que pueden dar lugar a extradición en cualquier tratado de extradición que puedan celebrar entre sí.

3. Cuando una Parte que condicione la extradición a la existencia de un tratado reciba una solicitud de extradición de otra Parte con la que no haya celebrado ningún tratado de extradición, podrá aplicar el presente Convenio como fundamento jurídico de la extradición respecto de cualquier delito mencionado en el apartado 1 del presente artículo.

4. Las Partes que no condicionen la extradición a la existencia de un tratado reconocerán los delitos mencionados en el apartado 1 del presente artículo como delitos que pueden dar lugar a extradición entre ellas.

5. La extradición estará sujeta a las condiciones establecidas en el derecho interno de la Parte requerida o en los tratados de extradición aplicables, incluidos los motivos por los que la Parte requerida puede denegar la extradición.

6. Cuando se deniegue la extradición por un delito mencionado en el apartado 1 del presente artículo únicamente por razón de la nacionalidad de la persona buscada o porque la Parte requerida se considera competente respecto de dicho delito, la Parte requerida deberá someter el asunto, a petición de la Parte requirente, a sus autoridades competentes para los fines de las actuaciones penales pertinentes, e informará a su debido tiempo del resultado final a la Parte requirente. Dichas autoridades tomarán su decisión y efectuarán sus investigaciones y procedimientos de la misma manera que para cualquier otro delito de naturaleza comparable, de conformidad con la legislación de dicha Parte.

7. a) Cada Parte comunicará al Secretario General del Consejo de Europa, en el momento de la firma o del depósito de su instrumento de ratificación, aceptación, aprobación o adhesión, el nombre y la dirección de cada autoridad responsable del envío o de la recepción de solicitudes de extradición o de detención provisional en ausencia de un tratado.

b) El Secretario General del Consejo de Europa creará y mantendrá actualizado un registro de las autoridades designadas por las Partes.

Cada Parte garantizará en todo momento la exactitud de los datos que figuren en el registro".

El Convenio sobre Cibercrimen prevé asimismo otros procedimientos de cooperación judicial en el ámbito de los ciberdelitos.