El cibercrimen en el ámbito económico y patrimonial

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

Tema 7º

Hacia un nuevo Derecho Internacional y Europeo contra el cibercrimen.
El Convenio Europeo sobre Cibercrimen.
El Derecho supranacional de la Unión Europea.
Conclusiones de política legislativa.

29. La necesidad de un Derecho Penal Internacional sobre el cibercrimen

Tanto en el Derecho comparado como en el Derecho supranacional e internacional se han venido dando pasos importantes con el fin de prevenir y combatir estas nuevas formas de la criminalidad telemática. En concreto, son notables los esfuerzos que durante los últimos años han venido desplegando en este sector de la criminalidad organismos tan diferentes como el Consejo de Europa, el G8, la OCDE, Interpol y Naciones Unidas.

De todos modos, se ha puesto de relieve que si durante las décadas de los setenta y los ochenta apenas se encuentran actividades preventivas o normativas en el ámbito internacional, en la actualidad este vacío se ha suplido considerablemente, pero nos encontramos con una falta de coordinación de tantas iniciativas, con el riesgo de que se solapen unas con otras, con respuestas todavía demasiado imprecisas y por lo general con un recurso excesivo a los aspectos legales.

Las razones que justifican e incluso imponen esta dimensión jurídica de cooperación internacional han sido explicadas en el Preámbulo del Convenio sobre el Cibercrimen -al que me referiré más abajo- con gran precisión:

- Es necesaria una política penal común con el fin de proteger a la sociedad de la criminalidad en el ciberespacio, en concreto mediante la adopción de una legislación adecuada y mediante la mejora de la cooperación internacional.

- Un factor relevante sobre esta necesidad es la constatación del incremento, convergencia y mundialización permanente de las redes informáticas.

- Existe la preocupación de los organismos internacionales porque las redes informáticas y la información electrónica estén siendo utilizadas también para cometer infracciones penales y que las pruebas de estas infracciones sean transmitidas por medio de tales redes.

- En consecuencia, es necesaria una cooperación entre los estados y la industria privada en la lucha contra la cibercriminalidad, así como proteger los intereses legítimos en relación con la utilización y el desarrollo de las tecnologías de la información, por lo que dicha cooperación internacional en materia penal debe aumentar y debe ser asimismo rápida y eficaz.

- Los actos más necesitados de esta cooperación, prevención y, en su caso, represión penal, son los vinculados con la confidencialidad, la integridad y la disponibilidad de los sistemas informáticos, de las redes y de los datos, así como la utilización fraudulenta de dichos sistemas, redes y datos.

En el ámbito supranacional también la Unión Europea ha venido mostrando su preocupación e interés por dotar de medios jurídicos adecuados para lograr una efectiva persecución de los delitos relacionados con la delincuencia organizada con expresión a través de de las TIC. Diversas Decisiones-Marco reflejan esta acción, pues si bien durante los últimos años se venía discutiendo, sobre todo entre los penalistas europeos hasta qué punto era admisible la afirmación de que la UE no tenía atribuciones para entrar directamente en asuntos penales, en coherencia con el limitado alcance de sus competencias en este sector, lo cierto es que se ha dado un giro al respecto, en especial a partir de la aprobación del Tratado de Lisboa.

30. INICIATIVAS INTERNACIONALES Y SUPRANACIONALES SOBRE LA PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL. EL CONVENIO SOBRE CIBERCRIMEN

30.1. El Derecho Internacional Europeo

En el Derecho internacional europeo se ha proclamado de forma reiterada el reconocimiento del respeto de la vida privada como derecho fundamental.

Así, el Convenio Europeo para la protección de los derechos humanos y de las libertades fundamentales, de 4 de noviembre de 1950, establece que "toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia" (art. 8.1), vedando toda injerencia de la autoridad en el ejercicio de este derecho, sino "en tanto en cuanto esta injerencia esté prevista por la Ley y constituya una medida que, en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención del delito, la protección de la salud o de la moral, o la protección de los derechos y libertades de los demás" (art. 8.2).

También contamos con la aportación, en su momento innovadora, del Convenio nº 108, de 28 de enero de 1981, sobre la Protección de las personas en relación con el tratamiento automatizado de datos de carácter personal, que ha sido revisado en diversas ocasiones. El cumplimiento de las obligaciones contraídas con este Convenio (el Instrumento de ratificación por parte del Reino de España es de 27 de enero de 1984), así como del mandato constitucional establecido en el art. 18.4 de la CE, dio origen a la

primera ley del ordenamiento jurídico español destinada a la protección de datos de carácter personal, si bien permaneció en vigor tan sólo durante siete años (LORTAD, de 1992). Asimismo, si bien es cierto que fue discutida por la doctrina su aplicación y alegación directas ante los tribunales de justicia (en virtud no de su naturaleza jurídica obligatoria, a partir de la cual no cabe duda de que la respuesta no podía ser más que afirmativa, sino por la propia estructura del Convenio), en todo caso constituye todavía hoy un instrumento jurídico interpretativo en la materia (a este respecto, el TC, en su sentencia 254/1993, de 20 de julio, destaca que constituye un instrumento interpretativo e informador del contenido básico esencial del derecho reconocido en el art. 18.4 de la CE). El respaldo penal de la protección de datos de carácter personal se produjo con el CP de 1995, desde que en varios proyectos de reforma del CP se previeran algunos delitos con una estructura poco afortunada. Aunque la interpretación y aplicación de los delitos incluidos en el art. 197 y siguientes del CP vigente es extremadamente dificultosa y censurable en muchos aspectos, estos preceptos son, con mucho, más acertados que los que se habían incluido en los textos prelegislativos previos.

En relación con la protección de datos de carácter personal el Consejo de Europa ha tomado otras iniciativas, concretadas en su mayor parte en Recomendaciones. Así, la R (87) 15, dirigida a regular la utilización de datos de carácter personal en el sector de la policía.

No cabe duda de que los datos de carácter personal, de las comunicaciones entre particulares, en suma, de la vida privada, no constituyen el único objetivo de las conductas criminales vinculadas al cibercrimen. En efecto, existen otras conductas que se mueven en torno a intereses sociales diferentes y que pueden afectar a bienes jurídicos de muy diversa naturaleza e importancia y que se han mostrado especialmente vulnerables cuando de algún modo se desenvuelven en le ciberespacio. Por consiguiente, los esfuerzos que se habían venido realizando en el ámbito internacional con el fin de dotar de nuevos instrumentos jurídicos frente a las agresiones informáticas resultaban cuando menos insuficientes.

Con el propósito de cubrir estas carencias y más directamente vinculado con el Derecho Penal y con figuras delictivas no orientadas únicamente a la protección de los datos de carácter personal, es decir, con un objeto de interés mucho más amplio

que los convenios anteriores, se encuentra el Convenio del Consejo de Europa sobre el Cibercrimen (*Convention on Cybercrime*), cuyo articulado ha sido citado en varias ocasiones a lo largo de estos materiales. Por la trascendencia que puede representar en el futuro –confiemos en que no muy lejano- como fuente de inspiración de los legisladores de los Estados europeos y como herramienta de armonización y uniformización de la legislación penal europea en relación con estos delitos, merece una breve exposición aparte.

30.2. El Convenio Europeo sobre Cibercrimen

El interés y la preocupación del Consejo de Europa por la correcta utilización de los sistemas y datos informáticos, por la protección de los ciudadanos en relación con ellos y, finalmente, por la prevención y represión de las infracciones penales que pudieran cometerse, no es reciente, al contrario, cuenta con una larga trayectoria de trabajos, resoluciones y recomendaciones que han culminado, por el momento, en el Convenio sobre el Cibercrimen de 2001. Así, pueden citarse varias Recomendaciones, como la R (89) 9, sobre la delincuencia en relación con el ordenador, que indica a los legisladores nacionales principios directrices para definir ciertas informaciones informáticas, la R (95) 13, relativa a los problemas de procedimiento penal vinculados con las tecnologías de la información.

El Convenio Europeo sobre Cibercrimen, elaborado en el seno del Consejo de Europa y aprobado en Budapest el 23 de noviembre de 2001, que ha sido firmado por el Reino de España y está pendiente todavía de ratificación. Por lo demás, el Convenio ya ha entrado en vigor, y entre los Estados signatarios deben destacarse los EEUU, al no ser un estado europeo. Indudablemente, su incorporación al ordenamiento jurídico español comportará obligatoriamente la revisión del Código Penal vigente, como consecuencia de la estricta vigencia del principio de legalidad de los delitos, pues prevé la introducción de numerosos delitos, podemos adelantar ya que la estructura de algunos de ellos puede plantear no pocos problemas político-criminales y dogmáticos.

El Convenio constituye un buen ejemplo de la culminación efectiva de un instrumento internacional en este sector jurídico-penal de la cibercriminalidad. Para el logro de tan importante objetivo de cooperación internacional no han sido ajenos los

trabajos previstos que se han ido realizando en su seno, según se ha expuesto más arriba.

La importancia que ha concedido la comunidad internacional a este Convenio como medio de cooperación contra una forma de delincuencia en plena expansión y sobre todo con modalidades comisivas muy complejas y difíciles de encajar se ve reflejada que a la apertura de la firma fue ya suscrito por veintiocho estados miembros del Consejo de Europa, entre ellos España, así como por Canadá, Estados Unidos, Japón y Sudáfrica. Su relevancia en particular se refleja en que presta una atención intensa tanto a los aspectos sustantivos como a los procesales y de cooperación internacional.

Debe señalarse que introduce nuevas figuras delictivas, como son, en primer lugar, las dirigidas específicamente a la protección de la confidencialidad e integridad de datos y sistemas informáticos: delitos de acceso ilegal (art. 2º), de interceptación ilegal (art. 3º), interferencia de los datos (art. 4º) o del sistema (art. 5º); dispositivos ilegales (art. 6); delitos informáticos, constituidos por la falsedad informática (art. 7) y el fraude informático (art. 8); infracciones relativas al contenido: pornografía infantil (art. 9); delitos contra la propiedad intelectual y derechos conexos (art. 10). Con posterioridad, el Protocolo Adicional al Convenio de 2003 ha añadido un grupo más de delitos, relativos a actos de naturaleza racista, xenófoba o apología o negación del genocidio y de los crímenes contra la humanidad. A este Protocolo me he referido en el Tema 6º.

La introducción de estos delitos comportará asimismo una revisión de los bienes jurídicos protegidos, pues aparentemente no parece que vayan a conciliarse de forma pacífica con la sistemática de bienes jurídicos del actual CP.

Merece asimismo ser destacado que el Convenio prevé la sanción penal de la participación y la tentativa en estos delitos (art. 11), establece la responsabilidad de las personas jurídicas (art. 12), así como medidas para la conservación rápida de datos informáticos almacenados a efectos de la prueba, previniendo así el riesgo de su modificación o eliminación (art. 16).

Por lo que se refiere a la aplicación de la ley penal, esto es, a la jurisdicción competente, el Convenio supone ya un importante paso de armonización normativa (art. 22), aunque esté limitada al

marco europeo. En relación con esta cuestión el Convenio prevé disposiciones específicas relativas a la aplicación de la ley penal en el espacio, si bien no resultan suficientes, pues únicamente consagra el principio de territorialidad completado por el de personalidad (el Estado se atribuye competencias para la persecución de sus nacionales por los delitos cometidos en otro Estado), siempre que el hecho constituya delito en el lugar de su realización, o en el caso de que el delito no de lugar a competencia territorial por parte de ningún Estado (art. 22.1, d), sin perjuicio de no excluir otras competencias que pudieran tener asumidas los Estados Parte. Estos principios habrán de completarse con otros, como los principios de oportunidad, de doble incriminación, etc. También en este ámbito se plantea y se resuelve la concurrencia de jurisdicciones (art. 22.5).

Según el art. 22 del Convenio: "1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para afirmar su jurisdicción respecto de cualquier delito previsto con arreglo a los artículos 2 a 11 del presente Convenio, siempre que se haya cometido: a) en su territorio; o b) a bordo de un buque que enarbole pabellón de dicha Parte; o c) a bordo de una aeronave matriculada según las leyes de dicha Parte; o d) por uno de sus nacionales, si el delito es susceptible de sanción penal en el lugar en el que se cometió o si ningún Estado tiene competencia territorial respecto del mismo. 2. Cualquier Estado podrá reservarse el derecho a no aplicar o a aplicar únicamente en determinados casos o condiciones las normas sobre jurisdicción establecidas en los apartados 1.b) a 1.d) del presente artículo o en cualquier otra parte de los mismos. 3. Cada Parte adoptará las medidas que resulten necesarias para afirmar su jurisdicción respecto de los delitos mencionados en el apartado 1 del artículo 24 del presente Convenio, cuando el presunto autor del delito se encuentre en su territorio y no pueda ser extraditado a otra Parte por razón de su nacionalidad, previa solicitud de extradición. 4. El presente Convenio no excluye ninguna jurisdicción penal ejercida por una Parte de conformidad con su derecho interno. 5. Cuando varias Partes reivindiquen su jurisdicción respecto de un presunto delito contemplado en el presente Convenio, las Partes interesadas celebrarán consultas, siempre que sea oportuno, con miras a determinar cuál es la jurisdicción más adecuada para las actuaciones penales."

En cuanto a la cooperación internacional entre los Estados se establecen facilidades para la extradición, mediante la ampliación automática de la misma de los tratados ya existentes a estos delitos (art. 24); para la entreayuda judicial y policial (art. 25), así como información espontánea (art. 26).

30.3. El Derecho supranacional: Derecho de la Unión Europea

Respecto al Derecho comunitario, la Unión Europea ha ido asumiendo a lo largo de los últimos años competencias en materia penal, en particular a partir del nuevo régimen competencial que se establece en el nuevo Tratado de la Unión Europea (Tratado de Lisboa).

En primer lugar, debe destacarse previamente la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, que ha sido el origen de la armonización legal de esta materia en todos los Estados miembros de la Unión. En el caso de España, esto se hizo mediante la transposición de esta Directiva con la LO 1999/15, de 13 de diciembre, sobre protección de datos de carácter personal. Por tanto, aunque no recoge aspectos penales, esta Directiva tiene interés desde el punto de vista penal, porque constituye asimismo un referente para la interpretación de la figura delictiva relativa a los datos de carácter personal o familiar. El objetivo de esta importante regulación comunitaria es compatibilizar la protección de los derechos fundamentales de las personas físicas con el libre flujo de los datos, como proyección del libre flujo de productos y mercancías que caracteriza a la Unión Europea:

> "1. Los Estados miembros garantizarán, con arreglo a las disposiciones de la presente Directiva, la protección de las libertades y de los derechos fundamentales de las personas físicas, y, en particular, del derecho a la intimidad, en lo que respecta al tratamiento de los datos personales. 2. Los Estados miembros no podrán restringir ni prohibir la libre circulación de datos personales entre los Estados miembros por motivos relacionados con la protección garantizada en virtud del apartado 1".

No menor interés para nuestro objeto de estudio presenta la Directiva 97/66/CE, del Parlamento Europeo y del Consejo, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las telecomunicaciones. Esta disposición ha sido superada por la Directiva 2000/31/CE, de 8 de

junio, relativa a determinados aspectos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior.

Por último, no cabe duda de la trascendencia que tendrá para el futuro comunitario el Tratado de Lisboa, nueva constitución de la Unión Europea, para los Estados miembros, pues ha dado acogida al derecho a la protección de los datos de carácter personal. Sus antecedentes se encuentran en la Carta Europea de los derechos fundamentales, proclamada en Niza el 28 de septiembre de 2000. Su art. II-68 establece:

> "Protección de datos de carácter personal. 1. Toda persona tiene derecho a la protección de datos de carácter personal que la conciernan. 2. Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que la conciernan y a su rectificación. 3. El respeto de estas normas quedará sujeto al control de una autoridad independiente".

Más específico es el instrumental jurídico que aprobó el Consejo de la Unión Europea, pues está dirigido a diversos delitos relacionados con la red. Se trata de la Decisión Marco de 2002, relativa a los ataques dirigidos contra los sistemas información, y tiene por objeto reforzar la cooperación entre las autoridades judiciales y policiales, por medio de la aproximación de las legislaciones penales de los Estados miembros.

Conforme a esta Decisión Marco los Estados miembros precederán a tomar las medidas necesarias para sancionar como delito en sus legislaciones internas el "acceso ilegal a los sistemas de información" (art. 3) la "intromisión ilegal en los sistemas de información" (art. 4). Con la primera infracción se pretende perseguir penalmente los supuestos de *hacking*, referidos tanto al acceso, con cualquier finalidad, a sistemas protegidos como no protegidos, siempre que se realice intencionadamente. Con la segunda se persigue un variado conjunto de conductas dirigidas a entorpecer el funcionamiento de los sistemas de información.

Con la Decisión Marco 2005/222/JAI del Consejo de la Unión Europea, de 24 de febrero de 2005, relativa a los ataques contra los sistemas de información, se vuelven a incluir los delitos anteriores y otro más: delitos el *acceso ilegal a los sistemas de información*, entendiendo por tal "el acceso intencionado sin autorización al conjunto o a una parte de un sistema de información", dejando a

la discrecionalidad de los Estados miembros que este hecho sea únicamente sancionable cuando la infracción se cometa transgrediendo medidas de seguridad (art. 2); la *intromisión ilegal en los sistemas de información*, es decir, el "acto intencionado, cometido sin autorización, de obstaculizar o interrumpir de manera significativa el funcionamiento de un sistema información, introduciendo, transmitiendo, dañando, borrando, deteriorando, alterando, suprimiendo o haciendo inaccesibles datos informáticos" (art. 3); y la *intromisión ilegal en los datos*, "el acto intencionado, cometido sin autorización, de borrar, dañar deteriorar, alterar, suprimir o hacer inaccesibles datos informáticos contenidos en un sistema de información" (art. 4). Se establece la persecución penal obligatoria de la inducción y la complicidad de estos delitos, así como la tentativa, en este caso al menos en los dos últimos delitos (art. 5). Se prevén penas de prisión, que pueden tener una duración de una a tres años en las dos variantes de intromisión (art. 6), así como algunas circunstancias agravantes (art. 7) y la responsabilidad de las personas jurídicas (art. 8) y sus sanciones específicas (art. 9). Como medidas de control añadidas se prevé el intercambio de información entre los Estados miembros relativa a las infracciones que incluye esta Decisión Marco, lo que se hará a través de la Secretaría General del Consejo y de la Comisión (art. 11).

También encontramos previsiones penales sobre el terrorismo, incluido el que pueda valerse de los sistemas de la información. Así, Decisión marco 2002/745/JAI del Consejo, de 13 de junio de 2002, sobre la lucha contra el terrorismo, que a su vez fue modificada por la Decisión Marco 2008/919/JAI del de 28 de noviembre de 2008. Tiene interés mencionar algunos de sus considerandos, en cuanto que vincula las actividades terroristas con Internet, no porque éste pueda ser un objetivo de las bandas terroristas, sino, sobre todo, porque los terroristas se valen de la red para comunicarse, para captar a nuevos agentes o para realizar actividades de aprendizaje y entrenamiento:

> "(3) La amenaza terrorista ha crecido y se ha desarrollado rápidamente durante estos últimos años, con cambios en el *modus operandi* de los terroristas y sus partidarios, incluida la sustitución de grupos estructurados y jerárquicos por grupúsculos semiautónomos ligados entre ellos con flexibilidad. Tales grupúsculos forman redes internacionales y recurren cada vez más a las nuevas tecnologías, en especial Internet.

> (4) Internet se utiliza para inspirar y movilizar a redes terroristas locales e individuos en Europa y también sirve de fuente de información sobre medios y métodos terroristas, funcionando por lo tanto como un «campo de entrenamiento virtual». Por ello, las actividades de provocación a la comisión de delitos de terrorismo, la captación y el adiestramiento de terroristas se han multiplicado con un coste y unos riesgos muy bajos".

31. CONCLUSIONES DE POLÍTICA LEGISLATIVA

A la vista de cómo se manifiestan las diversas modalidades de la llamada cibercriminalidad (y de los delitos informáticos), de la vulnerabilidad de las TIC y de que algunas herramientas jurídicas actuales no son suficientes para captar sus diversas dimensiones, se hace imprescindible una política legislativa que afronte con enfoques más modernos y dinámicos este fenómeno. Este punto de partida implica asumir que el caber espacio no debe sustraerse a cualquier forma de regulación, amparándolo como un teórico espacio de libertad. Puesto que contra o a través de las redes telemáticas pueden cometerse delitos, el Derecho Penal debe dar una respuesta adecuada a los mismos.

De todos modos, la adopción de reacciones penales ha de basarse escrupulosamente en el principio de proporcionalidad, teniendo en este caso como referente la mínima interferencia en la libertad de expresión, el respeto de la intimidad y de los datos personales, y el libre flujo de las comunicaciones telemáticas. Asimismo, es preciso estar atentos a las diferencias culturales existentes en los diversos países, puesto que a través de Internet podrían entrar en contacto y verse enfrentadas: xenofobia, ideologías extremistas, ofensas religiosas, etc.; mientras que, al mismo tiempo, en otros países podrían ser, simplemente, manifestaciones de la libertad de expresión reconocida constitucionalmente. La persecución penal de estas conductas podría comportar al mismo tiempo la criminalización de ciertas valoraciones de origen cultural.

La prevención de los delitos informáticos y cibernéticos debe abordarse de una forma integral, es decir, con el recurso simultáneo a medidas jurídicas penales y no penales, así como a otro tipo de medias no legales (técnicas, autorregulación de las empresas del sector, educativas, etc.), teniendo en cuenta, en todo caso, las características técnicas en las que se desenvuelven estos delitos, si quiere evitarse la aprobación de leyes que resultarán

inaplicables en la práctica y por ello ineficaces para la persecución de estos delitos.

Las acciones de política legislativa habrán de tener presentes otros aspectos más específicos de estas tecnologías. Una de estas características más peculiares es la naturaleza incorpórea de la información, su intangibilidad. Desde un punto de vista jurídico significa que no debe pretenderse proteger esta información aplicando criterios semejantes a los utilizados para la protección de los objetos materiales. Así, es necesario distinguir el propietario de los datos, su tenedor, la persona a la que se refieren esos datos, la propia sociedad. Al mismo tiempo, debe prestarse atención a los sujetos del delito, pues en unos casos como en otros (es decir, los sujetos activos y pasivos del delito) se presentan especificidades que requieren tanto un examen dogmático como político-criminal.

Las nuevas manifestaciones de criminalidad en el ciberespacio exigen su tratamiento jurídico-penal desde una perspectiva internacional, pues la sola acción de los Estados, la aplicación de las leyes penales nacionales, se agota en su propio espacio territorial, mientras que la red es global y transnacional; como efecto, este limitado horizonte podría dar lugar a la creación de "paraísos informáticos o cibernéticos". La proliferación de esta situación no sólo daría lugar al aumento de las dificultades para la persecución de estos delitos, sino que, además, podría tener como efecto la restricción de los mercados del sector y la imposición de barreras nacionales al libre flujo de la información, y no es deseable que prolifere este tipo de reacciones. En consecuencia, demandan grandes esfuerzos de armonización normativa -penal y extrapenal-, aparte de intensificar otras formas de colaboración en esta dimensión internacional, a la vista de los numerosos y complejos problemas de extraterritorialidad que pueden plantear estos delitos y de los conflictos de atribución de competencias por parte de más de un Estado. El Convenio Europeo sobe Cibercrimen constituye un logro en esta dirección, al haber entrado ya en vigor en una docena de Estados europeos, aunque todavía no en el español.

En concreto, es previsible que haya que completar el principio básico de la territorialidad respecto a la aplicación de la ley penal en el espacio con los principios real o de protección de intereses o, incluso, de justicia mundial, lo que requeriría una modificación de la legislación oportuna (Estos principios se hallan regulados en

el Derecho español en el art. 23.3. y 4 de la LOPJ) y el correspondiente apoyo, en su caso, por medio del Derecho Internacional Convencional, es decir, a través de Tratados y Convenios Internacionales que prohíban algunos de los hechos relacionados con la ciberdelincuencia.

De acuerdo con el principio real o de protección de intereses, un Estado se considera competente para conocer de determinados delitos, señalados previamente por la ley, aunque no se hayan cometido en el territorio de ese Estado ni el autor sea un nacional del mismo, siempre que lesiones intereses que se consideran esenciales para ese Estado (ej., la falsificación de moneda). Por lo que se refiere al principio de justicia mundial, el Estado que ha detenido a un delincuente se considera competente para conocer de determinados delitos sea cual fuere el lugar de su comisión, la nacionalidad del autor y, en su caso, del propio sujeto pasivo. Se entiende que aquí se lesionan los intereses de la comunidad internacional reflejados por tratados internacionales y requiere una cierta uniformidad de la legislación penal de los Estados.

Asistimos desde los últimos decenios a una cierta ampliación de este último principio, facilitado por la existencia de una mayor comunicación entre los Estados en diversos ámbitos y por diversas circunstancias:

- mayor solidaridad entre los Estados;
- las legislaciones penales de los Estados son más homogéneas entre si;
- aumento de la delincuencia internacional, como una excrecencia de los procesos de globalización;
- existencia de una entreayuda judicial más estrecha (extradición, cooperación policial).

Algunos de los delitos recogidos en la LOPJ que responden al principio de justicia mundial, son comparables, en cuanto a su gravedad, a las formas más graves de los ciberdelitos. Este principio aparece recogido en el Derecho español en relación con los siguientes delitos: "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 relativos a la prostitución y los de corrupción de menores o incapaces [téngase en cuenta que, de acuerdo con la rúbrica correspondiente a estos delitos en el CP español, acogería ya la pornografía infantil]. 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" (art. 23.4 de la LOPJ).

Si añadimos a lo anterior la mayor y en ocasiones extrema dificultad de su persecución efectiva, podrían muy bien incorporarse a la lista de aquéllos (p. ej., el ciberterrorrismo, la incitación a la xenofobia y al odio racial, incluso daños en sistemas o archivos informáticos con efectos devastadores para un elevado número de usuarios o titulares de aquéllos, siempre que se acote debidamente el ámbito conceptual de cada uno de estos delitos), o bien como consecuencia de las obligaciones derivadas de la firma y ratificación de convenios o tratados dirigidos a la persecución de determinados delitos especialmente graves (v. art. 23.4, h, de la LOPJ).

El llamado principio de justicia supletoria, que actuaría como principio subsidiario y supletorio de todos los anteriores, no parece que sea una solución indicada en esta materia, a la vista de las reflexiones apuntadas más arriba sobre la necesidad de contención de la atribución de competencias punitivas por parte de los estados y de que éstos (en concreto, algunos de ellos) puedan convertirse, desde una posición hegemónica, en guardianes de la justicia mundial, por su puesto, exterior a su territorio, aplicando su propio ordenamiento jurídico a hechos que ni afectan a sus intereses ni a los de la comunidad internacional.

En relación con los demás delitos que no tuvieran acogida en los principios de extraterritorialidad mencionados, el principio de doble incriminación podría delimitar mejor el campo de aplicación de la ley penal correspondiente.

Es necesario, asimismo, investigar las vinculaciones que se han establecido o pueden hacerlo en el futuro entre estas tecnologías y el crimen organizado: traficantes de materiales prohibidos (armas, drogas), trata de blancas, terrorismo. Sólo de este modo se

tendrá un conocimiento suficiente a qué necesidades y frente a qué conductas criminales ha de enfrentarse el Derecho Internacional.

Los procesos de armonización legal han de tener presentes también las discrepancias en la forma de abordar la criminalización y tipificación de estos hechos en los diversos sistemas del Derecho comparado, así como en relación con la aplicación de la ley penal en el espacio y la extradición. En concreto, pueden manifestarse estas diferencias tanto en los aspectos político-criminales (p. e., cómo se concibe y aplica el principio de intervención mínima del Derecho Penal) como dogmáticos (así, cómo se entiende la tentativa de delito). En este punto el Derecho Internacional desempeñará un papel esencial en el logro de una mínima puesta en común y uniformización de las normas, así como en la aplicación de algunas instituciones de entreayuda internacional (p. ej., estableciendo el principio de doble incriminación como condición previa para la concesión de la extradición del responsable de uno de estos delitos).

Finalmente, los delitos cibernéticos pondrán a prueba la efectividad de la entreayuda judicial, en particular de la extradición, pues estas formas de cooperación pueden ser decisivas para lograr una efectiva persecución y, en su caso, condena, de los autores.