DETERMINACIÓN DE LA JURISDICCIÓN Y COMPETENCIA PARA LA INVESTIGACIÓN Y ENJUICIAMIENTO DE LOS DAÑOS INFORMÁTICOS[1]

Juan Carlos Ortiz Pradillo
Profesor de Derecho Procesal
Universidad de Castilla-La Mancha

[1] Ponencia impartida el 23 de mayo de 2016 en el Centro de Estudios Jurídicos del Ministerio de Justicia, con motivo del Curso de Formación "Los delitos de daños informáticos", dirigido por el Ilmo. Sr. D. Roberto Valverde Megías, Fiscal Delegado de Criminalidad Informática. Fiscalía Provincial de Barcelona. Cualquier comentario será bienvenido en la siguiente dirección: JuanCarlos.Ortiz@uclm.es.

RESUMEN

Los delitos de daños informáticos cometidos a través de Internet presentan una característica que dificulta la determinación de la competencia judicial: se trata de delitos a distancia en donde los elementos constitutivos del delito (la concertación, la puesta en marcha, la ejecución, y la consumación) suelen tener lugar en fases temporalmente distintas y en espacios geográficos muy lejanos.

Más allá de la imposible adaptación legislativa al continuo desarrollo tecnológico, la jurisprudencia tampoco ayuda en esta labor. A nivel interno, la determinación de la competencia judicial se caracteriza por una enorme casuística que aplica diversos criterios (actividad, resultado o ubicuidad) en función del tipo delictivo, y con sus correspondientes excepciones, lo cual constituye un foco de inseguridad y un semillero de dilaciones indebidas. Y a nivel internacional, la atribución de la jurisdicción penal a los tribunales españoles también se enfrenta a la inexistencia de unas reglas claras de distribución de la competencia judicial internacional en materia penal.

A pesar de todo ello, este trabajo tiene por objetivo ofrecer soluciones y argumentos jurídicos a la hora de "territorializar" Internet de cara a determinar el órgano judicial competente para investigar y enjuiciar los delitos cometidos a través de la Red por ser el órgano que guarde el punto de conexión más estrecho con la conducta delictiva, lo cual, eso sí, resulta ser una tarea ciertamente compleja.

1. LA HETEROGENEIDAD DE LOS DELITOS DE DAÑOS INFORMÁTICOS

La expansión del uso de las tecnologías de la información y de Internet, en lo que podría calificarse como la digitalización de nuestras vidas, ha generado nuevas

modalidades delictivas que pueden quedar agrupadas bajo la expresión "ciberdelincuencia": un fenómeno delictivo en rápida propagación bajo el cual se englobarían todos aquellos delitos que pueden cometerse por medio de un equipo conectado a una red informática o contra un sistema conectado a la red. La ciberdelincuencia representa una *ulterior generación*[2] de la delincuencia vinculada a las TIC; una modalidad de "delincuencia informática" caracterizada por la utilización de Internet como entorno-medio en el que son atacados los propios sistemas informáticos o sus archivos y programas, o a través del cual se cometen múltiples actividades ilícitas. Por ello, el factor diferenciador de la ciberdelincuencia frente a la delincuencia informática radica, no ya en la utilización de sistemas informáticos, sino en el empleo de la Red y de las telecomunicaciones informáticas como elemento clave para la comisión delictiva[3]. Precisamente es la arquitectura de la Red la principal fuente de los distintos problemas jurídicos relacionados con la determinación del órgano jurisdiccional competente para conocer de tales delitos.

Antes de abordar tales cuestiones, es importante tener presente otro problema añadido: la diversa tipología y heterogeneidad de los delitos referidos a daños informáticos. Sin perjuicio de que los daños sobre sistemas y datos informáticos puedan ejecutarse de un modo "amanuense" (incendio, martillazos, etc.), en las diversas fuentes normativas podemos apreciar la abultada tipología de conductas subsumibles en el bloque de delitos referidos a daños informáticos.

Por ejemplo, el Convenio del Consejo de Europa sobre el Cibercrimen distingue cuatro grupos diferentes de infracciones: de ellos, el primer grupo "delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos" incluye múltiples conductas punibles, como el acceso ilícito a un sistema informático; la interceptación ilícita de datos informáticos comunicados en transmisiones no públicas; la interferencia sobre datos informáticos –actos que dañen, borren, deterioren, alteren o supriman datos informáticos- y sobre sistemas informáticos -la obstaculización grave, deliberada e ilegítima del funcionamiento de un sistema informático mediante la introducción, transmisión, provocación de daños, borrado, deterioro, alteración o supresión de datos informáticos-; así como el abuso de dispositivos informáticos –por ej., la producción, venta, obtención para su utilización, importación, difusión u otra forma de puesta a disposición de un dispositivo, incluido un programa informático, diseñado o adaptado principalmente para la comisión de cualquiera de los delitos previstos de conformidad con los artículos 2 a 5, o de una contraseña, un código de acceso o datos informáticos similares con los mismos fines-.

También en nuestro Código Penal existen múltiples conductas encuadrables como daños informáticos, pues aquél ha sido continuamente reformado para adaptarse a los compromisos supranacionales (con especial atención, véanse las reformas de las Leyes Orgánicas 5/2010 y 1/2015 para cumplir con lo dispuesto en la Decisión Marco 2005/222/JAI, de 24 de febrero de 2005, y en la Directiva 2013/40/UE, de 12 de agosto,

[2] ROMEO CASABONA, C. M., "De los delitos informáticos al cibercrimen: una aproximación conceptual y político-criminal", en AA VV.: *El cibercrimen. Nuevos retos jurídico-penales, nuevas respuestas politico-criminales*, ed. Comares, Granada, 2006, p. 8.

[3] Un concepto amplio de lo que debe entenderse por «ciberdelito» lo encontramos, por ejemplo, en el Décimo Congreso de las Naciones Unidas sobre Prevención del Delito y Tratamiento del Delincuente (Viena, 10 a 17 de abril de 2000), en donde se declara que "Por delito cibernético se entiende todo delito que puede cometerse por medio de un sistema o una red informáticos, en un sistema o una red informáticos o contra un sistema o una red informáticos".

relativa a los ataques contra los sistemas de información y la interceptación de datos electrónicos cuando no se trata de una comunicación personal). El tenor literal de los arts. 264, 264 bis, 264 ter y 264 quáter CP dan muestra de la diversa tipología de hechos delictivos incardinables en el bloque referido a los daños, lo que demuestra que el "daño" en el sabotaje informático se aleja de la tradicional noción de destrucción física permanente[4] y se orienta más bien a un concepto funcional de la propiedad más allá del concepto de indemnidad de la cosa. Los daños informáticos podrán producirse, entonces, no sólo por la destrucción de los datos –incluso temporal, pudiendo recuperarse si existe un *backup*-, sino también por actos que afecten a su interconexión lógica, su accesibilidad, su obstrucción, interrupción, inutilización, etc.

Y en la clasificación tripartita establecida en la *Instrucción del Fiscal General del Estado 2/2011 sobre el Fiscal de Sala de Criminalidad Informática y las Secciones de Criminalidad Informática de las Fiscalías*, también comprobamos como el bloque referido a "Delitos en los que el objeto de la actividad delictiva son los propios sistemas informáticos o las TICs" se encuentra constituido por las conductas punibles conforme a los delitos de daños, sabotaje informático y ataques de denegación de servicios previstos y penados en el art. 264 y concordantes del Código Penal; Delitos de acceso sin autorización a datos, programas o sistemas informáticos previstos y penados en el art. 197.3 CP; Delitos de descubrimiento y revelación de secretos del art. 197 CP cometidos a través de las TICs o cuyo objeto sean datos que se hallen registrados en ficheros o soportes informáticos electrónicos o telemáticos; Delitos de descubrimiento y revelación de secretos de empresa previstos y penados en el art. 278 CP cometidos a través de las TICs o cuyo objeto sean datos que se hallen registrados en ficheros o soportes informáticos ó electrónicos; y Delitos contra los servicios de radiodifusión e interactivos previstos y penados en el art. 286 CP[5]. Por supuesto, también las conductas subsumibles bajo la noción de *ciberterrorismo* constituirían un tipo de daño informático, aunque con una sustantividad propia por tratarse de ataques contra infraestructuras esenciales de la información.

2. PROBLEMAS PARA LA DETERMINACIÓN DE LA JURISDICCIÓN Y LA COMPETENCIA PENAL EN EL CIBERESPACIO

La famosa alusión a la "aldea global" de Marshall McLuhan resulta cada vez más frecuente para ilustrar los nuevos retos que plantea la utilización de Internet como medio de comisión delictiva, porque la ciberdelincuencia representa un claro ejemplo de las nefastas consecuencias derivadas de la comisión de un "delito de tipo transnacional", si por aquél entendemos el que i) se ha cometido en más de un país, ii) se ha cometido en un país, pero una parte considerable de su preparación, planificación, dirección o control ha tenido lugar en otro país, iii) se ha cometido en un país, pero con la intervención de un grupo delictivo organizado que esté implicado en actividades delictivas en más de un país, iv) se ha cometido en un país, pero tiene consecuencias importantes en otro país, o v) se ha cometido en un país y el autor del delito se encuentra en otro país o tiene la intención de viajar a otro país[6].

[4] VAN DEN EYNDE, A., "Análisis jurídico del sabotaje informático". Post publicado el 9 de marzo de 2015 en el blog http://eynde.es/es/analisis-juridico-sabotaje-informatico/.
[5] Téngase en cuenta las nuevas modalidades incorporadas tras la reforma del Código Penal en 2015.
[6] Dicho concepto se establece en el Acuerdo entre los Estados Unidos de América y la Unión Europea sobre la utilización y la transferencia de los registros de nombres de los pasajeros al Departamento de Seguridad del Territorio Nacional de los Estados Unidos. DOUE L 215, de 11 de agosto de 2012.

En caso de disparidad de criterios nacionales a la hora de determinar su jurisdicción para decidir perseguir la ciberdelincuencia, el resultado puede ser que el ciberespacio se convierta en un *reino de Taifas* similar al surgido en España en el siglo XI tras la desaparición del Califato de Córdoba. Frente a tal situación, una de las soluciones propuestas pasaría por convertir tales ciberdelitos en delitos contra la comunidad internacional, y por lo tanto, perseguibles de acuerdo con el principio de jurisdicción universal, pero no existen argumentos sólidos e internacionalmente consensuados acerca de incluir los ciberdelitos en el listado de los más graves crímenes contra la humanidad. Por ello, la alternativa consiste en la armonización penal y la cooperación judicial internacional para luchar contra esta nueva amenaza global, aunque no faltan voces que defiendan la unilateralidad a la hora de proteger los intereses nacionales frente a ciberataques provenientes del extranjero[7].

Calificables como «delitos a distancia», la fragmentación temporal y geográfica existente entre sus diferentes elementos constitutivos da lugar a importantes problemas jurídicos para determinar el tiempo y lugar de comisión del delito[8], sobre todo cuando la transnacionalidad de la conducta afecta a diversas jurisdicciones, en cuyo caso podemos ya anticipar que a nivel internacional no existe un sistema único de resolución de los conflictos positivos de jurisdicción y a nivel interno no existe un criterio homogéneo y claro de atribución de la competencia a los distintos órganos jurisdiccionales[9]. Esa fragmentación temporal resulta habitualmente apreciable en los delitos de daños informáticos, que suelen acometerse en distintas fases (tradicionalmente agrupadas en cinco: reconocimiento, escaneo, acceso, mantenimiento del acceso y borrado de huellas). Un ejemplo de tales etapas efectuadas a lo largo de distintos momentos -y lugares- nos lo muestra la Sentencia de la Audiencia Nacional de 11 de junio de 2015[10] ("operación mariposa"), en la que se explica cómo se lleva a cabo la creación de una red de *botnets* para efectuar un ataque informático: *«Existen varias etapas en el desarrollo de una botnet. En primer término, el creador de una botnet diseña la red que va a crear, definiendo los objetivos y los medios necesarios que va a emplear, incluyendo el sistema de control de la red. Además, necesitará un malware que se aloje en los equipos y permita el control del mismo, denominado bot. Este malware puede ser creado por él mismo (el creador de la red) o puede comprar este bot a un creador de malware. Finalmente, el delincuente debe distribuir el bot por cualquier método: correo basura, páginas con vulnerabilidades, ingeniería social, etc. El objetivo final es que las víctimas ejecuten el programa y se infecten. Si tiene éxito, el número de zombis puede llegar a crecer exponencialmente. Junto a ello, el creador de la red puede alquilarla a un tercero. A cambio de una cantidad pagada, el arrendatario tendrá a su disposición todas las posibilidades de la red de ordenadores zombis para realizar ciber-ataques. Los creadores sólo se preocupan de mantener una cantidad suficiente de sistemas infectados para que resulten atractivas y puedan alquilarla por una mayor cantidad de dinero»*.

[7] GOLDSMITH, J. L., "Cybercrime and Jurisdiction". Presentation at the *Conference on International Cooperation to Combat Cyber Crime and Terrorism,* Hoover Institution, Stanford University, Stanford, California, Dec. 6-7, 1999.

[8] GONZÁLEZ TAPIA, M. I., "El concepto de delito a distancia", en *VV.AA. El Código Penal de 1995, cinco años después,* ed. Servicio de Publicaciones de la Universidad de Córdoba, Córdoba, 2002, p. 101.

[9] Sobre esta cuestión, véase mi monografía *Problemas Procesales de la Ciberdelincuencia*, ed. COLEX, Madrid, 2013.

[10] Sentencia núm. 17/2015, de 11 de junio de la Audiencia Nacional (Sala de lo Penal, Sección 4ª).

Como veremos a continuación, si la acción llevada a cabo despliega sus efectos en otras jurisdicciones, y dicha conducta está tipificada tanto en el lugar donde se realiza la acción como en el lugar donde se producen las consecuencias de dicho acto, es muy probable que varios Estados reclamen para sí la competencia para enjuiciar tales actos, y es ahí donde la territorialidad del Derecho Penal y de las reglas de competencia dificultan una eficaz lucha contra el cibercrimen, sin que la simple aplicación de las reglas de lugar donde se produce el daño o donde se genera la voluntad delictiva, resuelvan estos problemas[11].

2.1. COMPETENCIA PENAL Y CIBERESPACIO

La paternidad del término "ciberespacio" es atribuida al escritor William Ford Gibson, para denominar el espacio virtual creado por las redes informáticas y para quien el ciberespacio es el "lugar" entre dos módems. Sin embargo, dicho término debe ser desmitificado a efectos jurisdiccionales, pues aun cuando se hable de delitos cometidos *en Internet* o *en el ciberespacio*, éste no es un lugar, sino un medio de comunicación. Es decir, no es un «dónde» sino un «a través de»; se trata de un vehículo o medio de comunicación a través del cual se prepara o concierta el delito, se ejecuta, o se propagan sus efectos, a la vez que sirve para el encubrimiento de sus autores, pero siempre relacionado con una conducta atribuible a un sujeto que podrá ser declarado penalmente responsable por unos tribunales, estos sí, geográficamente predeterminados. El problema, por tanto, reside en determinar si los delitos que se cometen a través de internet ("mundo virtual") deben someterse a las mismas reglas de determinación de la jurisdicción penal competente que los cometidos en el mundo "físico", lo cual no siempre acontece. Por citar un ejemplo concreto, el lugar de comisión del delito de allanamiento de morada será el lugar donde radique la vivienda, empresa, oficina o establecimiento. Y sin embargo, cuando lo invadido sea un sistema o dispositivo informático, el Tribunal Supremo opta por considerar el lugar de comisión del delito allí donde se encuentra el atacante y no donde se ubica el sistema invadido.

2.1.1. Competencia objetiva penal e internet

Al margen de aquellos hechos delictivos cometidos a través de Internet cuyo enjuiciamiento pudiera atribuirse a la Jurisdicción militar cuando concurran todos los requisitos para reputar que tales hechos se han cometido "en el ámbito estrictamente castrense" y de los supuestos en los que la competencia objetiva venga determinada por razón de las personas (bien porque se trate de personalidades aforadas a determinados órganos judiciales, bien porque se trate de menores penalmente responsables), las mayores dificultades en nuestro Ordenamiento para determinar el órgano judicial competente para el enjuiciamiento de delitos cometidos a través de Internet se plantean desde la perspectiva territorial.

La determinación de la competencia objetiva plantea pocas dificultades: básicamente, determinar, por razón de la materia, en qué supuestos el delito debe ser investigado por los Juzgados Centrales de Instrucción de la Audiencia Nacional, porque se trate de uno de los supuestos establecidos en el art. 65 LOPJ. Se ha llegado a plantear una reforma legal para centralizar la competencia para conocer de los ciberdelitos en órganos nacionales como la Audiencia Nacional o en órganos de capitalidad territorial

[11] CLIMENT BARBERÁ, J., "La justicia penal en Internet: territorialidad y competencias penales", en VV.AA., *Internet y derecho penal*, ed. CGPJ, Madrid, 2001, vol. X, p.657.

(Audiencias Provinciales de las capitales de las CC.AA.) al menos en los casos de delitos informáticos que puedan tener entidad estatal o territorial[12]. Por el momento, y en lo referido a daños informáticos, los supuestos de los que conocerá la Audiencia Nacional serán principalmente dos: a) los *delitos cometidos en el extranjero*, cuyo enjuiciamiento corresponda a los Tribunales españoles, en donde habrá que incluir también aquéllos cuya investigación se inició en el extranjero pero cuya continuación se atribuya a nuestros órganos judiciales en virtud de un Tratado internacional o Norma Comunitaria en dicho sentido. Y b) los delitos de daños informáticos calificables como *ciberterrorismo y actividades relacionadas con el terrorismo*, pues el terrorismo no es ajeno a la evolución de la Sociedad de la Información y al empleo de las nuevas tecnologías para la concertación, preparación, comisión, o difusión de toda clase de actividades terroristas. Es más, el art. 573.2 CP establece expresamente que *se considerarán igualmente delitos de terrorismo los delitos informáticos tipificados en los artículos 197 bis y 197 ter y 264 a 264 quater* –el apartado 4º del artículo 264 tipifica el ataque a infraestructuras críticas nacionales, de la Unión Europea o de un Estado Miembro de la Unión Europea- *cuando los hechos se cometan con alguna de las finalidades a las que se refiere el apartado anterior* (Subvertir el orden constitucional, etc.).

2.1.2. Competencia territorial penal e internet: múltiples criterios y casuística jurisprudencial

Para la determinación del *locus delicti commissi* a los efectos establecidos en los arts. 14.2 y 15 LECrim, el Tribunal Supremo ha ido aplicando las distintas teorías de la actividad, resultado y ubicuidad, en función del tipo delictivo, pero no siempre de un modo preciso y sin excepciones, lo cual ha originado una enorme casuística que no hace sino aumentar la inseguridad jurídica, pero sobre todo las dilaciones en la investigación y persecución de los hechos, a juzgar por las innumerables cuestiones de competencia que los juzgados de instrucción han planteado y siguen planteando cuando los delitos a investigar se estiman cometidos a través de Internet.

Así por ejemplo, con carácter general y cuando se trata de ilícitos en los que la conducta castigable es la difusión de determinadas ideas, informaciones, o contenidos ilícitos a través de Internet, el Tribunal Supremo ha utilizado con bastante asiduidad la «teoría de la actividad», y ha establecido como regla general que "En los delitos a distancia en que la actividad delictiva se desarrolla en un lugar y los efectos o resultados en otro distinto, el competente será el primero, ya que es la conducta o comportamiento castigados por la Ley y el lugar donde se realiza, el que debe contar para dilucidar la competencia[13]". Este criterio, aplicado generalmente a los ciberdelitos de injurias y calumnias o de difusión de pornografía infantil, significa que debe atribuirse la competencia al tribunal del lugar en que, en origen, *el sujeto pone en marcha a través del servidor, la concreta información facilitada, con independencia de que el efecto difamador persista en el tiempo y alcance a cualquier lugar, no sólo de España, sino del mundo*[14], aunque en algún caso se ha optado por aplicar el criterio de la ubicuidad, y

[12] FLORES PRADA, I., *Criminalidad informática. Aspectos sustantivos y procesales*, ed. Tirant lo blanch, Valencia, 2012, p. 329.

[13] Por todos, vid. ATS de 4 marzo 2009 (rec. 20356/2008).

[14] Sobre injurias y calumnias, vid. ATS de 19 de septiembre de 2001 (cuestión 19/2001). En el mismo sentido, vid. ATS de 19 de enero del 2004 (cuestión 89/2003); ATS de 23 de noviembre de 2004 (cuestión 85/2004) y ATS de 12 de marzo de 2009 (rec. 20590/2008). Sobre el criterio de la actividad a

atribuir la competencia al juzgado que primero conoció de la investigación, que generalmente coincide con el lugar del domicilio del ofendido y es donde se perciben las ofensas[15].

Aplicar el criterio de la actividad a los actos consistentes en la difusión de *malware* y demás modalidades de virus informáticos nos debería conducir a estimar competente el órgano judicial del lugar desde donde se difunde el virus o se inicia el ciberataque, y sin embargo, el Tribunal Supremo ha atendido en estos casos al criterio del resultado. Sin embargo, ello no ha sido así. El Tribunal Supremo ha declarado que para los delitos de accesos ilícitos a sistemas informáticos (mero acceso no autorizado, sin llegar a apoderarse, modificar, borrar, difundir o revelar los datos y programas informáticos), el *locus* sería el lugar desde donde se haya accedido ilegalmente a esos ficheros o equipos[16]; cuando junto con el acceso inconsentido se produce una "sustracción" de información que da lugar a la condena por descubrimiento y revelación de secretos de empresa, el Tribunal Supremo ha designado como *locus* el lugar "donde radican los datos supuestamente sustraídos[17]"; y cuando la conducta tiene como resultado el ataque a páginas web, o cualquiera otra de las conductas que podrían quedar integradas en el delito de daños informáticos, el Tribunal Supremo ha optado por la teoría del resultado, de modo que *"el delito no se comete desde donde se lanza el ataque sino donde se producen los daños, se destruye el sistema operativo o se contaminan los archivos, cuya forma de operar refleja unos altos conocimientos informáticos de donde se deriva que nos encontramos ante una acción conjunta realizada por expertos hackers y de común acuerdo, y un ataque planificado y organizado desde diferentes IP a múltiples páginas web*[18]".

---

los delitos de difusión de pornografía infantil, en donde el criterio es *el lugar desde donde se hayan subido a la Red los contenidos presuntamente delictivos*, vid. AATS de 23 de noviembre de 2004 (cuestión 85/2004), 4 de marzo de 2009 (rec. 20534/2008); 6 de mayo de 2009 (rec. 20059/20091); de octubre de 2009 (rec. 20299/2009); 14 de octubre de 2009 (rec. 20338/2009); 15 de enero de 2010 (rec. 20349/2009); 19 de febrero de 2010 (rec. 20455/2009); 14 de enero de 2011 (rec. 20628/2010); y 17 de marzo de 2011 (rec. 20766/2010).

[15] Vid. ATS de 11 de enero de 2008 (rec. 20386/2007): Esta Sala ha venido pronunciándose reiteradamente en relación con la consumación del delito de injurias y se había mantenido que se consumaba en el lugar de la emisión de las ofensas y no donde las percibe el ofendido, más tras el acuerdo del Pleno no jurisdiccional de 3 de febrero de 2005, en el que se adopta el principio de ubicuidad "el delito se comete en todas las jurisdicciones en las que se haya realizado algún elemento del tipo, en consecuencia, el juez de cualquiera de ellas que primero haya iniciado las actuaciones procesales, será en principio competente para la instrucción de la causa" (ver auto de 4/11/05, entre otros) este criterio es el que se debe aplicar para resolver esta cuestión de competencia y así habiéndose iniciado las actuaciones en Valencia, lugar del domicilio del ofendido y lugar donde percibe las ofensas el mismo, es el Juzgado de Valencia núm. 7 el competente. También el ATS de 29 mayo 2008 (rec. 20695/2007), en un caso de injurias recibidas a través de correo electrónico, entiende aplicable el principio de ubicuidad, según el cual es competente tanto el juzgador de donde se emite como el de donde se recibe, y resuelve a favor de la competencia del que primero inició las actuaciones.

[16] Vid. AATS de 19 de mayo de 2011 (rec. 20003/2011), 22 de septiembre de 2011 (rec. 20291/2011) y de 4 de febrero de 2016 (rec. 20766/2015), en donde se opta por "el lugar desde el que se accede ilegalmente a ficheros ajenos".

[17] Vid. ATS de 4 de octubre de 2000 (cuestión 1960/2000), en donde en caso de delito de descubrimiento y revelación de secretos de empresa, el TS advierte que el lugar desde el que se accede a la información es distinto al de la existencia de los datos sustraídos, y estima aplicable la teoría del resultado, declarando competente al órgano judicial del lugar donde radican los datos supuestamente sustraídos

[18] ATS de 5 de octubre de 2011 (rec. 20137/2011).

En la citada SAN de 11 de junio de 2015, sobre uso de una red de *botnets* para efectuar un ataque informático, el factor clave no fue el lugar donde se produjeron los daños (que en aquella ocasión se estimó en una infección masiva de ordenadores para efectuar ataques a páginas web en España, Estados Unidos y Canadá), sino el lugar en que se encontraba el responsable de la *botnet*. Esta sentencia es reflejo de la opción jurisprudencial, en los casos de que exista una multiplicidad de lugares en donde pueden producirse los daños en los sistemas y dispositivos informáticos, de acudir como solución al "lugar de operaciones" o "sede de la empresa". Como ejemplos, en determinadas estafas informáticas se ha atribuido la competencia al juzgado del lugar de la sede social de la empresa responsable de los hechos y no de la empresa o usuario perjudicado[19]. Y en determinados delitos contra la propiedad industrial e intelectual cometidos a través de una página web, el Tribunal Supremo ha concretado como lugar de comisión del delito aquél en donde se diseña o confecciona la página web y se sube a la red, o incluso el lugar desde donde se administra dicha página web –entendiendo por dicho lugar también aquél donde tiene su sede la empresa que gestiona dicha página web-, con independencia del lugar en donde se aloje la misma o donde tengan su sede las empresas perjudicadas cuyos derechos pudieran haberse visto afectados por estos hechos[20].

2.1.3. Ciberdelincuencia y teoría de la ubicuidad: solución interna y provisional

Como puede apreciarse, la jurisprudencia del Tribunal Supremo sobre el lugar de perpetración del ciberdelito resulta excesivamente casuística. No existe uniformidad en el criterio a aplicar cuando se trata de delitos cometidos a través de la Red, pues a pesar de que para los delitos de difusión se aplica mayoritariamente la teoría de la actividad, y para los delitos patrimoniales y de daños se aplica preferentemente la teoría del resultado, lo cierto es que existen ejemplos de delitos de actividad (amenazas) en los que se opta por la teoría del resultado, y abundan también las resoluciones del Tribunal Supremo en las que entiende aplicable la teoría de la ubicuidad y decide atribuir la competencia al órgano jurisdiccional que primero hubiera iniciado actuaciones judiciales por tales hechos.

Esta opción de aplicar la teoría de la ubicuidad con carácter general a la investigación de los delitos cometidos a través de Internet se consolidó con el Pleno no jurisdiccional de la Sala Segunda del Tribunal Supremo de 3 de febrero de 2005, y a partir de ahí ha sido frecuentemente aplicada, tanto a delitos de actividad (difusión de pornografía infantil en Internet[21]), como a delitos de resultado (estafas informáticas), sobre todo, en aquellos supuestos en los que la conducta delictiva presenta elementos en múltiples lugares y ha motivado la apertura de diligencias judiciales en todos ellos[22], y

[19] Vid. ATS de 2 de marzo de 2016 (rec. 20908/2015).

[20] ATS de 18 abril 2002 (cuestión 77/2001; y ATS de 22 de julio de 2002 (cuestión 76/2001). El ATS de 18 de enero de 2008 (rec. 20411/2007) considera el lugar de administración de la página web como "el centro de las actividades criminales". En el ATS de 6 de abril de 2016 (rec. 20063/2016) se afirma que en los delitos del art. 273 CP que castiga al que, con fines industriales o comerciales, fabrica, importa, posea, utilice, ofrezca o introduzca en el comercio objetos amparados por una patente, hay que estar al lugar del domicilio social de la empresa que comercialice a través de su página web los productos protegidos bajo patente.

[21] Vid. AATS de 13 de julio de 2006 (rec. 20117/2006); 9 de julio de 2007 (rec. 20186/2007); o 19 de septiembre de 2007 (rec. 20095/2007).

[22] Entre otros, vid. AATS de 11 de enero de 2008 (rec. 20386/07); 29 de mayo de 2008 (rec. 20695/07); 21 de abril de 2009 (rec. 20011/09); y 6 de octubre de 2011 (rec. 20023/2011).

en aquellas defraudaciones en las que existen víctimas repartidas por toda la geografía nacional debido a que las estafas se han cometido de forma continuada a través de portales de venta online[23], aunque con una marcada excepción: que el juzgado que primero conoció del caso sea únicamente el del lugar donde se presentó la primera denuncia pero en cuya circunscripción no se cometió ninguno de los hechos integrantes del tipo delictivo, en cuyo caso habrá que atribuir la competencia al del lugar de la infracción[24].

2.2. JURISDICCIÓN PENAL Y CIBERESPACIO

2.2.1. Ventajas e inconvenientes de las reglas de determinación de la competencia territorial

Acudir a la teoría de la actividad para atribuir la jurisdicción a los tribunales españoles presenta como ventaja la mayor facilidad de los tribunales para recabar las pruebas y aprehender al autor de los hechos, a lo que cabe sumar que al tratarse del lugar donde se encuentra el denunciado, "por razones procesales directamente relacionadas tanto con el derecho de defensa como con la facilitación de la realización de las diligencias sumariales, es precisamente el domicilio del denunciado donde las facilidades son mayores[25]". Pero igualmente plantearía importantes perjuicios, pues quedarían fuera de enjuiciamiento todas aquellas actividades delictivas desplegadas desde fuera de nuestras fronteras y que, a pesar de atentar contra ciudadanos o intereses españoles, no afectaran a bienes jurídicos cuya defensa amparan otros principios (real, de personalidad o universal), por lo que no resultarían perseguibles en España[26].

La utilización de la teoría del resultado simplifica igualmente la determinación del lugar de comisión del ciberdelito cuando éste produce sus efectos en otra lugar distinto al lugar desde donde actúa el acusado, y suele ser el lugar más cercano a la víctima, lo cual, a su vez, le permitirá con mayor facilidad personarse en el proceso y reclamar la oportuna condena penal junto con la reparación del daño. Sin embargo, esta teoría tampoco es la más adecuada para el enjuiciamiento de todos los ciberdelitos "de resultado", sobre todo de aquéllos que se caracterizan por poder desplegar sus efectos (v. gr., los daños informáticos) en múltiples lugares. En el plano interno, esa multiplicidad de lugares donde se ha producido el hecho dañoso puede ser superada, bien con la atribución del caso a un órgano centralizado (v. gr., la Audiencia Nacional), bien optando por la preferencia temporal (el juzgado que primero conoció de los hechos). Pero en el plano internacional significaría que habría potencialmente tantos países competentes como lugares en los que el delito provocó daños.

---

[23] Vid. AATS de 4 de mayo de 2009 (rec. 20045/2009); 15 de enero de 2010 (rec. 20580/2009); 18 de noviembre de 2010 (rec. 20508/2010); 4 de mayo de 2011 (rec. 20733/2010); 12 de mayo de 2011 (rec. 20013/2011); y 6 de julio de 2011 (rec. 20238/2011).

[24] Por todos, vid. AATS de 13 de enero de 2011 (rec. 20547/2010) y de 26 de octubre de 2011 (rec. 20358/2011). Esta excepción también ha sido aplicada a los delitos de difusión de pornografía infantil en el ATS de 13 julio de 2011 (rec. 20110/2011), en el que se afirma que "la actividad ilícita partió de diversas ciudades, desde donde operaban distintos participes a los que les fueron intervenidos los respectivos ordenadores, sin que en la ciudad de Valencia se haya cometido actividad ilícita alguna, ya que se limitó a incoar las diligencias Previas iniciales a partir de un oficio de la Brigada de Investigación tecnológica".

[25] ATS de 31 de mayo de 2000 (cuestión 4620/1999).

[26] MARCHENA GÓMEZ, M., "Dimensión jurídico penal del correo electrónico", *Diario La Ley*, 4 de mayo de 2006, p. 12.

En tercer lugar, optar por el empleo de la teoría de la ubicuidad significa utilizar el criterio de la prioridad temporal en el inicio de la investigación como *forum praeventionis* a los solos efectos de la instrucción, y como "principio de facilitación de la investigación" para evitar dilaciones, tal y como expresamente se declara en el ATS de 10 de febrero de 2006, según el cual *Este criterio, doctrinalmente conocido por el de la ubicuidad y de uso en múltiples países de nuestro entorno, es respetuoso con el tenor literal del precepto indicado, puesto que se atiene al dato de la realización de actos concretos de ejecución del posible delito en un determinado espacio físico, con lo que evita la arbitrariedad interesada en la fijación de la competencia. Y, muy en particular, impide que se produzcan situaciones de conflicto como la planteada en este caso, en la que la negativa a conocer de algún juez, que podría ser competente para ello determina dilaciones difíciles de justificar, y que aparte el perjuicio que, ya solo por esto, deparan a los afectados, podrían constituirse en obstáculo para la eficacia de la posible investigación*[27]. Por ello, se ha acudido a la aplicación de esta teoría, bien por defecto (esto es, cuando no existen elementos que indiquen dónde se ha iniciado la acción o si ésta procede desde el extranjero[28]), o bien porque el resultado pudiera entenderse producido en múltiples lugares y pretenden evitarse dilaciones en la investigación de los hechos (sobre todo, cuando hay múltiples víctimas repartidas geográficamente pero no resulta competente la Audiencia Nacional porque, a pesar de que el perjuicio afecte a una "generalidad" de personas, se rechaza que exista una trascendencia económica relevante, o una complejidad importante en la instrucción de la causa).

La aplicación de la teoría de la ubicuidad a los delitos cometidos a través de Internet facilita extraordinariamente la continuación de la investigación de los mismos y cuando alguno de los lugares coincide con el domicilio de la víctima, la aplicación de este criterio permitirá que los derechos de aquélla puedan ser mejor atendidos[29], pero no representa la solución definitiva, y menos aún para la persecución de los delitos de ámbito transnacional[30], pues no hay que olvidar dos aspectos esenciales:

a) De una parte, constituye una *regla interina* a los efectos de determinar la competencia instructora cuando inicialmente se desconoce el concreto lugar de comisión del delito, ya que las decisiones sobre competencia territorial en materia penal, cuando se suscitan en la fase instructora, ostentan un mero cariz provisional y por tanto sin perjuicio de lo que se resuelva en estadios posteriores de la tramitación[31]. Tal y como ha afirmado nuestro Tribunal Supremo, "las cuestiones de competencia ofrecen siempre una nota de provisionalidad, lo que implica que en un determinado momento del *iter* procesal e incluso de la propia investigación puede determinarse un cambio

[27] ATS de 10 de febrero de 2006 (rec. 138/2005).

[28] Vid. el ATS de 25 de abril de 2005 (cuestión 11/2005), relativo a un uso fraudulento de tarjetas a través de internet: al no conocerse el lugar de realización material, es competente el del lugar de descubrimiento de las pruebas materiales por ser el lugar correspondiente al denunciante y el que primero incoó diligencias.

[29] AATS de 22 de septiembre de 2005 (cuestión 27/2005) y 20 de julio de 2011 (rec. 20278/2011).

[30] En la Memoria FGE correspondiente al año 2008 (pág. 960) se afirma que dicho criterio constituye una "Solución adecuada para el supuesto de que el hecho sea competencia de un solo Estado, pero cuando la conducta delictiva se realiza en varios países, el resultado se produce en otro u otros, y su descubrimiento a través de investigaciones realizadas en otro distinto, se pueden producir situaciones de impunidad si en algunos de esos países no está perseguida penalmente la conducta investigada, situación muy común en los denominados «paraísos informáticos», los cuales son utilizados habitualmente en esta forma de criminalidad".

[31] ATS de 12 de marzo de 1992 (rec. 1340/1991).

procedimental que afecta incluso al ámbito de la pura competencia territorial, ya decidida entre dos órganos jurisdiccionales contendientes, en atención a concretas circunstancias y que después bajo otros presupuestos fácticos presenta diferentes conclusiones jurídicas[32]".

b) Y de otra parte, porque es una *regla interna*. El hecho de que el citado Acuerdo del Tribunal Supremo de 3 de febrero de 2005 utilice la expresión «todas las jurisdicciones» no debe entenderse referida a diversas jurisdicciones estatales, sino a diversos partidos judiciales dentro de España. Y aunque es cierto que se ha propuesto como una solución amplia y comprensiva de ambos tipos de problemas (jurisdicción y competencia[33]), no puede ser extrapolada a la determinación de la jurisdicción a nivel internacional porque aplicar dicha teoría en el plano internacional no sólo no solventa, sino al contrario, favorecería la aparición de conflictos de Jurisdicción cuando el delito afecte a varios países, pues tanto el Estado donde se lleve a cabo la actividad delictiva como el Estado o los Estados donde se produzcan los resultados de dicha conducta podrían considerarse competentes para investigar el delito. Por ello debe rechazarse el uso de «interpretaciones expansionistas[34]» del criterio de la ubicuidad. Y además, en dicho plano internacional no parece que la determinación de la Jurisdicción más apropiada para la investigación y enjuiciamiento de los delitos cometidos a través de la Red deba resolverse en virtud de cuál de los Estados concurrentes ha comenzado a investigar los hechos en primer lugar. Se hace preciso acudir a otros criterios más significativos[35] que evidencien un *vínculo de conexión real y apropiado*, basado en aspectos constatables y predecibles, entre el Estado que reclama para sí el enjuiciamiento del ciberdelito y los hechos en cuestión.

En el plano internacional hay que estar a los criterios de atribución de la Jurisdicción penal consensuados entre los Estados en los instrumentos internacionales, y ahí es donde reside el primer y principal problema: La ausencia de unas reglas claras de distribución de la competencia judicial internacional en materia penal, ni a nivel internacional ni a nivel europeo, lo cual dificulta la tarea de conocer, *a priori*, en qué jurisdicción se enjuiciarán determinados delitos cometidos a través de Internet, lo que tiene importante repercusiones negativas.

---

[32] ATS de 21 de enero de 1998 (cuestión 3550/1997).

[33] Para MARCHENA GÓMEZ ("Dimensión jurídico penal…", op. cit., p. 11), "tanto en los casos en los que el marco territorial del delito se circunscribe al ámbito jurisdicción español, como en aquellos otros en los que pueden converger los límites jurisdiccionales de distintos Estados, la solución propugnada permite optar por el doble criterio de lugar de ejecución y lugar del resultado. La teoría de la ubicuidad, por ej., permitirá entender que la inoculación de un potente virus destructivo llevada a cabo desde fuera de España por un extranjero, pero que expande sus efectos en sistemas informáticos radicados en territorio español, puede ser perseguida en nuestro país en la medida en que el delito, atendiendo al resultado, también puede reputarse cometido en España".

[34] SÁNCHEZ GARCÍA, I. y BLANCO CORDERO, I., "Problemas de derecho penal internacional en la persecución de delitos cometidos a través de internet", Actualidad penal 2002-1, p. 191. En el plano internacional, véase el Estudio *Extraterritorial criminal jurisdiction*, elaborado por el Comité Europeo de Problemas Penales, Consejo de Europa, 1990.

[35] CABEDO VILLAMÓN, F. y otros ("Criterios de los órganos judiciales y el ministerio fiscal, en la investigación y enjuiciamiento de los fraudes por Internet", en VV.AA. *Fraude Electrónico: Entidades Financieras y Usuarios de Banca. Problemas y Soluciones*, ed. Aranzadi, Navarra, 2011, p. 125) sostienen que utilizar el criterio de la ubicuidad y atribuir la competencia al órgano judicial que lleve más avanzada la investigación "parece una solución extremadamente práctica y poco jurídica".

En primer lugar, porque la determinación de la jurisdicción competente para el enjuiciamiento de tales hechos delictivos es condición *sine qua non* para la determinación del Derecho Penal aplicable, por lo que la incertidumbre sobre la determinación de la jurisdicción competente redundará también en inseguridad o imprevisibilidad de las consecuencias penales de la conducta, lo que puede servir de artimaña para decidir delinquir, a modo de *forum shopping*, en aquel Estado que disponga de una legislación penal más benigna o incluso con determinadas conductas destipificadas como ilícitos penales, reglas sobre exclusión probatoria, medidas cautelares menos gravosas para su situación personal o patrimonial, una aplicación amplia del principio de oportunidad en el ejercicio de la acción penal, etc.[36].

En segundo lugar, porque la gran heterogeneidad de las conductas delictivas que pueden llevarse a cabo a través de Internet, y en su caso, la distinta tipificación que pudieran recibir unos mismos hechos (por ejemplo, "sabotaje informático" en unas legislaciones y "ciberterrorismo" en otras) también constituye un obstáculo a la hora de aplicar la misma regla de determinación de la Jurisdicción. Para evitar la impunidad de determinados ataques informáticos, resulta incluso positivo que los Estados aboguen por el establecimiento de criterios de determinación de la jurisdicción de carácter extensivo, pero una inadecuada resolución de tales conflictos puede provocar una merma en la cooperación judicial internacional futura de los Estados entre sí, pues generará reservas de los países a ceder ante otros en supuestos futuros a la hora de cooperar en la persecución y enjuiciamiento de los ciberdelitos. Por ejemplo, si el principal elemento utilizado por los Estados a la hora de procesar a un sujeto por la difusión de un malware que ha causado daños en diversas jurisdicciones lo constituye el haber sido el primero en aprehender físicamente al acusado (*forum aprehensionis*), ello podría dar pie a la generalización del principio *male captus, bene detentur* como una práctica aceptable como mal menor por parte de la comunidad internacional en aquellos supuestos en los que se trate de crímenes de carácter transnacional con intereses nacionales en juego. Como ya se puso de manifiesto en el *Libro Verde de 2005 de la Comisión Europea sobre los conflictos de jurisdicción y el principio non bis in idem en los procedimientos penales*[37], dicho principio no evita los conflictos de jurisdicción derivados de la existencia de múltiples procesamientos en curso en dos o más Estados miembros, y sin un sistema que atribuya los asuntos a la jurisdicción adecuada en el curso del procedimiento, el principio *non bis in idem* puede producir resultados imprevistos e incluso arbitrarios: al dar preferencia al primer órgano jurisdiccional que pueda dictar una resolución definitiva, produce un efecto similar al "principio de orden de llegada".

El problema se acrecienta al comprobar que la existencia de una investigación penal iniciada en un Estado contra una persona es, por regla general, causa de denegación de la entrega de dicho sujeto a otro Estado que lo reclama para su enjuiciamiento o para el cumplimiento de una condena impuesta por esos mismos hechos[38]. Por lo tanto, si dos Estados se consideran competentes para el enjuiciamiento

[36] ORMAZÁBAL SÁNCHEZ, G., "Proceso penal con implicaciones extranjeras y principio de legalidad en el ámbito de la Unión Europea", en VV.AA., *La Justicia y la Carta de Derechos Fundamentales de la Unión Europea*, ed. Colex, Madrid, 2008, p. 135.

[37] COM(2005) 696 final, pág. 3.

[38] En el plano internacional, vid. el art. 8 del Convenio europeo de extradición de 1957, así como el art. 3 de la Ley 4/1985, de 21 de Marzo, de Extradición Pasiva. Y en el ámbito comunitario, vid. el art. 4.2 de la Decisión Marco 2002/584/JAI del Consejo, de 13 de junio de 2002, relativa a la orden de detención europea y a los procedimientos de entrega entre Estados miembros; o la propia Ley 23/2014, de 20 de noviembre, de reconocimiento mutuo de resoluciones penales en la Unión Europea, cuyo art. 48.2.a)

de unos daños informáticos, las reglas previstas para la extradición y entrega del acusado no solventan el conflicto. Y la aplicación de la regla *ne bis in idem* se sitúa a la cola de los mecanismos dirigidos a prevenir o resolver conflictos positivos de jurisdicción[39], pues si bien impide la doble sanción penal en los casos en que se aprecie la identidad del sujeto, hecho y fundamento, no impide una múltiple persecución penal de un mismo sujeto en varios Estados diferentes. La vertiente procesal del principio *ne bis in idem* incluye la interdicción de un doble proceso penal con el mismo objeto, pero para ello es preciso que el primer proceso haya concluido con una resolución con efectos de cosa juzgada[40].

Para dotar de eficacia internacional a la regla *ne bis in idem*, en el sentido de que ésta no sólo se aplicaría en su efecto negativo o excluyente, sino también en la proscripción de la litispendencia, esto es, de la simultaneidad de dos o más procesos frente a una misma persona, por los mismos hechos[41], hubiera sido de gran utilidad para los tribunales españoles contar con la regla sobre suspensión del proceso por razón de litispendencia internacional contenida en el art. 93 de la Propuesta de Código Procesal Penal de 2013, que facultaba al Fiscal director de la investigación acordar la suspensión del proceso en interés de la justicia, cuando le constase la tramitación de un proceso contra el encausado ante un Tribunal internacional o ante un Tribunal extranjero en el que pudiera dictarse sentencia que despliegue efecto de cosa juzgada en España, hasta que finalizase dicho proceso seguido en el extranjero, si bien no hay que perder de vista que se trataría de una regla facultativa para el órgano instructor.

2.3. INSTRUMENTOS INTERNACIONALES PARA RESOLVER LOS CONFLICTOS DE JURISDICCIÓN PENAL EN EL CIBERESPACIO

Uno de los instrumentos más importantes para combatir eficazmente cualquier tipo de delincuencia trasnacional lo representa la cooperación internacional, pues sin ella resultará casi inocua cualquier iniciativa doméstica de los Estados para atajar y perseguir adecuadamente aquellas conductas que exceden de sus fronteras nacionales. En el caso de la ciberdelincuencia, las iniciativas más destacables a nivel internacional en materia de lucha contra los ciberdelitos se han centrado, de una parte, en una mayor armonización internacional de lo que debe considerarse ilícito, y de otra parte, en promover la cooperación judicial y policial entre las autoridades estatales para facilitar la obtención y transmisión de pruebas a través de múltiples "redes de contacto". Sin embargo, los esfuerzos internacionales no han sido tan deslumbrantes a la hora de atajar la posible concurrencia de jurisdicciones en la persecución y enjuiciamiento de la ciberdelincuencia.

2.3.1. El Convenio del Consejo de Europa sobre el Cibercrimen de 2001

---

establece como causa facultativa de denegación "Cuando la persona que fuere objeto de la orden europea de detención y entrega esté sometida a un procedimiento penal en España por el mismo hecho que haya motivado la orden europea de detención y entrega".

[39] Vid. RAFARACI, T., "Ne bis in idem y conflictos de jurisdicción en materia penal en el espacio de libertad, seguridad y justicia de la Unión Europea", en VV.AA., *Espacio Europeo de Libertad, Seguridad y Justicia: Últimos avances en cooperación judicial penal,* ed. Lex Nova, Valladolid, 2010, p. 140.

[40] Entre otras, vid. SSTC 159/1987, 222/1997, 2/2003 y 60/2008.

[41] A favor de esta tesis, vid. DE LA OLIVA, A., "La regla *non bis in idem* en el Derecho Procesal Penal de la Unión Europea: algunas cuestiones y respuestas, en VV.AA., *El Derecho Procesal Penal en la Unión Europea*, ed. Colex, Madrid, 2006, p. 185.

Se trata del principal instrumento internacional disponible actualmente en materia de cooperación internacional en la lucha contra la delincuencia informática, aunque no fue hasta finales de 2010 cuando fue ratificado por España[42]. Sin embargo, dicho instrumento internacional no solventa los posibles conflictos internacionales de jurisdicción para perseguir y enjuiciar un delito de daños informáticos que afecte a diversas jurisdicciones. El art. 22 del Convenio utiliza como criterios de atribución de competencia tanto el principio de territorialidad ("cuando la infracción se haya cometido en su territorio, a bordo de una nave que ondee pabellón de ese Estado, o a bordo de una aeronave inmatriculada en ese Estado"), como el principio de personalidad activa ("cuando la infracción se haya cometido por uno de sus súbditos, si la infracción es punible penalmente en el lugar donde se ha cometido o si la infracción no pertenece a la competencia territorial de ningún Estado"). Y, como es habitual, otorga preferencia al principio de territorialidad, pero no establece ninguna indicación de cuándo se entiende que un ciberdelito se comete *en el territorio* de un Estado parte (i. e., en un ciberataque, ¿hay que atender al lugar de la actividad –creación y/o difusión del comando dañino- o lugar del resultado -daños-?).

A la hora de resolver los posibles conflictos de Jurisdicción que puedan producirse entre los Estados parte, el apartado 5º del citado art. 22 se limita a advertir que *"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"*. Es decir, no establece un mecanismo preciso de resolución de eventuales conflictos de jurisdicción, ni con carácter preferente ni subsidiario[43], más allá de la simple previsión de realización de "consultas" entre los Estados parte y sólo cuando "sea oportuno", algo por otra parte habitual en la mayoría de los Convenios aprobados por las Naciones Unidas (v. gr., lo dispuesto en el art. 15 del Convenio de 2000 contra la delincuencia organizada transnacional, o en el art. 42 del Convenio de 2003 contra la corrupción); por el Consejo de Europa (v. gr., el art. 31 del Convenio sobre la lucha contra la trata de seres humanos firmado en Varsovia en 2005, el art. 14 del Convenio sobre la prevención del terrorismo, también firmado en Varsovia en 2005, o el art. 25 del Convenio sobre la protección de los niños en contra de la explotación y el abuso sexual, firmado en Lanzarote en 2007), así como en otros tratados internacionales, cuyo modelo lo ejemplifica el Convenio Europeo de 15 de mayo de 1972 sobre la transmisión de procedimientos en materia penal[44], cuyos arts. 31 y 32 establecen que "los Estados interesados *se esforzarán* (sic) en todo lo posible por determinar, después de proceder a una evaluación en cada caso concreto […], a cuál de esos Estados corresponderá proseguir el procedimiento instruido. Durante la tramitación

[42] En vigor desde el 1 de octubre de 2010. Véase el Instrumento de Ratificación del Convenio (BOE de 17 de septiembre de 2010). A primeros del año 2012, más de cuarenta países han firmado dicho Convenio y más de una treintena lo han ratificado. El listado de dichas ratificaciones puede consultarse en: http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=185&CM=8&DF=14/02/2012&CL=ENG.

[43] Entre otros, vid. HOPKINS, S., "Cybercrime Convention: A Positive Beginning to a Long Road Ahead", *Journal of High Technology Law*, 2003, p. 118; PODGOR, E., "Cybercrime: nacional, Transnacional or internacional?, *The Wayne Law Review*, vol. 50, 2004, p. 107; BRENNER, S. W. / KOOPS, B. J., "Approaches to Cybercrime Jurisdiction", *Journal of High Technology Law*, vol. 1, nº1, 2004, p. 42; KASPERSEN, H. K., "Cybercrime and Internet Jurisdiction", Discussion paper (draft) de 5 de marzo de 2009, pág. 20 (disponible en: www.coe.int/cybercrime).

[44] Ratificado por España el 24 de junio de 1988 (BOE núm. 138/1985, de 10 de junio de 1985).

de las consultas, los Estados interesados aplazarán la sentencia en cuanto al fondo de la causa".

2.3.2. La Decisión Marco 2009/948/JAI sobre la prevención y resolución de conflictos de jurisdicción penal

Con el fin de resolver la concurrencia de jurisdicciones penales nacionales en la Unión Europea sobre unos mismos hechos, se han presentado iniciativas muy interesantes, como el *Corpus Juris* de 1995 y la idea de instaurar un "principio de territorialidad europea", la Iniciativa griega de una *Decisión marco del Consejo relativa a la aplicación del principio ne bis in idem*[45], la *Propuesta de Friburgo sobre concurrencia de jurisdicciones* de 2003[46], o el *Libro Verde sobre los conflictos de jurisdicción y el principio non bis in idem en los procedimientos penales* de 2005[47]. Sin embargo, ninguna de las iniciativas contiene una solución adecuada a la determinación de la jurisdicción competente para el enjuiciamiento de los delitos cometidos a través de Internet.

A pesar de tales antecedentes en los que incluso se llegaba a apostar por una solución precisa (i. e., el TJCE como órgano encargado de resolver la jurisdicción penal competente en el supuesto de concurrencia de jurisdicciones), la Unión Europea no dispone aún de una normativa que contenga criterios claros de distribución de la competencia judicial penal entre los Estados miembros, ni con carácter particular para el enjuiciamiento de los ciberdelitos, ni siquiera con carácter general en materia penal, de modo que a efectos jurisdiccionales, no es posible hablar de un verdadero *territorio judicial europeo*, aunque hay quien aprecia un movimiento imparable en pro de la consecución del mismo[48]. Sus múltiples iniciativas, propuestas, planes de acción, reformas de disposiciones sectoriales, etc., no han conseguido resolver de manera clara el problema de la determinación de la jurisdicción penal competente en el Espacio Judicial Europeo, pues no existe un texto jurídico que disponga criterios firmes, precisos, y sobre todo, jerárquicamente distribuidos, para precisar qué Estado miembro será competente para juzgar un delito cometido a través de Internet.

Lo peor de todo es que la normativa comunitaria aprobada para tal fin (La Decisión Marco de 30 de noviembre de 2009 sobre la prevención y resolución de conflictos de ejercicio de jurisdicción en los procesos penales[49]) no contiene unos fueros precisos de distribución de la Jurisdicción entre los Estados miembros, sino fórmulas de

[45] DOUE C 100, de 26 de abril de 2003, p. 24.

[46] *Freiburg Proposal on Concurrent Jurisdictions and the Prohibition of Multiple Prosecutions in the European Union*, Max Planck Institute for Foreign and International Criminal Law, Freiburg i.Br., November 2003, publicada en *Revue Internationale de Droit Pénal*, 2004, vol. 73, p. 1195.

[47] COM(2005) 696 final. No obstante, la posibilidad de encomendar a un órgano de la UE la facultad de decidir sobre la jurisdicción competente se consideraba "muy difícil de realizar en el marco del actual Tratado. En primer lugar, habría que crear un nuevo órgano, ya que los papeles de mediador y de instancia que adopta decisiones obligatorias, no parecen compatibles. En segundo lugar, se plantearían cuestiones complejas sobre el control judicial de una decisión adoptada a nivel de la UE".

[48] QUINTERO OLIVARES, G., "La unificación de la Justicia Penal en Europa", *Revista penal*, nº3, 1999, p. 59. Por su parte, PRADEL ("Vías para la creación de un espacio judicial europeo único", *Revista penal*, nº3, 1999, p. 42) defiende la existencia de dos espacios judiciales penales europeos: el del Consejo de Europa y el de la Unión Europea.

[49] Decisión Marco 2009/948/JAI del Consejo, de 30 de noviembre de 2009, sobre la prevención y resolución de conflictos de ejercicio de jurisdicción en los procesos penales (DOUE L 328 de 15.12.2009, p. 42/47).

resolución meramente informales[50]. Con razón ha sido calificada por la Fiscalía General del Estado en su Memoria del año 2010 como «decepcionante» por su escasa profundidad, *toda vez que no llega a establecer mecanismo alguno que permita en la práctica eludir los problemas derivados de la concurrencia de jurisdicciones, limitándose a proponer fórmulas de consenso o acuerdo entre las autoridades implicadas*[51]. En efecto, dicha Decisión Marco propone consultas entre los Estados en orden a lograr un consenso, y en último término, la encomienda a Eurojust para que se pronuncie a través de un «dictamen escrito no vinculante» sobre cuál de los Estados "puede estar en mejores condiciones para llevar a cabo una investigación o unas actuaciones judiciales sobre hechos concretos[52]".

Para pronunciarse sobre la jurisdicción más apropiada, Eurojust cuenta con una serie de criterios recogidos en su Informe Anual del año 2003[53], pero a los solos efectos orientativos y no distribuidos jerárquicamente, por lo que no responden a la cuestión que planteábamos al principio del trabajo. En dicho Informe de 2003 se parte de una presunción inicial: en la medida de lo posible, el procedimiento penal se debe llevar a cabo en la jurisdicción en la que se produjeron la mayor parte de los hechos delictivos o en la que se ocasionó la mayor parte del perjuicio. Es decir, aboga por acudir indistintamente y sin ninguna preferencia al criterio de la acción (lugar de producción de los hechos) o del resultado (lugar del perjuicio), con lo que ante un hipotético conflicto entre el país donde se hayan producido la mayor parte de los hechos y aquel otro país donde se hayan ocasionado los mayores perjuicios, los factores a tener en cuenta en dicho Informe son criterios que, a nuestro juicio, poco tienen que ver con ejercer la jurisdicción "en mejores condiciones". Tales factores son los siguientes: La localización del acusado; la capacidad de conseguir la extradición o entrega al acusado desde otro Estado; la posibilidad y consecuencias de repartir el procedimiento en dos o más jurisdicciones; la comparecencia de testigos; la protección de testigos; las posibles demoras; el interés de las víctimas; la disponibilidad del material probatorio obtenido en debida forma; el cumplimiento de obligaciones jurídicas existentes en un país y no en otro; la condena esperada; la mayor o menor efectividad en la recuperación de los productos del delito; los costes del procedimiento.

En nuestra opinión, la mayoría de esos criterios (por ej., cuál de las jurisdicciones está en condiciones de ofrecer un programa de protección de testigos y cuál no; o lo relativo a problemas a la hora de obtener pruebas) no deberían ser factores para determinar la "jurisdicción más apropiada", sino que tales cuestiones se refieren a problemas de asistencia y cooperación judicial o reconocimiento mutuo de resoluciones en el ámbito penal, para lo cual existe un importante catálogo de instrumentos legales comunitarios y nacionales que tratan de solventar estas cuestiones que poco o nada deberían influir en la determinación de la Jurisdicción.

---

[50] GONZÁLEZ CANO, I., "La Decisión Marco 2009/948/JAI del Consejo, de 30 de noviembre de 2009, sobre prevención y resolución de conflictos de jurisdicción en procesos penales", *Revista Unión Europea Aranzadi*, abril 2010, pp. 7-23.

[51] Memoria FGE año 2010, p. 1118 (disponible en: http://www.fiscal.es).

[52] (vid. Art. 7.1.a.ii) y 7.2 de la Decisión Marco 2002/187/JAI, modificada por la Decisión 2009/426/JAI del Consejo, de 16 de diciembre de 2008, por la que se refuerza Eurojust y se modifica la Decisión 2002/187/JAI por la que se crea Eurojust para reforzar la lucha contra las formas graves de delincuencia (DOUE L 138/14 de 4.6.2009).

[53] Los Informes Anuales de Eurojust pueden ser consultados en la siguiente página web: http://www.eurojust.europa.eu/doclibrary/corporate/eurojust%20Annual%20Reports/Annual%20Report%202003/Annual-Report-2003-ES.pdf.

Además, en dicho Informe se reconoce expresamente que *"la prioridad o el peso que se otorgue a cada uno de estos factores será diferente en cada caso. Nuestra intención es suministrar criterios y definir los aspectos que resultan relevantes en la toma de decisiones de este tipo*[54]", con lo cual, al igual que sucede con la posible solución ofrecida en el Convenio internacional sobre el Cibercrimen, la principal crítica que cabe hacer sobre esta normativa comunitaria reside en que hace depender algo tan importante como la determinación de la Jurisdicción competente de la hipotética consecución de un consenso entre las distintas autoridades implicadas, y para el caso de no darse dicho consenso, atribuye la resolución de la cuestión a Eurojust: un órgano de coordinación y asistencia, pero sin atribuciones para resolver los conflictos de una manera unívoca e imponer sus decisiones a los Estados miembros. Su labor concluye con esa "facilitación de asistencia en la resolución de conflictos de jurisdicción" (considerando nº14 de la Decisión Marco). De hecho, en la Memoria de la Fiscalía General del Estado del año 2010 se recogen las diversas respuestas por parte de España de las recomendaciones de Eurojust para la cesión de jurisdicción a autoridades extranjeras[55], y en la que no siempre se aceptó ceder la investigación de los hechos a otras autoridades judiciales.

En España, el procedimiento interno para acudir a Eurojust en caso de un posible conflicto de jurisdicción con otro Estado miembro de la UE ha sido objeto de desarrollo a través de la Ley 16/2015, de 7 de julio, y en dicha Ley se establece un listado de criterios a valorar por parte de la autoridad judicial española a la hora de pronunciarse sobre si la jurisdicción española está en mejores condiciones para conocer de los hechos[56]. Todo ello resulta meritorio y positivo, pero igualmente insuficiente, pues la solución final será la misma: a falta de consenso con la autoridad competente del otro Estado miembro, procederá solicitar del Colegio de Eurojust un dictamen escrito no vinculante.

2.3.3. La Directiva 2013/40/UE relativa a los ataques contra los sistemas de información

El último cartucho a emplear a nivel supranacional para evitar la concurrencia de jurisdicciones y determinar la competencia judicial penal de los Estados UE frente a los ciberdelitos lo constituyen las diversas disposiciones comunitarias aprobadas para determinados ámbitos sectoriales (pornografía infantil, terrorismo, ataques a sistemas informáticos, criminalidad organizada, etc.). Todas ellas se caracterizan por contener una delimitación más precisa de las reglas de competencia a aplicar para el reparto de la

[54] Informe Anual de 2003, op. cit., pág. 66.
[55] Vid. Memoria FGE 2010, pág. 1132 y ss.
[56] Ley 16/2015, de 7 de julio, por la que se regula el estatuto del miembro nacional de España en Eurojust, los conflictos de jurisdicción, las redes judiciales de cooperación internacional y el personal dependiente del Ministerio de Justicia en el Exterior (BOE núm. 162, de 8 de julio de 2015). Los criterios se enumeran en el apartado 5º del art. 32: a) Residencia habitual y nacionalidad del imputado; b) Lugar en el que se ha cometido la mayor parte de la infracción penal o su parte más sustancial; c) Jurisdicción conforme a cuyas reglas se han obtenido las pruebas o lugar donde es más probable que éstas se obtengan; d) Interés de la víctima; e) Lugar donde se encuentren los productos o efectos del delito y jurisdicción a instancia de la cual han sido asegurados para el proceso penal; f) Fase en la que se encuentran los procesos penales sustanciados en cada Estado miembro; y g) Tipificación de la conducta delictiva y pena con la que ésta viene castigada en la legislación penal de los distintos Estados miembros implicados en el conflicto de jurisdicción.

misma entre los distintos Estados, de modo que es posible afirmar que dichas normas superan lo establecido en el Convenio de Budapest de 2001 o en la mencionada Decisión Marco 2009/948/JAI, y aunque no arrojan una solución única, entendemos que sus reglas deberían ser tenidas en cuenta, en caso de concurrencia de jurisdicciones europeas en la investigación de un delito transnacional cometido a través de Internet, como argumentos a considerar de cara a una distribución de la competencia judicial penal a escala europea.

En materia de daños informáticos, el art. 10 de la Decisión Marco 2005/222/JAI del Consejo[57] utilizaba como criterios de atribución de la competencia el principio de territorialidad y el principio de personalidad. Sus reglas superaban lo dispuesto en el Convenio del Consejo de Europa sobre el Cibercrimen y en la Decisión Marco para la prevención y resolución de los conflictos de Jurisdicción, de acuerdo con dos motivos.

En primer lugar, porque definía con mayor nitidez cuándo se entiende que el delito se ha cometido "total o parcialmente en su territorio": a) cuando el autor de la infracción comete ésta estando físicamente presente en su territorio, independientemente de que la infracción se cometa o no contra un sistema de información situado en su territorio; y b) la infracción se comete contra un sistema de información situado en su territorio, independientemente de que el delincuente cometa o no la infracción estando físicamente presente en su territorio. Como puede observarse, la letra a) representaba la elección de la *teoría de la actividad*, con lo que se permitiría a los Estados miembros que pudieran ejercer su competencia para enjuiciar aquellos ataques dirigidos desde sus territorios contra sistemas informáticos que se encuentren en el extranjero, aunque se trate de terceros países no miembros de la UE, lo cual "muestra el compromiso asumido por la Comisión de luchar contra los ataques de los que son objeto los sistemas de información tanto en la Unión Europea como a escala mundial[58]". Por su parte, la letra b) sintetizaba la apuesta por la *teoría del resultado*, de modo que los Estados miembros podrían reclamar para sí la investigación y enjuiciamiento de aquellos ataques orquestados desde otro país pero dirigidos contra sus sistemas informáticos. No obstante, la elección de la teoría del resultado podría generar conflictos de jurisdicción entre los propios Estados miembros cuando dicho ataque provoque sus efectos en varios de ellos. En tal caso, el art. 10.4º remitía a la misma técnica que la recogida en el resto de Decisiones Marco: buscar un arreglo amistoso en primer término, o en su defecto, a acudir a Eurojust y el procedimiento de consultas de la DM 2009/948/JAI.

En segundo término, y al igual que la Decisión Marco 2002/475/JAI sobre la lucha contra el Terrorismo[59], establecía una cierta gradación en los criterios a seguir. Si el art. 9.2 de la DM sobre terrorismo declaraba que "se tendrán en cuenta *sucesivamente* los siguientes criterios para sumarse a ellas", el art. 10.4 de la DM sobre Ataques Contra Sistemas Informáticos apuntaba que "se podrán tener en cuenta los siguientes criterios *por orden consecutivo*: el Estado miembro en cuyo territorio se hayan cometido las

[57] DOUE L 69, de 16 de marzo de 2005, pág. 67, sustituida por la Directiva 2013/40/UE del Parlamento Europeo y del Consejo, de 12 de agosto de 2013, relativa a los ataques contra los sistemas de información y por la que se sustituye la Decisión marco 2005/222/JAI del Consejo (DOUE L 218, de 14 de agosto de 2013).

[58] Vid. la Propuesta de Decisión-marco del Consejo relativa a los ataques de los que son objeto los sistemas de información /* COM/2002/0173 final - CNS 2002/0086 */. DOUE n° 203 E, de 27 de agosto de 2002, pág. 109.

[59] Modificada en virtud de la Decisión Marco 2008/919/JAI del Consejo, de 28 de noviembre de 2008, (DOUE L 330, de 9 de diciembre de 2008, pág. 21).

infracciones de acuerdo con los apartados 1, letra a), y 2; el Estado miembro del que sea nacional el autor; y el Estado miembro en el que se haya encontrado al autor". La introducción por parte de ambas Decisiones Marco de cierta graduación en los criterios a seguir a la hora de determinar la Jurisdicción competente, en caso de concurrencia de varios Estados miembros[60], las convierte en una regulación más detallada que la contenida en el Convenio del Cibercrimen. Sin embargo, tampoco resultaba ser definitiva para resolver los múltiples casos de concurrencia de jurisdicciones que pueden darse cuando se trata de delitos cometidos a través de sistemas informáticos, pues precisamente el mayor *handicap* de esta DM es que se refería a ataques "contra" sistemas informáticos, esto es, se centra en los delitos de atentados contra la integridad de los datos o contra la integridad de los sistemas informáticos, en sus múltiples variantes —los que persiguen obstaculizar o interrumpir de manera significativa el funcionamiento de un sistema de información, introduciendo, transmitiendo, dañando, borrando, deteriorando, alterando, suprimiendo o haciendo inaccesibles datos informáticos, así como el acceso ilegal con la intención de borrar, dañar, deteriorar, alterar, suprimir o hacer inaccesibles datos informáticos contenidos en un sistema de información—, pero quedaría fuera de su ámbito de aplicación cualquier otro delito en el que el equipo informático sea un mero instrumento del delito (por ej., las estafas informáticas).

La mejora de las disposiciones de la DM de 2005 a través de la Directiva 2013/40/UE del Parlamento Europeo y del Consejo, de 12 de agosto de 2013, relativa a los ataques contra los sistemas de información[61], se centraron en ampliar los supuestos de infracciones que debían ser penalmente tipificadas por los Estados miembros en materia de ataques contra los sistemas de información –por ej., la producción intencional, venta, adquisición para el uso, importación, distribución u otra forma de puesta a disposición de aquellos instrumentos que permitan cometer cualquiera de las infracciones objeto de regulación, tales como programas informáticos o códigos de acceso, contraseñas, etc-, pero las reglas de competencia previstas en su art. 12 suponen una leve modificación con respecto a las previstas en 2005. Se sigue estableciendo como criterio prioritario el principio de territorialidad, si bien incorpora la posibilidad de que los Estados decidan atribuirse la competencia para aquellas infracciones cometidas fuera de su territorio, "cuando el autor tenga su residencia habitual en su territorio, o la infracción se cometa en beneficio de una persona jurídica establecida en su territorio".

Por otra parte, se excluye de su articulado cualquier mención a cómo resolver la concurrencia de jurisdicciones de los Estados miembros, ni al procedimiento de consultas de la DM 2009/948/JAI, aunque en su Considerando nº 27 se reconoce expresamente que *La naturaleza transnacional y transfronteriza de los modernos sistemas de información significa que los ataques suelen revestir un carácter transfronterizo, lo que plantea la necesidad urgente de proseguir la aproximación del Derecho penal en este ámbito. Por otra parte, la coordinación del enjuiciamiento de los*

[60] Cfr. la Decisión Marco 2008/841/JAI del Consejo, de 24 de octubre de 2008, relativa a la lucha contra la delincuencia organizada (DOUE L 300, de 11 de noviembre de 2008, p. 42), cuyo art. 7.2 no establece ninguna graduación para el mismo supuesto y establece simplemente que "Se tendrán especialmente en cuenta los siguientes elementos: a) el Estado miembro en cuyo territorio se hayan cometido los hechos; b) el Estado miembro del que el autor sea nacional o residente; c) el Estado miembro de origen de las víctimas; d) el Estado miembro en cuyo territorio se haya encontrado al autor".

[61] DOUE L 218, de 14 de agosto de 2013, pág. 8.

casos de ataques contra los sistemas de información debe facilitarse mediante la adecuada puesta en marcha y aplicación de la Decisión marco 2009/948/JAI del Consejo, de 30 de noviembre de 2009, sobre la prevención y resolución de conflictos de ejercicio de jurisdicción en los procesos penales.

3. SOLUCIONES

3.1. PROPUESTAS EN EL ÁMBITO INTERNACIONAL

En el ámbito internacional se ha sostenido la conveniencia de aprobar un Tratado internacional, bien específicamente referido a la lucha contra el cibercrimen y que solvente los posibles conflictos de jurisdicción a la hora de perseguir y enjuiciar los delitos cometidos a través de Internet, bien con carácter general para guiar el ejercicio de la jurisdicción penal por los tribunales nacionales y evitar la aparición de conflictos positivos de jurisdicción. Como ejemplo, la ONU incluyó en 1988 la delincuencia informática dentro de su informe *Propuestas para la acción internacional concertada contra las formas de delincuencia identificadas en el Plan de Acción de Milán*[62], y en la preparación del octavo congreso de la ONU sobre prevención del delito y tratamiento del delincuente, manifestó su preocupación por los efectos del progreso tecnológico en la comisión de delitos, lo que dio como resultado que en 1999 aprobara el *Manual de las Naciones Unidas de 1999 sobre Prevención y Control de la Delincuencia Informática*[63]. En dicho texto, se identificaban los problemas más importantes en torno a la cooperación internacional en el ámbito de la delincuencia informática y el derecho penal, entre otros, la insuficiencia de facultades legales para la investigación y el acceso a los sistemas informáticos, la falta de armonización entre las diferentes legislaciones nacionales de procedimiento relativas a la investigación de los delitos informáticos, el carácter transnacional de la delincuencia informática, así como la falta de la extradición y los tratados de asistencia mutua y de mecanismos sincronizados de aplicación de leyes que permitan la cooperación internacional, o la incapacidad de los tratados existentes para tener en cuenta la dinámica y necesidades especiales de investigación de crimen informático, por lo que ya se advertía acerca de la necesidad de negociar acuerdos sobre el tema de los conflictos positivos de jurisdicción. Durante el *12º Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal*, celebrado en Brasil en 2010, los Estados Miembros examinaron con cierto detalle la cuestión del ciberdelito y decidieron invitar a la Comisión de Prevención del Delito y Justicia Penal a que convocara a un grupo intergubernamental de expertos para que realizara un estudio exhaustivo del problema del delito cibernético y la respuesta ante ese fenómeno, cuyo proyecto se expuso en la reunión de dicho grupo, dependiente de la Oficina de Naciones Unidas contra la Droga y el Delito (UNODC), celebrada en Viena, del 17 a 21 de enero de 2011, y en la que las respuestas jurídicas al ciberdelito se agruparon en cinco esferas concretas: a) Armonización de la legislación; b) Derecho penal sustantivo; c) Instrumentos de investigación; d) Cooperación internacional; e) Pruebas electrónicas; y f) Responsabilidad.

---

[62] E/AC.57/1988/16.

[63] *United Nations Manual on the Prevention and Control of Computer Crime*, United Nations Commission on Crime Prevention and Criminal Justice, International Review of Criminal Policy - 8th Congress (Vienna, April 27 – May 6, 1999), apartados 254 a 284. Disponible en: http://www.uncjin.org/Documents/EighthCongress.html.

A nivel académico, merece ser tenida en consideración la *Propuesta de Stanford de un Convenio Internacional sobre el Cibercrimen y el Terrorismo del año 2000*[64], la cual resulta especialmente de interés, por cuanto su art. 5.4 propone un listado priorizado de fueros a nivel internacional que resultarían aplicables a la hora de determinar la jurisdicción más adecuada para el enjuiciamiento del cibercrimen en caso de conflicto de jurisdicción: 1º) el país en cuyo lugar se encontrase físicamente el autor a la hora de efectuar la conducta prohibida (esto es, clara preferencia por la teoría de la actividad); 2º) el país en cuyo territorio se produjera el principal daño con motivo de la conducta prohibida; 3º) el país de la nacionalidad del autor; 4º) cualquier país en donde el autor de los hechos fuera encontrado; y 5º) cualquier otro país con un vínculo efectivo con los hechos.

Otra propuesta presentada en el citado 12º Congreso de la ONU sobre Justicia penal y prevención del delito[65] consistía en considerar aquellos crímenes más graves contra la paz y la seguridad que se cometieran en el ciberespacio como crímenes de Derecho Internacional a través de un Tratado sobre el Ciberespacio de las Naciones Unidas, tanto si son o no punibles conforme a la legislación nacional, así como la posibilidad de crear un Tribunal Penal Internacional para el Ciberespacio, bien como una Subdivisión de la Corte Internacional de Justicia de las Naciones Unidas en La Haya, bien como una subdivisión de la Corte Penal Internacional, regido por el Estatuto de Roma, como piedra angular para la disuasión del cibercrimen a nivel mundial contra los ciberdelitos más graves de trascendencia mundial[66], al valorar la posibilidad de que los ciberataques masivos y coordinados contra infraestructuras críticas puedan ser calificadas como un "delito grave" a los efectos previstos en el art. 5 del Estatuto de Roma, de modo tal que, conforme con el art. 93.10.a) del mismo, "a solicitud de un Estado Parte que lleve a cabo una investigación o sustancie un juicio por una conducta que constituya un crimen de la competencia de la Corte o que constituya un crimen grave con arreglo al derecho interno del Estado requirente, la Corte podrá cooperar con él y prestarle asistencia".

Sin embargo, la posibilidad de crear tribunales internacionales *ad hoc* para el enjuiciamiento de los delitos cometidos a través de Internet no nos parece una solución realista, sobre todo si echamos la vista atrás para comprobar los problemas que generó en su momento la creación del Tribunal Penal Internacional, o si pensamos en la complejidad y lentitud que supondría intentar procesar ante dicha jurisdicción los millares de ciberdelitos de dimensión transfronteriza que se cometen en la actualidad. Y la misma opinión nos merece la idea de que los Estados en conflicto decidieran acudir a la Corte Internacional de Justicia de las Naciones Unidas en La Haya para que ésta

---

[64] *Draft International Convention To Enhance Protection from Cyber Crime and Terrorism*, elaborada por Abraham D. SOFAER, Seymour E. GOODMAN y otros, y publicado por The Hoover Institution, The Consortium for Research on Information Security and Policy (CRISP) y The Center for International Security and Cooperation (CISAC) en agosto de 2000. El texto se encuentra disponible en: http://web.stanford.edu/~gwilson/Transnatl.Dimension.Cyber.Crime.2001.p.249.pdf.

[65] *A Cyberspace Treaty - a United Nations Convention or Protocol on cybersecurity and Cybercrime*. Documento A/CONF.213/IE/7, 12º Congreso de la ONU sobre Justicia Penal y Prevención del Delito, celebrado en Salvador, Brasil, del 12 al 19 de abril de 2010. Documento disponible en: http://es.scribd.com/doc/87345574/UN-12th-Crime-Congress.

[66] SCHJOLBERG, S., "An International Criminal Court or Tribunal for Cyberspace (ICTC). Prosecution for the Tribunal Police investigation for the Tribunal", *East West Institute (EWI) Cybercrime Legal Working Group*, March 2012. Disponible en la página web: http://www.cybercrimelaw.net/documents/International_Criminal_Court_or_Tribunal_for_Cyberspace_(ICTC).pdf.

resolviera acerca de cuál resulta ser la jurisdicción más apropiada para el enjuiciamiento de los hechos[67]. La solución más práctica, más rápida y menos costosa a la hora de conseguir determinar una Jurisdicción «preferente» para el enjuiciamiento de los delitos con efectos transfronterizos no pasa, en nuestra opinión, por la creación de un órgano supranacional competente para resolver conflictos de jurisdicción entre los distintos Estados, sino por la promulgación de un listado de criterios de distribución de la competencia judicial internacional en materia penal, pues en la medida en que los Estados dispongan de unos criterios precisos y determinantes de cuál se considera la Jurisdicción más apropiada para el conocimiento de los hechos, se reducirán los supuestos de colisión de sus respectivas jurisdicciones a la hora de investigar y enjuiciar un determinado delito y, por tanto, la necesidad de acudir a un órgano supranacional para la resolución de tales conflictos.

3.2. PROPUESTAS EN LA UNIÓN EUROPEA

En la Unión europea no parece conveniente ni convincente que nos detengamos en un sistema de resolución de concurrencia de jurisdicciones basado en un dictamen no vinculante de un órgano intermediario y coordinador. Garantizar el principio de legalidad y seguridad jurídica que debe regir en el Espacio Común de Libertad, Seguridad y Justicia exige por parte de las Instituciones Europeas una necesaria actuación legislativa para que el ejercicio de la Jurisdicción por parte de los Estados miembros se base en un sistema de fueros precisos (y, en la medida de lo posible, jerárquicamente distribuidos) y recogidos en fuentes jurídicas vinculantes, sin que pueda quedar al albur de la consecución de un acuerdo, y sin que para llegar al mismo se manejen únicamente recomendaciones[68]. Sólo de esta manera será posible hablar de un verdadero «territorio europeo» o «espacio judicial europeo» a efectos penales. Incluso quienes han reclamado la necesidad de un nuevo marco legal europeo para la resolución de los conflictos de jurisdicción, que sea definido "con la mayor flexibilidad para que pueda ser compatible con las distintas tradiciones jurídicas y diferentes marcos legales de los países miembros de la Unión Europea", han admitido que "a largo plazo, sería deseable contar con unos criterios de determinación de la competencia uniformes y vinculantes para todos los Estados miembros[69]".

---

[67] Según KASPERSEN ("Cybercrime and Internet Jurisdiction", op. cit., pág. 19), "it is unlikely, impractical and counterproductive if parties to the cybercrime convention, instead of having a mutual consultation in order to determine the most appropriate jurisdiction, would invite the international court of justice in the Hague to rule on a conflict of jurisdiction". En España, FLORES PRADA (*Criminalidad informática. Aspectos sustantivos y procesales*, ed. Tirant lo blanch, Valencia, 2012, p. 316) advierte sobre los problemas de sumisión a la competencia de dicho tribunal por parte de los países, definición de su competencia, así como problemas de volumen de trabajo que soportaría dicho organismo internacional, por lo que no apoya tal solución.

[68] QUINTERO OLIVARES ("Derecho Penal y Unión Europea: Territorio y competencia. El Espacio Judicial Europeo", en VV.AA., *Derecho penal europeo. Jurisprudencia del TEDH. Sistemas penales europeos.* Colección *Estudios de Derecho Judicial*, nº155, 2009, p. 669) estima que "la mejor solución sería un acuerdo multilateral, al menos para el espacio UE, en donde se establecieran unos criterios de determinación de la competencia *que superaran la territorialidad*. Esos criterios podrían, y no en ese orden, ser la preferencia por prioridad temporal, la residencia del mayor volumen de perjudicados, la disponibilidad del mayor número de pruebas, el domicilio de las personas o sociedades que han ejecutado los hechos, y el último término, el acuerdo bilateral".

[69] VV.AA., *Conflictos de jurisdicción y principio ne bis in idem en el ámbito europeo* (Coordinadoras: Rosa Ana Morán Martínez e Isabel Guajardo Pérez), ed. Ministerio de Justicia, Madrid, 2007, p. 13.

En la Unión Europea, podemos afirmar que existen muy buenas intenciones, pero muy pocos resultados prácticos. Se ha advertido en múltiples ocasiones sobre la necesidad de potenciar el desarrollo de nuevos instrumentos de cooperación penal internacional para la represión de la ciberdelincuencia, y entre sus propuestas, se incluye la necesidad de clarificar las reglas atributivas de la competencia judicial internacional en materia penal, y en particular, la determinación de la jurisdicción competente para conocer de los ciberdelitos, pero muy poco se ha avanzado.

En la Comunicación de 10 de junio de 2009 «Un espacio de libertad, seguridad y justicia al servicio de los ciudadanos[70]», se propusieron, entre otras medidas, la creación de una red especializada que agrupase a los responsables nacionales de la lucha contra la delincuencia informática, y sobre todo, su intención de "clarificar las normas de competencia jurisdiccional y el marco jurídico aplicable al ciberespacio para favorecer las investigaciones transfronterizas". También en el «Libro Verde sobre la obtención de pruebas en materia penal en otro Estado miembro y sobre la garantía de su admisibilidad[71]», publicado el 11 de noviembre de 2009 con el fin de sustituir el actual régimen jurídico por un nuevo y único instrumento que cubra todos los tipos de prueba, en el que se podría incluir normas sobre la prueba electrónica, se insistía en la necesidad de aclarar la jurisdicción competente, al igual que en el Anexo del *Plan de Estocolmo*[72], de 20 de abril de 2010, en donde la Unión Europea expuso importantes medidas a adoptar frente a la ciberdelincuencia, y nuevamente insistía en su voluntad de "adoptar propuestas legislativas para establecer las normas de competencia jurisdiccional relativas a la ciberdelincuencia a escala europea e internacional". Apenas un mes después, en la Comunicación de la Comisión de 19 de mayo de 2010 sobre una Agenda Digital para Europa[73], la Comisión afirmó que "Presentará medidas, incluyendo iniciativas legislativas, para combatir los ciberataques contra los sistemas de información a más tardar en 2010, y una normativa conexa sobre la jurisdicción en el ciberespacio a nivel europeo e internacional a más tardar en 2013".

No obstante, debemos ser optimistas de cara al futuro, pues la aprobación de medidas comunes sobre las reglas de determinación de la jurisdicción penal en el Espacio Judicial Europeo son factibles de conformidad con la normativa comunitaria actual sobre cooperación judicial en materia penal del Tratado de Funcionamiento de la Unión Europea (arts. 82 y siguientes). El Parlamento Europeo y el Consejo disponen de la posibilidad de adoptar, con arreglo al procedimiento legislativo ordinario, *medidas tendentes a prevenir y resolver los conflictos de jurisdicción entre los Estados miembros* (art. 82.1.b). También se establece la posibilidad de que el Parlamento Europeo y el Consejo puedan establecer, mediante directivas, «normas mínimas» que, en el plano penal sustantivo se referirían a la definición de las infracciones penales y de las sanciones en ámbitos delictivos que sean de especial gravedad y tengan una dimensión transfronteriza (art. 83.1.II: entre dichos ámbitos se incluye expresamente la delincuencia informática) y que en el plano procesal se referirían, entre otras, a aquellos

[70] Comunicación de la Comisión al Parlamento y al Consejo, de 10 de junio de 2009. COM (2009) 262 final.
[71] Libro Verde sobre la obtención de pruebas en materia penal en otro Estado miembro y sobre la garantía de su admisibilidad, de 11 de noviembre de 2009 [COM (2009)624 final].
[72] Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones, de 20 de abril de 2010, titulado *Garantizar el espacio de libertad, seguridad y justicia para los ciudadanos europeos. Plan de acción por el que se aplica el programa de Estocolmo*. COM (2010) 171 final.
[73] COM(2010) 245 final.

elementos específicos del procedimiento penal que el Consejo habrá determinado previamente mediante una decisión, si se consideran necesarias igualmente para facilitar el reconocimiento mutuo de las sentencias y resoluciones judiciales y la cooperación policial y judicial en asuntos penales con dimensión transfronteriza (art. 82.2.d). En nuestra opinión, las normas de distribución de la jurisdicción entre los distintos Estados miembros son claves para la válida tramitación del proceso penal, y por lo tanto, podrían quedar incluidas dentro de tales «normas mínimas». En su defecto, sería posible atribuir a un órgano a nivel comunitario la facultad de adoptar una decisión obligatoria sobre la jurisdicción más adecuada. Y como tercera posibilidad, también debe tenerse en cuenta la posibilidad de que el Parlamento Europeo y el Consejo puedan determinar, mediante Reglamentos adoptados con arreglo al procedimiento legislativo ordinario, la estructura, el funcionamiento, el ámbito de actuación y las competencias de Eurojust, las cuales podrán incluir *la intensificación de la cooperación judicial, entre otras cosas mediante la resolución de conflictos de jurisdicción y una estrecha cooperación con la Red Judicial Europea* (art. 85.1.c).

3.3. PROPUESTAS INTERPRETATIVAS DE LA LEGISLACIÓN ESPAÑOLA

En defecto de un Tratado internacional que establezca los criterios de determinación de la jurisdicción en materia penal, las soluciones aportadas desde la Unión Europea en las diversas Directivas y Decisiones Marco analizadas (terrorismo, pornografía infantil, crimen organizado o ataques contra sistemas informáticos) constituyen un paso positivo en el camino hacia el establecimiento de un sistema legal de determinación de la jurisdicción penal entre los Estados miembros, pero sólo arrojan soluciones puntuales y aplicables únicamente a los supuestos de concurrencia de jurisdicciones de los Estados miembros, y no frente a conflictos de jurisdicción surgidos con terceros países (por ej., desde donde se preparen, concierten o ejecuten ataques –o se elabore el material a emplear- contra sistemas informáticos localizados en el territorio de uno o varios Estados miembros de la UE, etc.). La opción por acudir a los factores que maneja el *Informe Eurojust* a la hora de determinar la jurisdicción más apropiada para el enjuiciamiento de los hechos, así como utilizar los criterios internos de la Ley 16/2015, de 7 de julio, son otras opciones, pero adolecen de los mismos defectos: falta de jerarquía en el catálogo de criterios manejados e indeterminación de qué entender por "lugar de comisión del hecho". Para ello, proponemos diversos argumentos interpretativos que ofrecer a los tribunales a la hora de delimitar el ejercicio de la jurisdicción penal.

3.3.1. Criterios primarios y secundarios de determinación de la jurisdicción

En primer lugar, una posible solución a valorar a la hora de resolver la jurisdicción más apropiada para conocer de un ataque informático pasa por clasificar, por niveles de importancia, los criterios utilizados según permitan distinguir una mayor conexión entre el Estado que reclama para sí el conocimiento de los hechos con la conducta a enjuiciar, en función de que se trate de criterios «esenciales» (primarios) o «accidentales» (secundarios) a la hora de delimitar la jurisdicción de dicho Estado. Esta posibilidad de establecer una cierta prioridad entre los criterios a manejar ya fue apuntada en su momento por las Naciones Unidas en el *Manual de las Naciones Unidas*

de 1999 sobre Prevención y Control de la Delincuencia Informática[74], y en Europa en el *Libro Verde de 2005*[75].

En efecto, si entendemos la Jurisdicción como una manifestación de la soberanía de un Estado, podemos afirmar que las características definitorias de la extensión de ese poder estatal encuentra sus límites, al igual que sucede con su soberanía, en torno a tres pilares: el territorio, las personas y las conductas a desterrar o prohibir. Éstos serían los elementos primarios que definen aquélla, y tras ellos podríamos acudir a otros elementos atributivos de la misma con carácter secundario, pues no cabe duda de que no todos los factores utilizados tienen el mismo peso a la hora de otorgar prioridad a una jurisdicción para el enjuiciamiento de unos hechos[76]. Conforme a tales elementos —territorio, personas y bienes protegidos—, los criterios utilizados por los ordenamientos jurídicos para delimitar la jurisdicción de un determinado país se basan en la interpretación de dichos elementos, bien con un significado ordinario o preferente, bien con un significado secundario o alternativo. Así por ejemplo, dentro del elemento territorial, el significado ordinario de *territorio* es aquél que alude al "lugar de comisión del delito" (criterio primario para la determinación de la jurisdicción), y de hecho, el lugar de comisión del delito constituye el primer y principal criterio manejado por los Estados para la delimitación de su jurisdicción, para lo cual proceden a definir qué se entiende por "territorio" a los efectos de concretar dónde se entiende cometido el acto punible (espacio físico, aéreo, mar territorial, buques, aeronaves y recintos diplomáticos, etc.). Pero el territorio también puede usarse de manera secundaria o residual, como por ejemplo cuando se acude al lugar de captura del sospechoso, el lugar donde se encuentran las pruebas del delito, el lugar donde se ubican los equipos informáticos, etc. Todos ellos constituirían los "criterios secundarios" o "menos relevantes" a la hora de determinar la jurisdicción más apropiada para conocer de los hechos delictivos, pues el lugar de comisión del hecho ilícito guarda una mayor conexión con la competencia judicial para juzgar esos hechos que el lugar de captura del acusado.

Por citar un ejemplo concreto, en el caso del empleo de una red de ordenadores zombies para acometer un ataque de tipo DoS, los criterios preferentes deberían ser el lugar desde donde se controlan dichos equipos o el lugar en donde se producen los perjuicios, y no tanto el lugar en el que se encuentran los ordenadores o servidores empleados como meros instrumentos comisivos. En este sentido, y con respecto a valorar la importancia de la ubicación de los nodos –servidores- por los que transita la "ruta telemática" de la información comunicada a través de Internet, MARCHENA

---

[74] *United Nations Manual on the Prevention and Control of Computer Crime*, United Nations Commission on Crime Prevention and Criminal Justice, International Review of Criminal Policy - 8th Congress (Vienna, April 27 – May 6, 1999), apartados 254 a 284. Disponible en: http://www.uncjin.org/Documents/EighthCongress.html.

[75] COM(2005) 696 final, apartado 2.5: "(…) Es factible definir una serie de criterios relevantes que se aplicarán y ponderarán de forma flexible en cada caso, para lo cual las autoridades competentes tendrán que disponer de un considerable margen de discrecionalidad. Esos criterios, o elementos relevantes, que influirán en el proceso de determinación de la jurisdicción adecuada, deberán ser objetivos y se enumerarán en un futuro instrumento de la UE. En particular, la lista podría incluir la *territorialidad, criterios relativos al sospechoso o al demandado, los intereses de las víctimas, criterios relacionados con los intereses del Estado, y otros criterios relativos a la eficacia y rapidez de los procedimientos.* Tal vez podrían señalarse ciertos elementos *no* relevantes".

[76] En el mismo sentido, BRENNER, S., "Cybercrime jurisdiction", op. cit., p. 198.

GÓMEZ[77] ha advertido que el simple recorrido telemático a través del cual discurre el sofisticado medio ejecutivo no puede aspirar a definir una pretensión de jurisdiccionalidad allí donde no se ha desplegado la acción ni se ha verificado el resultado. Este razonamiento se ha reseñado en la anteriormente citada Sentencia de la Audiencia Nacional de 11 de junio de 2015 referida a la llamada "operación mariposa", en la que quedó acreditado que para evitar la localización del origen de los ataques, los botmaster iban cambiando de servidores de Comando y Control (un servidor usado para conectar a todos los equipos infectados), de tal modo que los ordenadores infectados no saben, a priori, dónde está su Comando, y la dirección de internet a la que comunicarse para recibir las órdenes se correspondía con un DNS dinámico, esto es, un dominio que cambia la localización del host o máquina al antojo de su administrador. Y en Italia también se ha señalado que el lugar de ubicación de los servidores donde se encuentran almacenados o a través de los cuales se difunden determinados contenidos ilícitos no debería ser valorado como punto de conexión para fundamentar la jurisdicción de los tribunales del país donde se ubican aquéllos, cuando éste constituye el único vínculo entre los hechos objeto de enjuiciamiento y los tribunales del foro[78].

3.3.2. Prioridad de la teoría de la actividad

El criterio preferente y más empleado por los Estados para la delimitación de su jurisdicción es el que tiene que ver con su territorio, entendido como «el lugar donde se comete el hecho delictivo», mientras que el criterio de la nacionalidad resulta utilizado de manera subsidiaria para cubrir aquellas conductas llevadas a cabo fuera del territorio nacional y evitar, bien un detrimento de las relaciones internacionales con otros países por culpa de las conductas realizadas por sus nacionales en el extranjero, bien que aquéllos puedan escudarse en su nacionalidad de origen para no ser juzgados en el lugar en donde cometieron los hechos delictivos. Dicho principio de territorialidad también es el que figura en primer lugar en los distintos Convenios internacionales y Decisiones Marco y Directivas analizadas, de modo que no resulta complicado concluir que el "lugar de comisión del delito" representa el punto de conexión más estrecho con la conducta delictiva, y por tanto, debe ser ese primer criterio primario a utilizar a la hora de distinguir la jurisdicción más apropiada.

El problema, por tanto, no reside en la inexistencia de un criterio preferente de determinación de la jurisdicción cuando se trata de delitos cometidos a distancia, sino las distintas interpretaciones manejadas por los ordenamientos domésticos y sus correspondientes órganos jurisdiccionales nacionales a la hora de determinar dicho "lugar de comisión del delito". Esto es, la cuestión se reduce a concretar cuál debe ser la «teoría prioritaria» (acción, resultado o ubicuidad) para determinar ese *locus delicti*

[77] MARCHENA GÓMEZ, M., "Dimensión jurídico penal…", op. cit., p. 11. Respecto a la irrelevancia de los "lugares de tránsito", vid. también SÁNCHEZ GARCÍA, I. y BLANCO CORDERO, I., "Problemas…", op. cit., p. 170 y GÓMEZ TOMILLO, M., *Responsabilidad penal por delitos cometidos a través de internet. Especial consideración del caso de los proveedores de contenidos, servicio, acceso y enlaces*. Ed. Aranzadi, Navarra, 2004, pp. 83 y ss. Cfr. FLORES PRADA, I., *Criminalidad informática…*, p. 327, para quien el lugar de comisión del delito podría resultar de la conexión de "lugares virtuales" (alojamiento de la información, dominios que la soportan, servidores que la difunden) con lugares físicos (territorios en los que radican los servidores, territorios que autorizan los dominios, territorios en los que se ha producido el daño, domicilio de la víctima o domicilio del autor de los hechos).

[78] Vid. las Sentencias de la Corte Suprema de 21 diciembre 2010 (nº2739/2010, depositada el 26-1-2011) y de 15 de marzo de 2011 (nº16307/2011, depositada el 26 de abril de 2011), que rechazan que el lugar donde se encuentra el servidor pueda ser utilizado a la hora de determinar la competencia penal.

cuando el ilícito se lleva a efecto en una jurisdicción pero produce sus resultados en otra.

Como hemos comprobado, nuestro Tribunal Supremo no aplica en todo caso la teoría de la actividad a los tipos clasificados como «delitos de actividad», ni la teoría del resultado a los «delitos de resultado», respectivamente. Y a nivel europeo, se aplica reiteradamente la conjunción disyuntiva «o», lo cual significa dotar a ambos hipotéticos foros (el lugar de la acción o el lugar del resultado) de equivalencia o de una posición similar, de modo que pueden emplearse indistintamente y sin ninguna preferencia entre las mismas. Con ello no se consigue solucionar el problema de delimitar la jurisdicción prioritaria: si aquélla donde se hayan producido la mayor parte de los hechos y aquel otro país donde se hayan ocasionado los mayores perjuicios.

Ahora bien, en el *Manual de las Naciones Unidas de 1999 sobre Prevención y Control de la Delincuencia Informática*[79], a la hora de establecer criterios determinantes de la jurisdicción con carácter prioritario para resolver posibles conflictos positivos de jurisdicción, se citó como ejemplo "el lugar del acto por encima del lugar del resultado, o el lugar de la aprehensión física del sospechoso por encima de condenas en ausencia o de extradición". Y existen diversos argumentos para priorizar como lugar de comisión del delito, como regla general, a los tribunales del lugar donde se pone en práctica la conducta delictiva –aquel lugar en donde el sujeto ejecuta todos o parte de los actos que objetivamente deberían producir el resultado, y específicamente referido a la comisión de delitos a través de la Red, allí donde el sujeto utiliza un sistema informático para acceder a la Red o para iniciar o mantener una comunicación electrónica, lo cual incluiría el lugar desde el que el sujeto se halla físicamente y teclea en un ordenador el comando oportuno- en detrimento del Estado donde se produzcan los resultados del delito.

En primer lugar, optar por la teoría de la actividad y atender al lugar en el que se despliega la conducta delictiva permitiría perseguir y enjuiciar aquellos supuestos de actos que no han dado lugar a un resultado, pero sí que tienen entidad suficiente para ser considerados actos preparatorios del delito y no simplemente actos internos no punibles. De este modo, aquellas conductas preparatorias punibles que puedan considerarse supuestos de tentativa, conspiración y proposición para delinquir –que deben ser perseguidas, según el art. 6 de la Directiva 2013/40/UE-, en los que el resultado ilícito no llega a producirse, también serían perseguibles por el Estado donde se pusieron en práctica. Si en el plano interno, el Tribunal Supremo ha advertido que en los supuestos punibles de conspiración es competente el juzgado del lugar donde se materializaron los actos conspiradores, independientemente del lugar donde el delito a ejecutar hubiese de realizarse[80], podría llegar a considerarse que en los delitos de daños informáticos que no llegan a producirse (ej., el *malware* que es inutilizado por un antivirus), el lugar al que asignar la competencia podría ser el lugar desde donde se lanzó dicho virus –teoría de la actividad- si ello pudiera determinarse sin excesiva complejidad.

---

[79] *United Nations Manual on the Prevention and Control of Computer Crime*, United Nations Commission on Crime Prevention and Criminal Justice, International Review of Criminal Policy - 8th Congress (Vienna, April 27 – May 6, 1999), apartados 254 a 284. Disponible en: http://www.uncjin.org/Documents/EighthCongress.html.

[80] El ATS de 4 de febrero de 2002 (cuestión núm. 60/2001) declaró que en el delito de conspiración para el asesinato a cometer en el territorio de otro partido judicial, es competente el del Juzgado del lugar donde se han producido efectivamente los actos conspiradores, independientemente del lugar donde el homicidio hubiese de realizarse.

En segundo lugar, también puede resultar preferible optar por el lugar donde se lleva a cabo la acción frente al lugar donde se produce el resultado, porque puede suceder que el delito despliegue sus efectos en los territorios de diversos Estados, como sucede con los supuestos de daños informáticos derivados de la difusión de *malware*. En el plano interno, una hipotética cuestión de competencia entre los órganos jurisdiccionales correspondientes a los distintos partidos judiciales donde se hayan ocasionado daños informáticos puede ser resuelta a través de la aplicación de la teoría de la ubicuidad, y atribuir la investigación al órgano judicial que primero iniciara actuaciones por tales hechos, pero esta solución no se antoja posible en el plano internacional, pues los Estados podrían argüir otros criterios igualmente importantes, como por ejemplo, el número de víctimas afectadas en su territorio (sistemas informáticos pertenecientes a particulares, empresas, organismos e instituciones, etc.) o la mayor gravedad de los daños ocasionados en el mismo (infraestructuras críticas, servicios públicos esenciales, etc.), con lo que habría que analizar qué parámetros resultan apropiados para medir dicha gravedad (perjuicio patrimonial constatable, número de sistemas afectados, etc.).

En aquellos casos en los que el lugar desde el que se lleva a cabo la acción coincida con el lugar donde se encuentra el sospechoso, su captura en dicho territorio facilitaría enormemente su procesamiento si finalmente el país de captura, que coincide con el lugar donde se puso en práctica la conducta antijurídica, es considerado como la jurisdicción más apropiada para el enjuiciamiento de dicha conducta. Y también facilitaría la futura ejecución de su condena, y en su caso, la reparación civil del daño si para ello hay que embargar su patrimonio, que generalmente se localizará en el mismo país de residencia. Desde la perspectiva del sujeto pasivo, también facilitaría el ejercicio del derecho de defensa por parte del sospechoso. En conclusión, el país donde se lleva a cabo la actividad delictiva es el que *a priori* se encuentra "en mejores condiciones para llevar a cabo una investigación o unas actuaciones judiciales sobre hechos concretos[81]",

Por otra parte, debe tenerse presente que en determinados delitos cometidos a través de la Red (por ejemplo, los ciberataques), es muy probable que el autor de los hechos ni tan siquiera conozca el lugar físico de producción del resultado, ya que su objetivo será el acto antijurídico en sí –destruir, dañar o inutilizar un sistema informático u obstaculizar su funcionamiento-, con independencia de si para ello se afecta a las jurisdicciones de uno o varios Estados. Supongamos que varios jóvenes activistas en contra de la explotación laboral infantil, consideran inmoral que una determinada multinacional de ropa deportiva utilice a niños de corta edad en oriente para la fabricación de sus productos, y deciden aprovechar la sala de ordenadores de su universidad para lanzar un denominado "ataque distribuido de denegación de servicio" (*DDoS*) contra la página web de venta online de dicha multinacional, para bloquear el acceso a dicha página y evitar así que se comercialicen a través de Internet dichos productos. A los ciberactivistas les resulta indiferente cuál es la sede social de la matriz de dicha empresa, cuál es la sede de la filial que se ocupa del marketing y venta online, o en qué jurisdicción radican los Servidores que alojan dicha página web, pues su

[81] Art. 7.1.a.ii) y 7.2 de la Decisión Marco 2002/187/JAI, modificada por la Decisión 2009/426/JAI del Consejo, de de 16 de diciembre de 2008, por la que se refuerza Eurojust y se modifica la Decisión 2002/187/JAI por la que se crea Eurojust para reforzar la lucha contra las formas graves de delincuencia (DOUE L 138/14 de 4.6.2009).

voluntad es impedir la venta en Internet de tales productos confeccionados por unas inocentes manos infantiles.

El vínculo más efectivo, para el caso de que pueda determinarse, sería el lugar desde donde se lanza el ataque (entendiendo por tal el lugar desde donde se controla o administra dicho ataque, aunque se utilicen millares de *botnets* dispersos en distintos países), y que es una conducta punible conforme a las leyes del país desde donde se pone en práctica. Empero, esta solución no resulta completamente satisfactoria, pues no solventaría la determinación de la jurisdicción más apropiada para castigar aquellas conductas concertadas que se ejecutan desde múltiples jurisdicciones para amplificar los efectos de su acción, ni aquellos supuestos en los que los delincuentes explotan las vulnerabilidades de la ausencia de fronteras en el mundo digital a través de realizar sus actividades desde países considerados un refugio seguro debido a la ausencia de regulación penal o a la inadecuada adaptación de la misma a la Era Digital.

Para paliar estos problemas competenciales cuando existe una pluralidad de jurisdicciones en donde se hayan producido los efectos dañosos del delito, se ha afirmado la existencia de bienes jurídicos supranacionales que pueden ser lesionados desde un territorio, pero expandiendo el efecto nocivo de la infracción por un espacio superior, dando lugar a supuestos de «ultraterritorialidad», en cuyo caso se ha defendido la competencia jurisdiccional simultánea de todos los Estados que hayan sufrido las consecuencias de la acción, pero sometiendo la misma a la "preferencia de paso[82]". Como ejemplo, la Decisión Marco 2000/383/JAI contra la falsificación de la moneda euro[83] establecía en su art. 7.2 la obligatoriedad de todos los Estados miembros que hubieran adoptado el euro de perseguir judicialmente los delitos de falsificación de la moneda euro *con independencia de la nacionalidad del autor del delito y del lugar en que éste se haya cometido*. De igual modo, y aunque la Decisión Marco 2005/222/JAI y la posterior Directiva 2013/40/UE no lo señalen expresamente, un ciberataque que tenga por objetivo infraestructuras informáticas críticas de la Unión Europea y cause daños en múltiples jurisdicciones puede ser perseguido por cualquiera de los Estados miembros, con independencia de dónde se ubiquen los sistemas informáticos atacados, aunque el país en donde tengan su ubicación las infraestructuras afectadas debería tener esa "preferencia de paso" (por lo que respecta a España, nuestros tribunales deberían ser igualmente competentes para perseguir la conducta expresamente tipificada en el apartado 4º del art. 264.2 CP).

3.3.3. La «doctrina de los efectos» y la protección de los intereses nacionales

La «doctrina de los efectos» constituye una excepción a la preferencia de la teoría de la actividad cuando la actividad ilegal es realizada en una jurisdicción y los efectos se aprecian en otra jurisdicción distinta, dado que atender a los efectos de la acción (resultado) representa una interesante opción para legitimar la extensión de la jurisdicción a conductas realizadas desde el extranjero que persiguen provocar un

[82] Respecto a dicha competencia jurisdiccional simultánea y esa "preferencia de paso", vid. QUINTERO OLIVARES, G., "Derecho Penal y Unión Europea…", op. cit., p. 684, quien defiende la competencia "del Estado desde el que se ha producido el daño o del Estado que peores consecuencias haya sufrido". Una vez más, no se prioriza ninguno de ambos lugares, con lo que el problema se mantendría irresoluble.

[83] Decisión Marco 2000/383/JAI, 29 de mayo de 2000, sobre el fortalecimiento de la protección, por medio de sanciones penales y de otro tipo, contra la falsificación de moneda con miras a la introducción del euro (DOUE L 140, de 14 de junio de 2000).

resultado lesivo en el territorio del foro, aunque ningún elemento constitutivo de la acción delictiva se haya producido en el Estado que reclama para sí su competencia, y evitar así la proliferación de "paraísos cibernéticos" desde donde las redes criminales puedan llevar a cabo sus conductas antijurídicas al amparo de la escasa o nula regulación penal de tales territorios, o en virtud de la sabida ausencia de cooperación penal de dichos países con aquéllos otros en donde se producen los efectos del delito.

En 1911, en el caso *Strassheim v. Daily*[84], el Tribunal Supremo estadounidense reconoció la posibilidad de que un Estado pueda ejercer su jurisdicción penal sobre los actos cometidos fuera de los límites territoriales del mismo si con tales actos realizados fuera de la jurisdicción, "existía la intención de producir efectos perjudiciales en su interior", lo cual justificaba la posibilidad de que el Estado castigase la causa del daño como si el autor del mismo hubiera estado presente en su territorio. Para aplicar dicha «doctrina de los efectos», resultará esencial constatar el conocimiento por parte del acusado del daño causado en el Estado del foro, o de la posibilidad de que su acción pueda generar un resultado lesivo en el territorio del foro[85]. Desde entonces, esta doctrina de los efectos para la determinación de la jurisdicción penal ha sido utilizada por los tribunales estadounidenses en casos relacionados con sitios web de apuestas ilegales en Internet, aunque tengan su centro de operaciones y su administración en el extranjero, por entender que despliegan sus efectos en territorio estadounidense porque reciben y remiten ingentes remesas de dinero desde los EE.UU hacia un lugar fuera de dicho país y viceversa, con la intención de promover el ejercicio de diversas actividades ilegales que generan sus efectos perniciosos contra los intereses estadounidenses (por ej., el movimiento de fondos para pagar las ganancias de los jugadores, la recepción de las cantidades correspondientes a las apuestas de ciudadanos estadounidenses, la contratación de distribuidores y anunciantes para promover las apuestas, etc.)[86]. La doctrina, no obstante, no es uniforme a la hora de estimar aplicable dicha doctrina al ciberespacio en materia penal[87].

---

[84] 221 U.S. 280; 31 S Ct 558; 55 L Ed 735 (1911).

[85] Vid. NORRIS, E. F., "Why the Internet isn't special: restoring predictability to personal jurisdiction", *Arizona Law Review*, Fall 2011, vol. 53, p. 1020, quien cita los casos *Plata v Brown*, 382 F. App'x 723, 728-30 (10th Cir. 2010), *Tamburo v. Dworkin*, 601 F. 3d 693, 706 (7th Cir. 2010), *Licciardello v Lovelady*, 544 F. 3d 1280, 1287/88 (11th Cir. 2008), y *Revell v. Lidov*, 317 F. 3d 467, 473 (5th Cir. 2002).

[86] Vid. *People v. World Interactive Gaming* 714 NYS2d 844, 850 (1999), de la Corte Federal de Nueva Cork: "[a] computer server cannot be permitted to function as a shield against liability, particularly in this case where respondents actively targeted New York as the location where they conducted many of their allegedly illegal activities". Así lo ha reconocido también expresamente la Fiscalía General de los EE.UU. en el caso *bodog.com*, un portal de apuestas localizado en Canadá, y frente a cuyos administradores se ha presentado un escrito de acusación formal (*indictment*) ante los tribunales de Maryland y se ha solicitado el bloqueo y decomiso (*seizure warrant*) del dominio de Internet de dicho portal. El escrito de acusación de encuentra disponible en: http://beta.images.theglobeandmail.com/archive/01379/Bodog_indictment_1379348a.pdf, y la solicitud de bloqueo y confiscación del dominio web se puede consultar en: http://beta.images.theglobeandmail.com/archive/01379/Bodog_website_seiz_1379347a.pdf.

[87] A favor de la aplicabilidad de la doctrina de los efectos en el ciberespacio, vid. WILSKE, S. / SCHILLER, T., "International Jurisdiction in Cyberspace: Which States May Regulate the Internet?", *Federal Communications Law Journal*, vol. 50, 1997, nº1, p. 132; BERG, T., "Criminal Law: State criminal jurisdiction in cyberspace: Is there a Sheriff on the electronic frontier?", *Michigan Bar Journal*, núm. 79, June 2000, pp. 659 y ss., y HAYASHI, M., "Objective Territorial Principle or Effects Doctrine? -Jurisdiction and Cyberspace-", *In.Law Journal*, 2006, nº6, p. 300 (Disponible en: http://www.morlacchilibri.com/inlaw/downloads/in.law_08_2.pdf. Mantienen sus dudas KRIZEK, M., "Protective Principle of Extraterritorial Jurisdiction: A Brief History and an Application of the Principle to Espionage as an Illustration of Current United States Practice", Boston University International Law Journal, 1988, p. 337 y ss.; CAMERON, I., The Protective Principle of International Criminal

Como vemos, esta aplicación extraterritorial de la ley penal cuando se entiende que el daño se ha producido en el territorio nacional, aunque la acción se realice en el extranjero, no dista mucho de la decisión *Lotus* de la Corte Permanente de Justicia Internacional en 1927, en el famoso litigio entre Francia y Turquía, en la que se reconoció el derecho de una nación, en determinadas circunstancias, para ejercer jurisdicción sobre las acciones que se originan en el extranjero, pero cuya efectos se hacen sentir dentro de la nación.

En España, si los daños informáticos son considerados actos terroristas en virtud de lo establecido en el art. 573.2 CP, el delito sería perseguible en España de conformidad con el art. 23.4.e) LOPJ con independencia del lugar desde donde se ejecute el ataque, y en este sentido, debemos recordar que la Decisión Marco 2002/475/JAI sobre la lucha contra el terrorismo[88] permite incluso perseguir esas conductas cuando el delito se cometa *parcial o totalmente, en su territorio, sea cual fuere el lugar en el que el grupo terrorista tenga su base o ejerza sus actividades delictivas* (art. 9.4).

En otros casos, la cuestión a resolver radicará en determinar si aquella actuación delictiva a través de Internet, ejecutada desde el extranjero pero dirigida a producir un "efecto sustancial" sobre los intereses españoles, puede o no ser objeto de enjuiciamiento en España de acuerdo con los fueros de jurisdicción penal del art. 23 LOPJ. En nuestra opinión, y además de los supuestos de ciberterrorismo, es evidente que en supuestos de espionaje militar, revelación de secretos relativos a la seguridad nacional, etc., se aprecia claramente la necesidad de que el Estado que sufre el ataque proveniente desde el extranjero reclame para sí el ejercicio de la jurisdicción penal, con independencia del foro desde donde se concertó o ejecutó el ataque y con independencia de la nacionalidad de los autores del mismo. Es cierto que la aplicación de dicho principio real quedaría reducida a los delitos incardinables en el listado del art. 23.3 LOPJ, y como sabemos, la ciberdelincuencia se caracteriza por una heterogeneidad comisiva, pero frente a ello cabe proponer dos vías para que los tribunales penales españoles puedan esgrimir su competencia judicial penal, y estas dos vías ya han sido utilizadas por la jurisprudencia para otros tipos delictivos.

En primer lugar, mediante una interpretación finalista del catálogo delictivo al que se refiere el principio real recogido en el art. 23.3 LOPJ, tal y como sucede con la noción de "falsificación que perjudique directamente al crédito o intereses del Estado, e introducción o expedición de lo falsificado" de la letra f) de dicho precepto. El Tribunal Supremo ha manifestado que la falsificación de documentos que permitan identificar a las personas (no sólo el pasaporte o el documento nacional de identidad, sino también el permiso de conducir) siempre afecta a los intereses del Estado, no sólo desde la perspectiva de las exigencias derivadas del art. 6 del Convenio Schengen, sino porque "en la realidad social en clave internacional no le puede ser indiferente a ningún país la identificación de personas provistas de documentos identificativos falsos, pues ello afecta a las políticas de visados, inmigración, como de seguridad, aun cuando el acto

---

Jurisdiction, Dartmouth Pub Co, 1994; y GERCKE, M., *Comprensión del ciberdelito: fenómenos, dificultades y respuesta juridical*, UIT, Ginebra, 2012, p. 252.

[88] Modificada a través de la Decisión Marco 2008/919/JAI del Consejo, de 28 de noviembre de 2008, (DOUE L 330, de 9 de diciembre de 2008, pág. 21).

falsario se haya cometido fuera de nuestras fronteras[89]". Si aplicamos dicha interpretación finalista a los delitos cometidos por funcionarios públicos en el extranjero o contra la Administración Pública española (art. 23.3.h LOPJ), los tribunales españoles podrían reclamar su competencia para perseguir aquellas actuaciones cibernéticas realizadas desde el extranjero, cuando desplieguen sus efectos contra bienes o intereses de la Administración Pública española (v. gr., el aprovechamiento por un particular del secreto o la información privilegiada que obtuviere a través de Internet de un funcionario público o autoridad, conforme al art. 418 CP).

Y en segundo lugar, mediante el empleo de la «doctrina de los efectos» como fórmula válida para estimar que el "lugar de comisión del delito" (principio de territorialidad) se corresponde con el lugar del resultado perseguido por el autor del ciberataque, tanto si éste llega a producirse como si no, tal y como ha sido interpretado el delito de favorecimiento de la inmigración ilegal establecido en el art. 318 bis CP. El Tribunal Supremo estima que tal tipo penal es un delito de simple actividad que sanciona cualquier conducta que directa o indirectamente promueva o favorezca la inmigración ilegal, que se consuma por la realización de los actos de promover, favorecer o facilitar el tráfico ilegal o la inmigración clandestina de personas "desde, en tránsito o con destino a España (…), siendo irrelevante que los inmigrantes lleguen a acceder a territorio español[90]".

En un primer momento, el criterio utilizado para la determinación de la jurisdicción española fue el principio de jurisdicción universal del art. 23.4 h) LOPJ en relación con el art. 8.7 del Protocolo contra el tráfico ilícito de migrantes por tierra, mar y aire. Sin embargo, posteriormente se ha manejado como criterio de atribución de la jurisdicción penal a los órganos españoles para conocer de esos delitos el principio de territorialidad, con unos criterios que podrían servir de sustento teórico para defender la competencia de nuestros tribunales para el enjuiciamiento de aquellos ciberataques realizados desde el extranjero (lugar de la actividad) pero dirigidos contra nuestro territorio, aunque no se trate de actos contra bienes jurídicos especialmente protegibles a través del principio real de protección del art. 23.3 LOPJ.

En su Sentencia de 3 de enero de 2008[91], el Tribunal Supremo advierte de la legitimidad reconocida internacionalmente para que los Estados tipifiquen determinados delitos que se cometan fuera de su territorio *con miras a la comisión de un delito grave dentro de su territorio*, de modo que "resulta evidente que la migración tenía como objetivo la inmigración en territorio Español, estando tal comportamiento tipificado y teniendo decidido el Estado español la extensión de su jurisdicción al enjuiciamiento de tal hecho". Y en su Sentencia de 23 de enero de 2008[92], el Tribunal Supremo destaca el Derecho Comparado que sostiene que en los casos de tentativa o preparación, el lugar de comisión será tanto el lugar donde se realice la preparación o donde se dé comienzo a la ejecución, "así como el lugar en el que, según la representación del hecho del autor, debía producirse el resultado (no acaecido)", y concluye que *El derecho europeo citado establece, por lo tanto, que en estos casos no corresponde aplicar otro principio que el*

[89] Vid. SSTS de 7 de octubre de 2003 (núm. 1295/2003); de 24 de septiembre de 2004 (núm. 1089/2004); de 26 de enero de 2005 (núm. 66/2005); de 5 de abril de 2006 (núm. 472/2006), de 9 de junio de 2009 (núm. 602/2009); de 18 de abril de 2011 (núm. 386/2011); y de 1 de junio de 2011 (núm. 522/2011).
[90] Vid. SSTS de 21 de junio de 2007 (núm. 628/2007).
[91] STS núm. 1121/2008.
[92] STS núm. 1/2008.

territorial, dado que el delito debe reputarse cometido en el territorio nacional. Las razones que sostienen esta regla especial de aplicación del derecho nacional a los casos que se preparan o que comienzan a ejecutarse para ser cometidos en el territorio del Estado son claras y tienen total paralelismo con las que conforman el criterio de la ubicuidad: el lugar de comisión debe estar determinado no sólo por la ejecución de la acción o el de la producción del resultado, sino también por el lugar en el que el autor piensa atacar el orden jurídico nacional.

En realidad, el Tribunal Supremo no está defendiendo la aplicación del principio de ubicuidad sino el de territorialidad por entender que la conducta que persigue producir sus efectos en territorio español debe entenderse igualmente cometida en España. El salto cualitativo entre ambas sentencias del año 2008 es destacable, pues la última de ellas enarbola el principio de territorialidad para defender la competencia judicial penal de los tribunales españoles en aquellos casos en los que el delito -iniciado o cometido en el extranjero- *amenace claramente el orden jurídico español*, por ser dicho territorio el lugar en donde, según la intención de los acusados, debería producirse el resultado esperado de su acción delictiva, sin necesidad de que el delito cometido sea uno de los enunciados en el art. 23.3 LOPJ. Es decir, el Tribunal Supremo español utiliza, para la determinación de la jurisdicción española, un planteamiento muy similar a la «doctrina de los efectos» manejada por los tribunales estadounidenses, pues identifica el lugar de comisión del delito, no sólo por el lugar donde se pone en marcha o se ejecuta la acción (teoría de la actividad) o por el lugar de producción del resultado (teoría del resultado), *sino también por el lugar en el que el autor piensa atacar el orden jurídico nacional*.

La utilización de esta interpretación teleológica del principio de territorialidad para la determinación del «lugar de comisión», cuando se trata de delitos cometidos a través de Internet, puede resultar muy positiva para que los tribunales españoles reclamen para sí el enjuiciamiento de aquellos ciberdelitos que, cometidos desde el extranjero, hayan provocado o persiguieran la comisión de un delito grave en España contra ciudadanos o intereses españoles, como por ejemplo, aquellas actuaciones concertadas desde el exterior para dañar la economía española, su mercado financiero y bursátil, etc. Al igual que el Principio Real tiene por objeto atribuir a la jurisdicción española el enjuiciamiento de aquellas conductas que desde el extranjero dañan los intereses nacionales, y el Principio de Jurisdicción Universal justifica la persecución en España de crímenes contra la comunidad internacional cuando existan víctimas de nacionalidad española, o se constate algún vínculo de conexión relevante con España, esta doctrina de los efectos garantizaría la perseguibilidad judicial en España de aquellos actos que desde el extranjero persigan *la comisión de un delito grave dentro del territorio español* o traten de *atacar el orden jurídico nacional*.

Somos conscientes de que esta doctrina no impedirá la aparición de conflictos jurisdiccionales entre los tribunales españoles y los tribunales del lugar de la actividad delictiva, pero España podría defender su preferencia por ser el país objetivo del ataque (*target-oriented country*). Tampoco solventaría aquellos supuestos en los que el fin conscientemente perseguido por el ciberdelincuente fuera causar daños en múltiples jurisdicciones (tal y como sucede, por ejemplo, con el envío de *malware* a través del correo electrónico), aunque en este segundo supuesto siempre quedaría la opción de fijar como Jurisdicción competente con carácter preferente el país del lugar desde donde opera el sospechoso, si resulta ser una única jurisdicción.

No obstante, cuando se trata de actuaciones concertadas desplegadas desde diversas jurisdicciones y contra múltiples foros, lo habitual es que, a partir de una operación coordinada internacionalmente, las autoridades judiciales y policiales de cada uno de los países implicados procedan a detener a las personas que actúan desde cada uno de tales Estados. Esta opción (por ej., aplicable a los ataques de denegación de servicio –DDoS- ejecutados desde múltiples jurisdicciones) se aplica por el Tribunal Supremo a los supuestos de pornografía infantil en los que diversos usuarios de programas informáticos de intercambio de archivos han procedido desde múltiples lugares geográficos a descargar y compartir o intercambiar imágenes y videos de contenido pedófilo[93], tras rechazar la existencia de un acuerdo previo de voluntades que supusiera la aplicación de las reglas de conexidad, pues el Tribunal Supremo entiende que cada uno de los imputados despliega una serie de comportamientos que, transgrediendo el mismo tipo penal, no se unifican ni en la acción ni en el resultado, por cometerse en distintos lugares y momentos, y referirse a la remisión o posesión de archivos pornográficos infantiles, con independencia de que se trate de los mismos archivos o no[94]. Si bien esta última argumentación del Tribunal Supremo no sería válida para los ciberataques coordinados, en los que sí suele existir ese acuerdo previo de voluntades, frente a ello podría argüirse la nueva regla del art. 17.1 LECrim que permite no acumular las investigaciones si suponen una excesiva complejidad o dilación para el proceso.

3.3.4. La suma de vínculos de conexión como mecanismo de resolución de conflictos

Finalmente, y para el caso de que no resultara factible establecer una gradación jerárquica de los criterios de distribución de la competencia judicial penal a nivel internacional, otra solución alternativa pasaría por atender a la concurrencia del mayor número de criterios primarios de determinación de la jurisdicción penal (mayor número de vínculos de conexión) como fórmula para evitar resultados injustos con motivo de priorizar el lugar de realización de la conducta por delante del lugar donde se produzca el resultado del delito, o viceversa.

Si la aplicación del principio de territorialidad (entendiendo por tal, tanto el lugar de la acción, como el lugar del resultado) no solventa la concurrencia de jurisdicciones, y no se consensua internacionalmente cuál de esas teorías resulta preferente, quizá pueda resultar ventajoso atender a la concurrencia cumulativa de los demás elementos claves en la delimitación de la jurisdicción. Así por ejemplo, si el país desde donde se lleva a cabo la conducta delictiva y el país donde se produce la mayor parte del resultado lesivo reclaman para sí el enjuiciamiento de los hechos, podría atenderse al principio de personalidad activa como *fórmula de desempate* y atribuir la competencia al Estado cuya nacionalidad posea el sospechoso, si éste es súbdito de uno

[93] En el citado ATS de 23 de noviembre de 2004 se afirma que "se trata de una introducción de pornografía infantil cometida en tres sitios distintos (…). Habrá que concluir que cada uno de estos tres Juzgados es competente para llevar a cabo la encuesta judicial relativa a la propaganda pornográfica introducida en la red de Internet en su respectivo ámbito territorial, sin perjuicio de que en un futuro pudiera acordarse una acumulación de todas en una única causa, lo que se dice como simple juicio de probabilidad, ya que en este momento no existen datos para apreciar conexidad alguna en los términos previstos en el art. 17.2º LECrim".

[94] Vid. los AATS de 22 de octubre de 2008 (rec. 20237/2008); 4 de noviembre de 2009 (rec. 20284/2009); 22 de enero de 2010 (rec. 20454/2009); 19 de febrero de 2010 (rec. 20455/2009); y 17 de junio de 2010 (rec. 20588/2008).

de esos dos países. Para el caso de que éste fuera nacional de un tercer Estado, otro criterio válido de desempate podría ser atender, por ejemplo, optar por el Estado donde resulte más fácil la obtención de las pruebas del delito. De este modo, aquel Estado en el que confluya el mayor número de tales criterios con motivo de la comisión de un delito sería el Estado con el mayor vínculo de conexión con los hechos, y por tanto, la «jurisdicción más apropiada» para el enjuiciamiento de los mismos[95].

[95] Para CORCOY BIDASOLO ("Problemática de la persecución penal de los denominados delitos informáticos: especial referencia a la participación criminal y al ámbito espacio temporal de comisión de los hechos", Revista *Eguzkilore*, núm. 21, diciembre 2007, p. 31), "La solución a esta cuestión de competencia debería solventarse a través del principio de personalidad. Es decir, de entre todos los Estados en principio competentes, sería competente aquel del que sea nacional el autor". No obstante, no compartimos su opinión conforme a la cual "el Estado de origen del sujeto también tiene competencia para juzgar los hechos cometidos en otro Estado, aunque en él no se haya realizado la conducta ni producido los resultados".