PREVENCIÓN Y SOLUCIÓN DE CONFLICTOS INTERNACIONALES DE JURISDICCIÓN EN MATERIA DE CIBERDELINCUENCIA

Ignacio Flores Prada

Profesor de Derecho Procesal. Universidad Pablo de Olavide de Sevilla

FLORES PRADA, Ignacio. Prevención y solución de conflictos internacionales de jurisdicción en materia de ciberdelincuencia. *Revista Electrónica de Ciencia Penal y Criminología* (en línea). 2015, núm. 17-21, pp. 1-40. Disponible en internet: http://criminet.ugr.es/recpc/17/recpc17-21.pdf
ISSN 1695-0194 [RECPC 17-21 (2015), 26 dic]

RESUMEN: La aparición del ciberespacio ha traído consigo nuevas modalidades de criminalidad basadas en la utilización de los sistemas informáticos como medio y como objetivo de la acción delictiva. Debido a la arquitectura de las redes informáticas, la ciberdelincuencia se ha convertido en un fenómeno expansivo y eminentemente transnacional. Sin embargo, la lucha jurídica contra este tipo de criminalidad se asienta todavía hoy, en gran medida, sobre un esquema penal y judicial nacional, territorialmente limitado y heterogéneo. Ello explica la aparición frecuente de procedimientos penales paralelos y de conflictos internacionales de jurisdicción, que afectan negativamente a la eficacia de la tutela judicial, a la duración de los procedimientos y a las garantías procesales, muy señaladamente al principio de *non bis in idem*. En este trabajo se analizan las causas que provocan la aparición de la litispendencia internacional en materia de ciberdelincuencia y se exploran las posibles vías para su prevención y solución, apostando por la cooperación internacional y por la armonización sustantiva y procedimental como instrumento más adecuado para identificar en cada caso la jurisdicción nacional idónea. Este proceso de cooperación y armonización normativa en materia jurisdiccional debe asentarse, fundamentalmente, sobre dos medidas complementarias, En primer, y con vocación preventiva, resulta imprescindible un acuerdo sobre los criterios para la identificación de la jurisdicción penal nacional con competencia preferente en la persecución de la ciberdelincuencia transnacional. En segundo lugar, como herramienta de solución de los problemas de convergencia jurisdiccional, conviene proponer la adopción de un procedimiento simplificado que permita adoptar consensuadamente la jurisdicción idónea en casos de litispendencia internacional penal o conflictos negativos de competencia en procedimientos contra la ciberdelincuencia transfronteriza.

PALABRAS CLAVE: Ciberespacio. Ciberdelincuencia. Competencia judicial transnacional. Cooperación internacional. Conflictos de jurisdicción. Concurrencia jurisdiccional. Jurisdicción idónea. Litispendencia internacional. Procedimiento consensual de solución de conflictos. Redes informáticas.

ABSTRACT: The emergence of cyberspace has brought new forms of criminality based upon the use of computer systems as a means and as an objective

of the criminal action. Due to computer networks' architecture, cybercrime has become an expansive and highly transnational phenomenon. Nevertheless, the legal struggle against this type of crime, largely, is still based upon a territorially limited and heterogeneous national criminal and judicial framework. This explains the frequent existence of parallel criminal proceedings and international conflicts of jurisdiction, which adversely affect the efficacy of judicial protection, the length of the procedures and due process, most particularly, the principle *non bis in idem*. In this paper we analyse the causes of the emergence of international lispendence on cybercrime and we examine the possible ways for its prevention and resolution. All of that is done relying on the international cooperation and on the substantive and procedural harmonization as the most appropriate instrument to identify in each case the most suitable national jurisdiction. This process of regulatory harmonization and cooperation in jurisdictional field must be based, primarily, upon two complementary measures. First, and with a preventive vocation, it is indispensable the existence of an agreement about the criteria for the identification of national criminal jurisdiction with preferential competence in prosecuting transnational cybercrime. Second, as a tool for solving problems of jurisdictional convergence, it should be proposed the adoption of a simplified procedure that allow to decide by consensus the ideal jurisdiction over criminal international lispendens or over negative conflicts of competence in proceedings against cross-border cybercrime.

KEYWORDS: Consensual dispute resolution procedure. Cyberspace. Cybercrime. Ideal jurisdiction / Most suitable national jurisdiction. International judicial competence. International cooperation. International lispendence. Jurisdictional conflicts. Jurisdictional convergence. Networks.

Fecha de publicación: 26 diciembre 2015

---

1. **El ciberespacio**

Desde su origen y hasta hace sólo unos años, el Derecho ha tomado como referencia para seleccionar conductas la única dimensión espacial conocida: la del mundo físico o real. En él suceden cosas visibles, perceptibles por los sentidos; las personas nacen realmente, tienen su identidad, comercian, forman familias, pagan impuestos, hacen testamentos y mueren de una manera pacífica o violenta. Desde finales del siglo XX, este mundo analógico —basado en los átomos o en la materia— convive con otro espacio, que se desarrolla en una dimensión distinta,

conocida como mundo digital o virtual[1]. Aunque no podamos verlo físicamente existe, y lo que en él sucede afecta de modo cada vez mayor al mundo físico o real. Se trata de una nueva dimensión del espacio formada por bits, cables de fibra óptica, satélites y terminales, que han creado un espacio en red convertido en un *lugar* de convivencia, comunicación e interrelación, cuyo lenguaje y cuyas claves son bien diferentes a las que rigen el mundo analógico.

Como ha explicado Negroponte[2], un bit no tiene color, tamaño ni peso, y viaja a la velocidad de la luz. Es el elemento más pequeño en el ADN de la información. Consiste en combinaciones binarias compuestas exclusivamente por dos números, el 1 y el 0. Los bits han sido siempre el elemento básico de la computación digital, pero durante los últimos veinticinco años hemos ampliado enormemente nuestro vocabulario binario hasta poder representar mucho más que números. Hemos conseguido digitalizar cada vez más tipos de información, auditiva y visual por ejemplo, reduciéndolos de igual manera a unos y ceros.

Los bits circulan, cada vez más comprimidos y más rápidamente, a través de los cables de fibra óptica que conectan los sistemas informáticos dentro del gran entramado de comunicaciones que es Internet[3]. Esta nueva tecnología no sólo permite transportar en segundos grandes cantidades de información, sino que además no se ve afectada por las interferencias y resulta muy difícil interceptar la información que transporta; una tecnología que hace posible la idea de una red transfronteriza no jerarquizada de comunicaciones y transmisión digital de información. Dentro de la Red, cada ordenador que se conecta a Internet se identifica por medio de lo que se conoce como dirección IP. Ésta se compone de cuatro grupos de números comprendidos entre el 0 y el 255 y separados por puntos. El usuario de Internet no necesita conocer ninguna de estas direcciones IP para comunicarse. Las direcciones las usan los ordenadores en la comunicación por medio del denominado protocolo TCP/IP de manera transparente para el usuario. Éste tan solo debe conocer el *nombre de dominio* de su interlocutor, es decir, su dirección normal de Internet del tipo de las que estamos acostumbrados a ver[4].

A través de la Red, la información no viaja toda junta y directamente por una sola

[1] Sobre el nuevo espacio digital y el concepto de ciberespacio vid. ampliamente LESSIG, *El código y otras leyes del ciberespacio*, Taurus, Madrid, 200, págs. 345 y ss.

[2] Vid. *El mundo digital*, Barcelona, 1999, pág. 28.

[3] La fibra óptica es, en palabras de TERCEIRO, *La sociedad digital*, Alianza, Madrid, 1996, pp. 70 y ss., un cable de vidrio más fino que un cabello, diseñado para transmitir luz, gracias a la confluencia de dos tecnologías: el láser y la fibra de vidrio. El material que utiliza la fibra de vidrio y la energía lumínica que

[2] Vid. *El mundo digital*, Barcelona, 1999, pág. 28.

[3] La fibra óptica es, en palabras de TERCEIRO, *La sociedad digital*, Alianza, Madrid, 1996, pp. 70 y ss., un cable de vidrio más fino que un cabello, diseñado para transmitir luz, gracias a la confluencia de dos tecnologías: el láser y la fibra de vidrio. El material que utiliza la fibra de vidrio y la energía lumínica que discurre por ella la distinguen sustancialmente de todos los antecesores en materia de soportes de comunicación.

[4] Sobre el funcionamiento de Internet vid. ALONSO, «La investigación policial de los delitos relacionados con nuevas tecnologías», *Estudios Jurídicos. Ministerio Fiscal* III, 2001, p. 613.

línea o camino hasta el destinatario, sino que se fracciona en pequeños paquetes que son enviados por separado cada uno por el camino que encuentre libre en ese momento, dependiendo de la saturación de rutas o posibles atascos, a través de varios dispositivos de interconexión de redes denominados *routers*, y sólo cuando han llegado todos los paquetes al final, allí se ordenan y la información está disponible. Los instrumentos que permiten enviar y recibir información a través de la Red son los módems y las tarjetas de red, que cumplen la función de empaquetar y desempaquetar la información, conectando la terminal con los canales de conexión.

Muy someramente descrito, es fácil advertir que el nuevo espacio digital permite múltiples aplicaciones en el almacenamiento, tratamiento, codificación y transmisión de la información. Internet, que nació en el ámbito militar como un sistema de conexiones entre ordenadores con el fin de garantizar la seguridad y la continuidad en las transmisiones, se ha convertido en la actualidad en una inmensa Red compuesta de servidores, clientes, nodos, redes locales, cables, satélites, etc., que ha superado con creces y a una velocidad de vértigo las primeras previsiones sobre sus utilidades[5].

El presente del ciberespacio, y lo que hoy puede adivinarse sobre su futuro, nos sitúa ante una revolución ciertamente espectacular[6]. Internet ya ocupa un espacio creciente en el mundo económico, comercial y financiero, en el que las transacciones, los acuerdos y los movimientos de capitales, bienes y servicios circulan a velocidad de la luz convertidos en combinaciones de bits[7]. De igual modo, la Red se

[5] El origen, como recuerda MUÑOZ MACHADO, *La regulación de la red. Poder y Derecho en Internet*, Taurus, Madrid, 2000, pág. 31, se debe a una idea de Paul Baran aprovechando la técnica del desglose y transmisión fragmentada de paquetes digitales; la idea de aquél, concebida en la *Rand Corporation* en 1962, se refería al diseño de un sistema de comunicaciones invulnerable a un ataque nuclear. El desarrollo lo hizo la *Rand Corporation* a petición de las fuerzas aéreas de Estados Unidos. Se basa en los principios y las ventajas de una estructura de malla muy descentralizada en la que están conectados muchos ordenadores. Dada esta estructura de red, en la que no existe ningún punto central estratégicamente decisivo para el gobierno del conjunto, es posible asegurar siempre el funcionamiento del sistema aunque una parte del mismo fuera destruido. En tal caso, los ordenadores restantes serían capaces de mantener la conexión entre ellos utilizando la parte de la red conservada, manteniendo plenamente su funcionalidad. El tejido de esa peculiar telaraña hace difícil la censura de los mensajes o el control o intervención de las informaciones que circulan por ella. Someramente sobre el funcionamiento y arquitectura de Internet y sobre sus conceptos básicos vid. el claro trabajo de PIQUERES CASTELLOTE, «Conocimientos básicos en internet y utilización para actividades ilícitas», en *Delitos contra y a través de las nuevas tecnologías. ¿Cómo reducir su impunidad?*, en Cuadernos de Derecho Judicial, CGPJ, Madrid, 2006, págs. 42 y ss.

[6] Como señala QUINTERO, «Internet y propiedad intelectual», en *Internet y Derecho Penal*, Cuadernos de Derecho Judicial, Madrid, 2001, págs. 369 y 370 «Internet no es una simple progresión en la evolución tecnológica, sino un cambio revolucionario en los modelos de relaciones sociales, que sirve a la fluidez de los intercambios comerciales y de todo tipo». Una segunda "Revolución industrial" en palabras de ABOSO y ZAPATA, *Cibercriminalidad y derecho penal*, B de F editorial, Montevideo-Buenos Aires, 2006, pág. 4. Sobre la dimensión de la revolución tecnológica y los retos que supone para el jurista vid. LÓPEZ ORTEGA, «Libertad de expresión y responsabilidad por los contenidos en Internet», *Internet y Derecho Penal*, Cuadernos de Derecho Judicial, Madrid, 2002. Como la nueva *era informática* ha sido calificada por MONTERDE FERRER, «Especial consideración de los 'atentados por medios informáticos contra la intimidad y la privacidad'», en *Delitos contra y a través de las nuevas tecnologías. ¿Cómo reducir su impunidad?*, Cuadernos de Derecho Judicial, CGPJ, Madrid, 2006, pág. 194

[7] Vid. SALOM CLOTET, "Delito informático y su investigación", en *Delitos contra y a través de las*

apropia cada vez a mayor velocidad de los canales de información, de las telecomunicaciones, de las comunicaciones interpersonales, de la oferta de ocio, cultura, arte, de la actividad científica, de la difusión del pensamiento, de los medios informativos, incluso de la política, amenazada en su concepción tradicional por la posible implantación de cibervoto y las consultas vinculantes a través de Internet[8].

Las nuevas tecnologías digitales y de la comunicación, muy especialmente Internet, han creado una nueva dimensión del espacio[9]. Tal y como ha explicado Lessig[10], «el ciberespacio es un lugar. La gente vive en él. Allí experimentan todos los tipos de cosas que experimentan en el espacio real. Alguna gente experimenta incluso más. Y esta experiencia no es como la de un individuo aislado jugando a un sofisticado juego de ordenador. Las personas experimentan la vida en Internet en grupos, en comunidades, entre extraños y entre personas que incluso llegan a conocer y con quienes llegan a veces a congeniar y a vivir historias de amor. Mientras están en aquel lugar, en el ciberespacio, siguen estando también aquí. Se encuentran frente a una pantalla de ordenador, comiendo patatas fritas, ignorando el teléfono. Están en su buhardilla, a altas horas de la noche, mientras sus parejas duermen. Están en el trabajo, en cibercafés y en laboratorios informáticos. Viven sus vidas en el ciberespacio mientras están aquí y entonces, llegado un momento, se desconectan y entonces se encuentran únicamente aquí. Se levantan de delante de sus pantallas, un poco aturdidos, y le dan la espalda. Acaban de regresar. Entonces ¿*dónde* están cuando están en el ciberespacio?»[11].

2. **Ciberdelincuencia y conflictos internacionales de jurisdicción**

Una de las características más relevantes del ciberespacio consiste en su posibilidad de interactuación constante con el espacio real. En esta posibilidad de interactuación estriba en buena medida la fuerza de las redes informáticas y de ella

nuevas tecnologías. ¿Cómo reducir su impunidad?, en Cuadernos de Derecho Judicial, CGPJ, Madrid, 2006, pág. 94.

[8] Hoy es una realidad lo que hace sólo pocos años pronosticaba gráficamente Bill GATES al afirmar en *Camino al futuro*, MacGraw-Hill, 2º ed., Madrid, 1996 —consulto la edición digitalizada y disponible en pdf a través de Internet en la dirección http//books/openlibra.com, pág. 8—, que: «llegará un día, no muy distante, en que seremos capaces de dirigir negocios, de estudiar, de explorar el mundo y sus culturas, de hacer surgir algún gran entretenimiento, hacer amigos, asistir a mercados locales y enseñar fotos a parientes lejanos sin abandonar nuestra mesa de trabajo o nuestro sillón. No abandonaremos nuestra conexión a la red ni nos la dejaremos en la oficina ni en el aula. Esta red será algo más que un objeto que portamos o un dispositivo que compremos. Será nuestro pasaporte para un modo de vida nuevo y mediático».

[9] Una sociedad paralela a la meramente física, como señala RODRÍGUEZ BERNAL, «Los cibercrímenes en el espacio de libertad, seguridad y justicia», en *Revista de Derecho Informático*, núm. 103, 2007, pág. 3.

[10] Vid *El Código* ..., cit., p. 348.

[11] Sobre el concepto y características del ciberespacio vid. ampliamente MIRÓ LLINARES, «La oportunidad criminal en el ciberespacio. Aplicación y desarrollo de la teoría de las actividades cotidianas para la prevención del cibercrimen», en *Revista Electrónica de Ciencia Penal y Criminología* (en línea), 2011, núm. 13-07, págs. 5 y ss.

deriva, también, su potencialidad ofensiva sobre bienes jurídicos protegidos en el espacio real, pero vulnerables a ataques con modernas conductas procedentes de un espacio nuevo y con enorme proyección futura[12]. En este sentido, cabe afirmar que el ciberespacio ha generado la aparición de nuevas conductas delictivas vinculadas a las nuevas tecnologías de la comunicación y la información, al tiempo que ha aumentado considerablemente la vulnerabilidad de determinados bienes jurídicos, señaladamente los relacionados con la intimidad, el honor, la propiedad, la autodeterminación informática, la libertad sexual, y la seguridad del mercado o del consumo[13].

La complejidad de las nuevas tecnologías informáticas y la variedad de conductas y posibilidades de afectación de bienes jurídicos a través de las mismas dificultan enormemente la tarea de delimitar y de designar con precisión estas nuevas formas de delincuencia[14]. Sobre los diferentes ámbitos y fórmulas de denominación que se utilizan por la doctrina[15] y por los textos internacionales[16], es

[12] Para MIRÓ LLINARES, «La oportunidad criminal…», cit., pág. 3, la cibercriminalidad «se realiza en un nuevo ámbito o espacio con características estructurales intrínsecas y extrínsecas tan distintas a las del espacio físico en el que se ejecuta la delincuencia tradicional, que obliga a una revisión criminológica de la explicación del evento delictivo, así como una adaptación de las normas jurídicas para una mejor prevención». Según señala RIBAS, *Aspectos jurídicos del comercio electrónico en Internet*, Aranzadi, Navarra, 1999, pág. 125, el ciberespacio es un mundo virtual en el que los defectos, miserias y malos hábitos del ser humano se reproducen con la misma fidelidad que las virtudes. El efecto de aldea global generado por el entramado de redes y la proliferación de nodos en todo el planeta ayuda a la difusión inmediata de los mensajes y permite el acceso a cualquier información introducida en la Red. A las reconocidas ventajas que ello supone se unen las distorsiones y los malos usos que pueden tener lugar en el sistema y que confirman una vez más que el mal no está en el medio utilizado sino en la persona que lo utiliza. Sobre la potencialidad ofensiva de la criminalidad informática vid. también CORCOY BIDASOLO, «Problemática de la persecución penal de los denominados delitos informáticos: particular referencia a la participación criminal y al ámbito espacio temporal de comisión de los hechos», en *Eguzkilore*, núm. 21, San Sebastián, diciembre de 2007, (ed. en línea) pág. 8.

[13] Vid. ampliamente, MORÓN LERMA, *Internet y Derecho Penal: hacking y otras conductas ilícitas en la Red*, (2ª edición), Aranzadi, Navarra, 2002. Para MATA, *Delincuencia informática y derecho penal*, Edisofer, Madrid, 2001, pág. 17, las enormes potencialidades que se abren en el tratamiento automatizado de datos, tienen un reverso que son los riesgos que se introducen para facilitar la realización de hechos que afecten a los intereses fundamentales de las personas. Es decir, la informática o, en general, el tratamiento automatizado de datos se presenta como factor criminógeno, pues permite el acceso y el manejo de bases de datos, programas de cualquier género, en ocasiones de forma lesiva para intereses básicos de las personas y de la sociedad, siendo más costosa la averiguación del autor y la prueba de los hechos debido a la naturaleza del procedimiento informático.

[14] Como ha puesto de relieve PÉREZ LUÑO, *Manual de Informática y Derecho*, Barcelona, 1996, pág. 70, la heterogeneidad de supuestos agrupados bajo la rúbrica del «*delito informático*» para hacer referencia a hipótesis que, en muchas ocasiones no son delitos en sentido estricto, ha determinado que en algunas culturas jurídicas se opte por la denominación más genérica y apropiada de «*criminalidad informática*». Así, en el ámbito anglosajón se ha popularizado la denominación de *Computer Crime*, y en el germano la expresión *Computerkriminalität*. Sobre la denominación de esta modalidad de delincuencia vid. más recientemente MIRÓ LLINARES, «La oportunidad criminal…», cit., pág. 3.

[15] Algunas definiciones desde la doctrina pueden encontrarse en CRUZ DE PABLO, *Derecho penal y nuevas tecnologías. Aspectos sustantivos*, Grupo difusión, Madrid, 2006, págs. 19 y ss.

[16] Según Naciones Unidas «El concepto de "delitos informáticos" o términos similares como "delitos cibernéticos" ha sido un tema de debate durante los últimos 30 años. El prototipo se remonta a un informe del Instituto de Investigación de Stanford y reapareció en forma ligeramente modificada en 1979 y en 1989. El esquema de organización se utilizó ampliamente en artículos posteriores sobre la delitos cibernéticos: la

necesario partir de un concepto y de una delimitación inicial de lo que consideramos delincuencia relacionada con las tecnologías de la información y la comunicación. La denominación que en este trabajo usaremos es ciberdelincuencia[17], siendo su ámbito el de los delitos que se cometen contra o a través de los sistemas informáticos. Por sistema informático se entiende todo dispositivo aislado o conjunto de dispositivos interconectados o relacionados entre sí, cuya función, o la de alguno de sus elementos sea el tratamiento automatizado de datos en ejecución de un programa[18].

Es precisamente la arquitectura de los sistemas informáticos la que explica que la regulación de las redes de comunicaciones digitales esté resultando una tarea compleja para los ordenamientos jurídicos, basados tradicionalmente en la doble dimensión —física y nacional— del espacio de conducta. En este sentido, las redes digitales —señaladamente Internet— plantean, al menos, tres grandes dificultades para su regulación por los modernos derechos nacionales: la universalidad, la horizontalidad, y la dependencia del código técnico. Por un lado, Internet está construida y funciona como una red sin fronteras, tal suerte que cualquier punto de conexión permite el acceso, en principio y con carácter general, a todo el sistema. La territorialidad o la nacionalidad es un factor muy diluido —cada vez más— en el funcionamiento de Internet, de tal modo que las limitaciones o restricciones de acceso o de comunicación resultan difíciles de lograr o de mantener por las autoridades en un espacio nacional determinado[19]. En segundo lugar, la arquitectura de la Red es, esencialmente, horizontal. Internet, pensada inicialmente para funciones militares y basada en la idea de descentralización, funciona como una red cuya operatividad no depende de un centro lógico de decisión, sino que cada terminal permite mantener, en sí, toda la potencialidad del sistema. La tercera dificultad relevante tiene que ver con el código técnico que Internet utiliza, y del que depende, en buena medida, la mayor o menor regulabilidad de la Red. En palabras de LESSIG[20], la regulabilidad de la Red depende básicamente del código

computadora como sujeto de un delito, o la computadora como un instrumento (la cuarta función, propuesta en 1973, la computadora como símbolo, parece haber desaparecido en los años 80). Una reformulación útil de este modelo conceptual es considerar los delitos informáticos como una conducta proscrita por la legislación y/o la jurisprudencia que a) ataca a las propias tecnologías de la computación y las comunicaciones; b) incluye la utilización de tecnologías digitales en la comisión del delito; o c) incluye la utilización incidental de las computadoras en la comisión de otros delitos y, en consecuencia, la computadora pasa a ser una fuente de datos digitales probatorios.»

[17] Es el término utilizado por el Convenio del Consejo de Europa de 2001 (Budapest), también empleado por el Convenio Iberoamericano de Cooperación sobre Investigación, Aseguramiento y Obtención de Prueba en materia de Ciberdelincuencia (2014), definiéndola este último tratado (art. 2.1) como «Cualquier forma de criminalidad ejecutada en el ámbito de interacción social definido por el uso de las Tecnologías de la Información y la Comunicación».

[18] La definición de "sistema informático" está tomada del art. 1.a del Convenio del Consejo de Europa sobre Ciberdelincuencia de 2001.

[19] Vid. RODRÍGUEZ BERNAL, «Los cibercrímenes...», cit., págs. 5 y ss. En el mismo sentido CORCOY BIDASOLO, «Problemática de la persecución…», cit., págs. 8 y 9.

[20] Vid. *El código*…, cit., pág. 207.

que permite funcionar al propio sistema: «no es la naturaleza quien determina el ciberespacio sino el código. El código no es constante. Cambia. Y, en estos momentos, está cambiando en la dirección de hacer más regulable el ciberespacio. Aunque también podría cambiar en la dirección contraria, la de hacer menos regulable el ciberespacio. El modo en que el código cambia depende de los autores del código. Y el modo en que los autores de código lo modifican puede depender de nosotros».

De entre los rasgos característicos de las nuevas redes informáticas, en este trabajo nos interesa fundamentalmente uno: la supraterritorialidad[21]. Esta propiedad de los sistemas digitales permite que la información circule con enorme velocidad por un espacio virtual mundial, que no cuenta con puntos físicos claros de referencia para ubicar las conductas ni sus efectos —deslocalización[22]—, ni con fronteras que definan los espacios jurídicos y jurisdiccionales nacionales —efecto transfronterizo—[23]. La nueva dimensión que supone la aparición del ciberespacio ha desbordado claramente los principios de localización delictiva tradicionales, basados en el principio de territorialidad. En el mundo físico, el delito se produce en un lugar más o menos determinado del territorio, o al menos cabe partir del territorio para asignar la jurisdicción nacional y la competencia interna en materia penal. Sin embargo, el espacio digital el territorio no cuenta, o al menos no cuenta como en el espacio físico[24]. Lo que cuenta en la Red son los terminales, los servidores, los proveedores, las conexiones y la información circulante por todo el mundo. Los anclajes de la Red con el mundo físico no siempre son fáciles de establecer; más aún, puede decirse que el desarrollo técnico del ciberespacio

[21] Como ha señalado WALL, *Cybercrime: the transformation of crime in the information age*, Polity Press, Cambridge, 2010, pág. 4 (cit. por MIRÓ LLINARES, «La oportunidad criminal…», cit., pág. 3), los delitos que integran la llamada cibercriminalidad ya no preocupan por tener como elemento característico el realizarse desde ordenadores, sino por el hecho de que tales sistemas informáticos estén conectados en un ámbito de comunicación transnacional-universal, el ciberespacio, y porque sea en ese nuevo «lugar» en el que, desde cualquier espacio físico, ubicado en cualquier nación, se cometen infracciones que pueden afectar en lugares distintos y simultáneamente, a bienes jurídicos tan diversos como el patrimonio, la intimidad, la libertad y la indemnidad sexuales, el honor, la dignidad personal, la seguridad del Estado o la libre competencia, entre otros muchos».

[22] Vid. MIRÓ LLINARES, «La oportunidad criminal…», cit., págs. 10 y ss.

[23] Como apunta GALÁN MUÑOZ, «La internacionalización de la represión y la persecución de la criminalidad informática: un nuevo campo de batalla en la eterna guerra entre prevención y garantías penales», en *Revista Penal*, La ley, núm. 24, julio de 2009, pág. 90, «los enormes avances tecnológicos y la facilidad del tránsito de personas, de capitales y de información a nivel mundial, han llevado a que ningún país del mundo pueda controlar todas las actividades que tienen o pueden tener efectos, incluso delictivos, dentro de sus fronteras. Terrorismo, tráfico de drogas, blanqueo de capitales, tráfico ilegal de personas, etc. Los ejemplos de delincuencia transnacional son múltiples y cada vez más numerosos. Sin embargo, si hay un campo en el que se ha mostrado lo inútiles que pueden ser los esfuerzos exclusivamente nacionales por controlar los peligros que genera el uso de las nuevas tecnologías, es en el ámbito de lo que se ha venido a denominar como delincuencia o criminalidad informática.»

[24] La aterritorialidad es una característica natural de la red de redes, vid. CLIMENT BARBERÁ, «La justicia penal en Internet. Territorialidad y competencias penales», *Internet y Derecho Penal*, Cuadernos de Derecho Judicial, Madrid, 2002, pág. 657.

proporciona cada vez mayor nivel de "deslocalización", que pugna con el interés de los Estados para lograr una mayor "regulabilidad" de la Red[25]. Basta con reparar en el extraordinario desarrollo que en los últimos años está teniendo el almacenamiento en la nube —*cloud computing*— para hacerse una idea de las dificultades del Derecho para situar el lugar físico en el que se desarrollan buena parte de las operaciones que a diario realizamos a través de nuestros ordenadores o teléfonos móviles[26].

Como ha puesto de relieve Muñoz Machado[27], mientras que Internet se ha convertido en un medio de comunicación mundial, el espacio por el que extiende sus dominios es plurijurisdiccional. Está repartido entre miles de órganos judiciales que desarrollan sus funciones en ámbitos territoriales concretos que llegan a alcanzar, como máximo, el espacio mismo del Estado al que pertenecen[28].

Las fronteras nacionales, señala Lezertua[29], constituyen un obstáculo evidente para la detección, investigación, persecución y castigo de los autores de ciberdelitos. Mientras que Internet está configurado como un espacio sin fronteras para los delincuentes, las autoridades encargadas de investigar y reprimir tales delitos —jueces, fiscales y policías— se encuentran confinadas en el interior del territorio definido por las fronteras nacionales.

En este contexto, la aparición de supuestos de litispendencia internacional y de los consiguientes conflictos de jurisdicción en la persecución y castigo de la ciberdelincuencia, es más que previsible ante la falta de una autoridad internacional jurisdiccional, y de normas eficaces de armonización sustantiva y procesal —señaladamente de normas que fijen la competencia territorial internacional— capaces de contribuir a la

[25] Vid. RODRÍGUEZ BERNAL, «Los cibercrímenes...», cit., págs. 8 y ss.

[26] De acuerdo con la definición establecida por el Instituto Nacional de Estándares y Tecnología de Estados Unidos, el *cloud computing* es un modelo que permite el acceso viable a las redes bajo demanda de un conjunto compartido de recursos de computación configurable, repartidos en servidores no físicamente vinculados, que pueden ser rápidamente abastecidos y administrados con un mínimo esfuerzo de gestión o interacción del prestador de servicios. Como señala VELASCO SAN MARTÍN, *La jurisdicción y competencia*…, cit., pág. 136, el *cloud computing* supone un cambio de paradigma sobre el uso de servicios basados en la web, que permite y facilita a las empresas, gobiernos y usuarios utilizar software, sistemas de información y datos —albergados en distintos servidores de internet y ubicados físicamente en distintos lugares— en lugar de ser guardados y ubicados en sistemas de cómputo personales o servidores locales.

[27] Vid. *La regulación*..., cit., pág. 221.

[28] Según afirma FERNÁNDEZ TERUELO, *Cibercrimen. Los delitos cometidos a través de Internet*, Constitutio Criminalis Carolina, Oviedo, 2007, pág. 13, «el derecho penal y el procesal (penal) vigentes, así como los principios garantistas inherentes a ambos, han sido construidos, en esencia, sobre la base de un modelo de criminalidad física, marginal e individual. Frente a ello, con la aparición de Internet, los distintos organismos encargados de su represión se han debido enfrentar a un cauce de ejecución delictiva que cuestiona plenamente muchos de los axiomas vigentes. Así, el medio Internet determina, en primer lugar, una notable y especial dificultad para la detección y persecución del delito debido, entre otros factores, a las posibilidades de anonimato que ofrece el mismo, a la escasa conciencia de los usuarios respecto a la necesidad de mantener una serie de medidas de seguridad, o al carácter transnacional de algunas conductas delictivas»

[29] Vid. «El Proyecto de Convenio sobre el Cibercrimen del Consejo de Europa», *Internet y Derecho Penal*, Cuadernos de Derecho Judicial, Madrid, 2002, pág. 24.

determinación de la jurisdicción nacional idónea en caso de tramitación de procedimientos paralelos por parte de diferentes jurisdicciones nacionales.

Conviene tener en cuenta que la arquitectura de Internet se diseñó, precisamente, para que funcionara como una estructura anárquica, formada por conexiones, nodos y sistemas sin un punto central de control, de tal forma que los circuitos por los que circula la información son "horizontales", imprevisibles por su automaticidad, y universales por la disposición y expansión de la Red. Como recuerda MORALES GARCÍA[30], Internet responde en todos los rincones del planeta a protocolos de transmisión y recepción de datos de carácter universal, lo que facilita que el flujo de datos no sea homogéneo, sino que los mismos circulen de un lado a otro del globo para atravesar distancias de apenas unos metros entre el ordenador que envía y el que recibe. La determinación del lugar de comisión del delito juega entonces un papel fundamental en la determinación de la jurisdicción nacional —primero— y en la asignación del tribunal concreto —después— que habrá de asumir la competencia para el conocimiento de los delitos transfronterizos cometidos a través de las redes informáticas. Se trata, sin embargo, de una tarea extraordinariamente difícil, no solo por la propia dificultad de determinar los anclajes físicos de la ciberdelincuencia, sino también porque este tipo de criminalidad presenta por lo general características que favorecen la concurrencia de jurisdicciones, como la posibilidad de duplicidad o multiplicidad de lugares físicos en los que situar la actividad —lugar donde actúa el actor, lugar donde se encuentra su terminal, lugar donde se activan los programas informáticos a través de los que actúa, lugar donde se encuentran los servidores o los proveedores de servicios—, o la multiplicidad de lugares en los que, con frecuencia, cabe situar el resultado de la conducta —delitos contra la propiedad intelectual, delitos contra el honor, estafas múltiples, etc.—.

En conjunto, puede afirmarse que la aparición del ciberespacio ha hecho nacer nuevas formas de delincuencia y ha aumentado la vulnerabilidad de ciertos bienes jurídicos. Además, y desde el punto de vista procesal, la arquitectura supraterritorial de las redes informáticas provoca importantes problemas para la determinación de la jurisdicción nacional competente, resultando previsiblemente frecuentes los supuestos de litispendencia internacional[31]. Un escenario que debe ser evitado porque los conflictos internacionales de jurisdicción provocan, entre otros efectos negativos, tensiones entre los Estados, perjudican una persecución eficaz de esta tipo de delincuencia, impiden de ordinario una adecuada satisfacción de la víctima y pueden, en último término, afectar a garantías básicas como el derecho a la tutela judicial efectiva, o al principio del *non bis in idem*[32]. Sin embargo, y a pesar de lo

[30] Vid. «Criterios de atribución... », cit., págs. 237 y 238.

[31] Vid. RODRÍGUEZ BERNAL, «Los cibercrímenes...», cit., págs. 9 y ss.

[32] Se trata, como es sabido, de un principio fundamental del derecho penal internacional y de los derechos penales internos, conforme al cual un acusado no puede ser juzgado más de una vez por los mismos hechos, aun cuando haya sido absuelto en alguna jurisdicción.

dicho, la realidad demuestra que, en materia de ciberdelincuencia, la determinación clara del lugar de producción del delito y la identificación de la jurisdicción idónea para castigarlo son cuestiones que, por el momento, no han recibido una respuesta razonablemente satisfactoria ni en términos dogmáticos ni en términos normativos[33].

3. **Respuestas jurisprudenciales**

3.1. *El caso Megaupload*

El 21 de marzo de 2005 Kim Dotcom, ciudadano alemán con residencia en Nueva Zelanda, funda Megaupload Inc. La empresa, con domicilio social en Hong Kong, gestionaba un conjunto de plataformas en Internet dedicadas al intercambio de archivos de imagen y sonido. Estas plataformas se basaban en un sistema de transmisión de archivos, de modo que cualquiera podía subir a la plataforma sus archivos y ponerlos a disposición de otros usuarios. La empresa ingresaba fondos por publicidad y por ofertas de suscripción con ventajas en velocidad de descarga. A su vez, los usuarios que subieran los archivos más demandados eran premiados por la empresa con cantidades entre 50 y 1000 dólares por archivo.

En el momento en el que comienza su intervención judicial, la empresa contaba con tres servidores ubicados en Canadá, Estados Unidos y Holanda. El equipo directivo estaba integrado, además de su creador, por seis personas de diversas nacionalidades y con residencias en distintos lugares del mundo. Se calcula que la empresa obtuvo beneficios por valor de ciento cincuenta millones de dólares, contando sólo en el año 2011 con más de ciento ochenta millones de usuarios registrados.

El 19 de enero de 2012, un tribunal federal de Virginia, lugar donde se situaba uno de los servidores que ofrecía soporte a Megaupload, ordenó, a instancias del FBI, el cierre de sus plataformas, la intervención de sus bienes y cuentas, y la detención de sus responsables, adoptándose además medidas cautelares en Nueva Zelanda, Holanda, Alemania, Filipinas, Reino Unido, Canadá y Estados Unidos[34]. Los cargos que motivaron la intervención fueron: violación de la propiedad intelectual, pertenencia a organización criminal, blanqueo de capitales y defraudación, calculándose en unos 500 millones de dólares las pérdidas producidas a los titulares de los derechos defraudados.

[33] Sobre estas cuestiones puede consultarse el trabajo de CLIMENT BARBERÁ, «La justicia penal…», cit., págs. 647 y ss.

[34] El acta de acusación, de 5 de enero de 2012, se dirigió contra Megaupload Limited, Vester Limited y contra Kim Dotcom, Fin Batato, Julius Bencko, Sven Echternach, Mathias Ortmann, Andrus Nomm y Bram Van Der Kolk. El acta de acusación ante el Gran Jurado presentada por la fiscalía federal de Estados Unidos puede consultarse en http://www.washingtonpost.com/wp-srv/business/documents/megaupload_indictment.pdf

Con independencia de cuál sea finalmente la solución judicial de este proceso[35], interesa destacar que estamos ante un caso en el que aparecen con toda claridad los problemas jurídicos derivados de la dualidad espacio físico y ciberespacio. En primer término, y a nivel sustantivo, surgen importantes interrogantes sobre la falta de armonización penal de las legislaciones nacionales de países que han colaborado judicialmente con Estados Unidos en las detenciones y en la obtención de fuentes de prueba. El hecho de que el intercambio personal de archivos a través de sistemas de links de enlace personal no fuese delito en alguno de los países —Nueva Zelanda entre ellos— puede poner en cuestión el uso en Estados Unidos de la información obtenida en estos países, incluso el propio trámite de la extradición de las personas reclamadas por infracción del principio de doble incriminación.

En segundo lugar, y desde el punto de vista procesal, los principales problemas surgen al examinar la idoneidad de la jurisdicción norteamericana para asumir la competencia en este proceso. Mientras el tribunal federal de Virginia sostiene su competencia en función de la ubicación de uno de los servidores en Estados Unidos y del flujo de transacciones comerciales —ingresos, transferencias, gestiones de pagos con *pay pal* y donaciones— con sede en entidades financieras en Virginia o con destino a ciudadanos o entidades domiciliadas en Virginia, la defensa de Megaupload alega, entre otros argumentos, el incumplimiento de un presupuesto de legitimación jurisdiccional cual es que, para poder ser acusados ante los tribunales norteamericanos, la empresa debe tener su domicilio en Estados Unidos, condición que no se cumple en este caso. Ni la empresa tiene domicilio social en Estados Unidos, ni ninguno de los acusados tiene nacionalidad norteamericana, ni residencia o domicilio en ese país.

A falta de conocer cuál sea finalmente la solución judicial en este procedimiento, sirve para advertir claramente la complejidad y la dimensión de los problemas que plantea la ciberdelincuencia transfronteriza, y las lagunas que, frente a ella, presentan los ordenamientos nacionales. En este tipo de delincuencia, las ideas de nacionalidad, territorio, localización y ubicación del perjuicio aparecen extraordinariamente difuminadas, lo que no solo dificulta la identificación de la jurisdicción nacional competente, sino que incluso pone en cuestión los propios criterios nacionales de determinación soberana de la extensión y límites de la jurisdicción nacional. No parece que, ante conductas delictivas no armonizadas a nivel

[35] En el momento de redactar este trabajo, el proceso se encuentra pendiente de la extradición solicitada por Estados Unidos a Nueva Zelanda del fundador y principal directivo de la empresa, así como de la decisión sobre la disponibilidad de las fuentes de prueba obtenidas por la policía neozelandesa durante las diligencias de entrada y registro practicadas a instancia del tribunal de Virginia. Por una parte, la vista del procedimiento de extradición, inicialmente fijada para el mes de julio de 2014 ha sido aplazada a febrero de 2015. Por otra parte, el tribunal de apelación de Nueva Zelanda ha rechazado la solicitud de los acusados, inicialmente acogida por el tribunal de instancia, de poner a disposición de la defensa las fuentes de prueba con las que cuenta la justicia norteamericana a fin de poder articular la defensa en el procedimiento de extradición.

internacional que, sin embargo, producen efectos en todo el mundo, la solución deba venir por el camino del imperialismo jurisdiccional y normativo a cargo de Estados que, actuando de forma individual y descoordinada respecto de la comunidad internacional, pueden acabar imponiendo las normas internas sustantivas y procesales a nivel mundial. El caso Megaupload, y más aún el caso Yahoo, que analizaremos a continuación, demuestran que las estrategias de solución deben discurrir, principalmente, por el camino de la cooperación internacional y de la armonización sustantiva y procesal.

3.2. *El caso Yahoo*

El caso Yahoo[36] es uno de los más conocidos en relación con los conflictos de jurisdicción derivados del funcionamiento de Internet. Yahoo Inc es una compañía de servicios de Internet creada en 1995, que ofrece servicios de búsqueda, alojamiento, correo electrónico, comercio e información a través de portales web. Tiene su domicilio en California (USA) y filiales en muchos países del mundo.

En el mes de abril de 2000, la Liga Contra el Racismo y el Antisemitismo (LICRA) y la Unión de Estudiantes Judíos de Francia (UEFJ), ambas organizaciones radicadas en Francia, advirtieron que en el portal de subastas de www.yahoo.com —accesible directamente a través de la referida dirección y también a través de www.yahoo.fr— se ofrecían objetos y propaganda relacionada con la ideología nazi, conducta constitutiva de delito en Francia[37]. Ambas asociaciones iniciaron el 10 de abril de 2000 un procedimiento contra Yahoo Inc ante el

[36] Sobre el caso Yahoo vid., ampliamente, RAMÍREZ PLASENCIA, «Conflicto de leyes y censura en Internet: el caso Yahoo!», en *Comunicación y sociedad*, Departamento de Estudios de la Comunicación Social, Universidad de Guadalajara, Nueva época, núm. 8, julio-diciembre de 2007, págs. 155 a 178.

[37] Según el art. R645.1 del Código Penal francés: «Est puni de l'amende prévue pour les contraventions de la 5e classe le fait, sauf pour les besoins d'un film, d'un spectacle ou d'une exposition comportant une évocation historique, de porter ou d'exhiber en public un uniforme, un insigne ou un emblème rappelant les uniformes, les insignes ou les emblèmes qui ont été portés ou exhibés soit par les membres d'une organisation déclarée criminelle en application de l'article 9 du statut du tribunal militaire international annexé à l'accord de Londres du 8 août 1945, soit par une personne reconnue coupable par une juridiction française ou internationale d'un ou plusieurs crimes contre l'humanité prévus par les articles 211-1 à 212-3 ou mentionnés par la loi n° 64-1326 du 26 décembre 1964. Les personnes coupables de la contravention prévue au présent article encourent également les peines complémentaires suivantes :

1° L'interdiction de détenir ou de porter, pour une durée de trois ans au plus, une arme soumise à autorisation

2° La confiscation d'une ou de plusieurs armes dont le condamné est propriétaire ou dont il a la libre disposition

3° La confiscation de la chose qui a servi ou était destinée à commettre l'infraction ou de la chose qui en est le produit

4° Le travail d'intérêt général pour une durée de vingt à cent vingt heures

Les personnes morales déclarées responsables pénalement, dans les conditions prévues par l'article 121-2, de l'infraction définie au présent article encourent, outre l'amende suivant les modalités prévues par l'article 131-41, la peine de confiscation de la chose qui a servi ou était destinée à commettre l'infraction ou de la chose qui en est le produit. La récidive de la contravention prévue au présent article est réprimée conformément aux articles 132.11, et 132.15.»

Tribunal de Gran Instancia de París, obteniendo un primer pronunciamiento cautelar el 22 de mayo de ese mismo año. En dicho pronunciamiento, el Tribunal francés asumió la competencia en el asunto y emitió una orden judicial preliminar para que el enlace a la subasta de objetos y el acceso a textos nazis desapareciera del portal yahoo.fr, imponiendo además a la compañía norteamericana la prohibición de que ciudadanos franceses pudieran acceder al sitio del portal yahoo.com en el que se subastaban los objetos de ideología nazi o en el que estaban disponibles determinados textos básicos de la ideología nazi —señaladamente *Mein Kampf* y *Los protocolos de los Sabios de Sión*— a través del enlace geocites.com, bajo apercibimiento de una multa de cien mil francos diarios en caso de incumplimiento.

Personada Yahoo Inc ante la jurisdicción francesa y alegada no solo la falta de jurisdicción nacional sino la imposibilidad técnica de impedir que los ciudadanos franceses accedieran directamente —sin enlazar a través de yahoo.fr— al portal yahoo.com en el que se encontraban los artículos y textos nazis, el Tribunal de Gran Instancia de París acordó la designación de una comisión de tres expertos a fin de informar sobre la viabilidad de las medidas de prohibición de acceso acordadas por el Tribunal en resolución de mayo de 2000[38]. A pesar de las dificultades expresadas por los expertos respecto de la limitación de acceso de los ciudadanos franceses a determinados espacios del portal www.yahoo.com, el Tribunal de Gran Instancia de París ratificó en sentencia, el 20 de noviembre de 2000 la decisión preliminar cautelar adoptada el mes de mayo, otorgando a Yahoo Inc un plazo de tres meses para el cumplimiento de las previsiones acordadas en la resolución de 22 de mayo de 2000.

A la vista de la resolución dictada por el Tribunal de Gran Instancia de París, Yahoo Inc decidió, en enero de 2001, acudir a la jurisdicción norteamericana interesando la decisión de inaplicabilidad en Estados Unidos de las disposiciones acordadas contra Yahoo Inc por la justicia francesa (*declaratory judgement*)[39]. La argumentación de Yahoo se basó en tres puntos de apoyo: a) Según la ley nacional de Estados Unidos, los proveedores de servicios no son responsables de los contenidos publicados en los portales; b) La venta online de artículos nazis no es delito en Estados Unidos, estando amparada por el derecho a la libertad de expresión consagrado en la primera enmienda de la Constitución de los Estados Unidos; y c) Los tribunales franceses no son competentes para conocer y juzgar hechos originados en Estados Unidos, imputables a personas físicas o jurídicas de

[38] Como explica RODRÍGUEZ BERNAL, «Los cibercrímenes...», cit., págs. 10 y 11, el comité de expertos nombrado al efecto admitió la posibilidad de que Yahoo implantara un sistema de identificación del origen de los usuarios, basándose en el IP de los ordenadores conectados, siempre y cuando dichos ordenadores utilizaran para la conexión proveedores franceses. El problema es que, ni todos los usuarios franceses de Internet se conectan a través de servidores franceses, ni todos los usuarios que utilizan servidores franceses son ciudadanos franceses.

[39] La competencia correspondió, en función del domicilio social de Yahoo Inc, al Tribunal Federal de Primera Instancia de San José (distrito de California).

nacionalidad norteamericana y considerados legales en su territorio nacional. En síntesis, la demandada entendía que legislación francesa no era aplicable a las actuaciones desarrolladas por Yahoo Inc, por más que sus espacios web fueran accesibles a través del portal www.yahoo.com[40].

En primera instancia, el juez federal Fogel, sin cuestionar los fundamentos de fondo de la decisión de la jurisdicción francesa, dio la razón a Yahoo Inc en el sentido de declarar la inaplicabilidad de la resolución del Tribunal de Gran Instancia de París en los Estados Unidos[41]. El problema se centraba en determinar el Derecho aplicable —y consiguientemente la jurisdicción competente— en casos controvertidos de libertad de expresión ejercida por ciudadanos norteamericanos desde Estados Unidos a través de Internet, cuando entrara en colisión con ordenamientos jurídicos de otros Estados con acceso a dicha información digital. El juez Fogel entendió que la protección a la libertad de expresión consagrada en la primera enmienda de la Constitución norteamericana no resultaba compatible con el cumplimiento de la orden francesa en el territorio de los Estados Unidos, esto es, con la primacía del Derecho francés que, en el caso de autos, pretendía imponer el Tribunal de Gran Instancia de París.

La sentencia del tribunal de primera instancia fue apelada por LICRA y UEFJ. Tras una primera resolución de la apelación, dictada el 23 de agosto de 2004, confirmando la sentencia de primera instancia[42], una segunda sentencia dictada por el tribunal del noveno circuito de apelaciones de California cambiaría la doctrina de las resoluciones precedentes —aunque no las consecuencias finales— al entender que desde el inicio del procedimiento en los Estados Unidos existió un defecto de legitimación pasiva, radicado en la imposibilidad de ejercer la jurisdicción nacional contra las dos asociaciones que en ningún caso habían acudido a la jurisdicción norteamericana, concluyendo que la justicia de Estados Unidos carecía de jurisdicción sobre las decisiones adoptadas por la jurisdicción francesa en el ejercicio de sus competencias[43].

[40] Sí lo es a la conducta del espacio www.yahoo.fr, por lo que tras la resolución del Tribunal de Gran Instancia de París de 22 de mayo de 2000, Yahoo procedió a retirar el contenido de vinculación nazi del referido espacio, así como los enlaces que desde esta página permitían el acceso al contenido controvertido en yahoo.com

[41] La sentencia de primera instancia (Juez Jeremy Fogel) fue dictada el 11 de julio de 2001 (Yahoo Inc a Delaweare Corporation vs La Ligue Contre le Racisme et L'antisemitisme, a French association et alli, Case number C-00-21275-JF, United States Dictrict Court for the Northern District of California, San Jose Division); puede consultarse en http://www.internetlibrary.com/pdf/Yahoo-La-Ligue-Contre-Le-Racisme.pdf.

[42] La primera sentencia de apelación (Yahoo Inc a Delaweare Corporation vs La Ligue Contre le Racisme et L'Antisemitisme, a French association; L'Union des Etudiants Juifs de France, a French association; D.C. No. CV-00-21275-JF, United States Court of Appeals for the Ninth Circuit) dictada por los jueces Ferguson, Wallace Tashima y Bruneti (opinión discrepante) el 23 de agosto de 2004, puede consultarse en: http://euro.ecom.cmu.edu/program/law/08-732/Jurisdiction/YahooNinthCircuit.pdf

[43] La segunda sentencia de apelación dictada por el Tribunal del Noveno Circuito en el caso Yahoo! Inc v. La Ligue Contra Le Racisme el L'Antisemitisme and L'Union Des Etudiants Juifs de France No. 01-17424, D.C. No. CV-00-21275-JF (12 de enero de 2006) puede consultarse en http://nacpec.org/en/links/jurisdiction/inter_case_law.html.

Paralelamente al proceso iniciado por la LICRA y la UEFJ, el Movimiento Contra el Racismo y por la Amistad entre los Pueblos (MRAP), así como la Asociación de Deportados a Auchswitz, presentaron ante el Tribunal Correccional de París una denuncia contra Timothy Koogle, entonces Presidente de Yahoo Inc, por apología del racismo y de crímenes contra la humanidad. En febrero de 2003, el Tribunal Correccional de París dictó sentencia absolutoria a favor Koogle, resolución confirmada por el Tribunal de Apelación de París el 6 de abril de 2005. A juicio de los tribunales penales franceses, en el curso del proceso no quedó acreditado que las informaciones que pudieran constituir apología del racismo y de los crímenes contra la humanidad tuvieran por autor a Yahoo Inc, ya que no estaban calificados ni retocados por la compañía, que se limitó a albergarlos en un espacio de su portal web destinado a subastas y ventas online. En suma, el Tribunal de Apelación de París señaló que, conforme a la legislación francesa, ni el portal ni sus directivos podían ser considerados responsables de los contenidos alojados por particulares[44].

Como puede advertirse, también el caso Yahoo plantea claramente los problemas para determinar la ley y la jurisdicción aplicable en supuestos de ciberdelincuencia transnacional sin armonización sustantiva. Pero a diferencia del caso Megauopload, aún pendiente de solución judicial, el caso Yahoo nos proporciona la posición de los tribunales, una solución compleja, contradictoria incluso en el ámbito interno de los Estados en conflicto, y que pone de manifiesto la insuficiencia de los instrumentos nacionales para afrontar de modo individual los problemas que genera la persecución y el castigo eficaz de la ciberdelincuencia internacional. En el caso Yahoo aparecen con claridad los tres problemas fundamentales que esta modalidad de delincuencia plantea a los modernos ordenamientos jurídicos, anclados aún en los principios de soberanía nacional y jurisdicción exclusiva. Por una parte, los hechos del caso Yahoo señalan la enorme dificultad de ubicar con precisión el lugar en el que se cometen los hechos cuando se trata de conductas desarrolladas a través de la Red. En los supuestos de difusión de contenidos a través de sitios web, son varias las posibles referencias espaciales que pueden determinar el anclaje físico de la conducta —residencia o domicilio del autor de la información, lugar del terminal desde el que dicha información se remite, lugar de ubicación del servidor, domicilio del proveedor de servicios que la aloja…—, sin que exista a priori un acuerdo sobre cuál debe ser tomada en consideración para determinar el Derecho aplicable y la jurisdicción competente. En segundo lugar, surgen evidentes problemas para determinar la autoría; no ya solo para identificar al presunto autor de los hechos, sino también para determinar el eventual reparto de responsabilidades entre el autor material, el intelectual y el proveedor de servicios. En tercer lugar, es fundamental, y muy compleja la tarea de determinar la ley penal

[44] Una decisión similar adoptó en noviembre de 2000 la Cámara Federal de San Martín (Argentina) ante una demanda criminal contra Yahoo por los mismos hechos.

aplicable cuando la acción y el resultado se producen en Estados diferentes —o en múltiples Estados, en el caso del resultado de muchos de los delitos cometidos a través de Internet—. Más aún cuando, en casos de diversidad de legislaciones sustantivas, no concurre el principio de doble incriminación, siendo los hechos delito en un Estado y atípicos en otro[45]. En cuarto lugar, la ambigüedad en cuanto a los referentes territoriales determina, como pone de relieve el caso Yahoo, la aparición de conflictos de jurisdicción por concurrencia de jurisdicciones nacionales que, a falta de una norma o criterio superior de competencia, conducen, en algunos casos a soluciones parciales, o en otros a vías procesales muertas, que no dejan de ser un estímulo para el desarrollo de este tipo de criminalidad[46].

3.3. *El caso Wintersteiger vs. Products 4U*

A diferencia de los ejemplos anteriores, reflejos claros del problema y de sus dificultades, el caso Wintersteiger aporta, además, un principio de solución por vía jurisprudencial. En efecto, el caso Wintersteiger *vs* Products 4U contiene una importante aportación del TJUE[47] a la solución de los problemas de jurisdicción internacional por responsabilidad delictiva en Internet, que a su vez recoge la jurisprudencia del TJUE en dos importantes sentencias precedentes: casos Fiona Shevil[48] y e-Data advertising[49].

[45] Es suficiente la existencia de lagunas o discordancias legislativas en Estados de Derecho avanzados o del llamado primer mundo para propiciar nichos de impunidad a los delincuentes informáticos. Según señala Naciones Unidas en las consideraciones previas al XII Congreso sobre Prevención del Delito y Justicia Penal (Salvador Brasil, 2010), A/CONF.213/9, pág. 5, «Un efecto práctico de la arquitectura en red de Internet es que los autores de los delitos cibernéticos no necesitan estar presentes en el lugar del delito. Por ello, impedir la existencia de refugios seguros para los delincuentes se ha convertido en un aspecto clave de la prevención del delito cibernético. Los delincuentes utilizarán refugios seguros para obstaculizar las investigaciones. Un ejemplo bien conocido es el gusano informático "Love Bug", desarrollado en Filipinas en 2000, que al parecer infectó a millones de computadoras en todo el mundo. Las investigaciones locales se vieron impedidas por el hecho de que, en esa época, el desarrollo y la difusión intencionales del programa informático dañino no estaban debidamente penalizados en Filipinas. La cuestión de la convergencia de la legislación es sumamente pertinente, puesto que un gran número de países fundamenta su régimen de asistencia judicial recíproca en el principio de la doble incriminación, según el cual un delito debe ser considerado como tal tanto en el Estado que solicita la asistencia como en el que la presta. Las investigaciones a nivel mundial se limitan, por lo general, a los actos que están tipificados como delito en todos los países afectados. Aunque existe una serie de delitos que pueden ser perseguidos en cualquier parte del mundo, las diferencias regionales desempeñan un papel importante. Por ejemplo, en diferentes países se penalizan diferentes tipos de contenidos, lo que significa que el material que se coloca legalmente en un servidor en un país puede ser considerado ilegal en otro».

[46] Como señala RODRÍGUEZ BERNAL, «Los cibercrímenes...», cit., pág. 12, si bien en el campo del derecho privado transnacional existe una regulación más o menos acertada que rige en materia de contratos, de responsabilidad extracontractual, etc., el derecho penal aparece desprovisto de esta mínima solvencia, dándose la paradoja de que, precisamente por los bienes jurídicos barajados, es en el derecho público donde debería existir una mayor claridad y seguridad.

[47] La sentencia trae causa de una petición de decisión prejudicial planteada por Austria; asunto C 523/10, y resuelta por STJUE de 12 abril de 2012. El texto puede consultarse en: eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=celex:62010CJ0523:es:html

[48] STJUE de 7 de marzo de 1995

[49] STJUE de 25 de octubre de 2011

Los hechos del caso Wintersteiger traen causa de una presunta vulneración del derecho de marca que enfrenta a compañías radicadas en dos Estados de la Unión Europea: Alemania y Austria. Wintersteiger (demandante) era una empresa austríaca que desde 1993 fabricaba y vendía maquinaria para el ajuste de esquís, físicamente en Austria y online al todo el mundo.Por su parte, Products 4U era una empresa alemana que desde 1995 también fabricaba y vendía —físicamente y online— máquinas de ajuste para esquís. Products 4U también vendía accesorios para su maquinaria, a los que denominaba *Wintersteiger-Zubehör*.

El 1 de diciembre de 2008, Products 4U reservó "Wintersteiger" como palabra clave de búsqueda y redirección en google.de, de modo que cuando en el buscador alemán de google se introducía la palabra Wintersteiger, aparecía, destacado, un anuncio en la parte superior derecha de la pantalla que encaminaba al internauta hacia el sitio web de Products 4U.

Una vez conocida esta operación, Wintersteiger demandó en 2009 a Products 4U ante los tribunales austríacos por vulneración de su marca en Austria[50], oponiendo Products 4U excepción de falta de competencia, entendiendo que la demanda debió haberse interpuesto en Alemania. Tras las correspondientes instancias internas, el Tribunal Supremo austríaco planteó ante el TJUE cuestión prejudicial solicitando la interpretación del artículo 5, número 3, del Reglamento (CE) nº 44/2001 del Consejo, de 22 de diciembre de 2000, relativo a la competencia judicial, el reconocimiento y la ejecución de resoluciones judiciales en materia civil y mercantil.

Tal y como adelantamos, en la sentencia Wintersteiger el TJUE aporta claves jurisprudenciales de interés para afrontar los problemas de concurrencia jurisdiccional internacional en el ámbito de la ciberdelincuencia. No conviene pasar por alto que tales reglas surgen en un espacio de integración jurídica internacional a nivel regional, como es el europeo; que en este espacio no existen aún reglas de reparto competencial internacional en materia penal, pero que las normas y criterios jurisprudenciales sobre infracciones de derechos civiles y mercantiles previstos en el derecho comunitario pueden resultar útiles no solo para orientar la solución de supuestos de litispendencia internacional penal en materia de ciberdelincuencia, sino también para entender que es la cooperación y la progresiva armonización normativa internacional el camino para determinar eficazmente la jurisdicción idónea en casos de conflictos internacionales de competencia penal en el ámbito de la cibercriminalidad.

En síntesis, la doctrina del TJUE en el caso Wintersteiger sienta las siguientes reglas:

[50] La pretensión de Wintersteiger consistía en que se prohibiese a Products 4U utilizar la marca austriaca «Wintersteiger» como palabra clave en el sitio de Internet del prestador de un servicio remunerado de redirección.

* Los criterios que determinan la competencia judicial internacional en ilícitos transfronterizos deben ser claros y previsibles, aportando seguridad jurídica a las partes.

* A la hora de resolver los eventuales conflictos internacionales de jurisdicción que puedan surgir entre Estados, el fuero principal debe ser el "lugar en que se ha producido el hecho dañoso".

* Cuando el hecho dañoso pueda entenderse producido en varios lugares, se adopta la teoría de la ubicuidad. Conforme a la teoría de la ubicuidad, son competentes, alternativamente, los órganos: a) del lugar en que se ha producido la acción (hecho causal) o, b) del lugar en que se ha producido el resultado.

* En los ilícitos a través de Internet es necesario definir con la máxima precisión posible el lugar en que se ha considerado realizada acción u omisión, y el lugar en que se ha producido el resultado. Por lugar de producción del hecho causal debe entenderse el centro de decisión del actor —lugar en que se adopta la decisión inteligente, no donde se produce el proceso técnico—. Por lugar de producción del daño debe entenderse el lugar en que la víctima tenga su centro de intereses, que no tiene porqué coincidir con su nacionalidad ni con el domicilio.

* Por último, a la hora de establecer la preferencia entre acción y resultado hay que tener en cuenta dos criterios, aplicados caso a caso: por un lado el lugar donde se disponga de un acceso eficaz a las fuentes de prueba; por otro lado, el lugar en el que se presuma que pueda producirse una adecuada y completa sustanciación del proceso en términos de eficacia y también en términos de garantía.

4. **Estrategias de solución**

4.1. *La creación de un Tribunal penal internacional en materia de ciberdelincuencia*

Entre las propuestas de solución de los conflictos internacionales de jurisdicción generados en la persecución y castigo de la ciberdelincuencia ocupa un lugar preeminente la idea de un tribunal internacional que, en ciertos casos funcionaría como tribunal de única instancia, mientras que en otros actuaría como órgano de atribución de la jurisdicción nacional idónea (instancia de solución de conflictos internacionales de jurisdicción).

Es cierto que, al menos en el terreno teórico, una justicia penal internacional para la delincuencia informática transfronteriza podría solucionar algunos de los problemas que plantea el actual marco de competencia territorial de las jurisdicciones nacionales, problemas que han sido destacados por nuestra jurisprudencia[51], y

[51] Vid. STS de 11 de diciembre de 2006: «[…] la intervención de los Tribunales españoles, respecto de hechos cometidos fuera de su territorio, puede plantear indudables conflictos desde el punto de vista de las relaciones internacionales del Estado español —competencia propia del Gobierno de la Nación (v. art. 97 CE)—, materia, por tanto, ajena a la función jurisdiccional, pero que, sin duda, los Tribunales no pueden

que han conducido a una progresiva limitación del principio de justicia penal universal plena[52].

Sin embargo, junto a los problemas de sumisión a la competencia, de los que dan buena cuenta las dificultades para conseguir las ratificaciones mínimas de cualquier Tribunal Internacional con competencias penales, deben situarse problemas técnicos derivados de la tipificación armonizada de las conductas, de la definición de su competencia, del volumen de trabajo que soportaría, de su composición, y de la eficacia de una jurisdicción que nunca sería plenamente universal[53].

Tal vez no deba descartarse una solución más sencilla, que no pasaría por crear un nuevo tribunal internacional sino aprovechar la existencia de la Corte Penal Internacional, atribuyéndole sólo aquellos delitos más graves relacionados con Internet, como por ejemplo la protección a gran escala y a nivel penal de la propiedad intelectual, la lucha contra las redes de pornografía infantil, los paraísos informáticos, o los fraudes económicos internacionales cometidos a través de la Red. Esta técnica selectiva, unida a un proceso avanzado de armonización penal y de cooperación policial y judicial, permitiría la convergencia entre las jurisdicciones nacionales y la jurisdicción internacional mediante el reparto de competencias, mejor ajustadas así a la extensión territorial de la conducta y a la gravedad del delito, configurando para muchos casos al juez nacional como juez universal en materia de ciberdelincuencia.

4.2. *La utilización de sistemas de ADR para la solución de conflictos internacionales de jurisdicción*

En segundo lugar, y dentro de un vigoroso movimiento actual a favor de los ADR, se han patrocinado con fuerza para la solución de los conflictos derivados del uso de los sistemas informáticos los métodos de composición de conflictos

desconocer de modo absoluto. Por lo demás, en cuanto al sometimiento de conductas desarrolladas fuera del ámbito territorial de los distintos Estados a la jurisdicción de sus Tribunales, en materias que interesan a la comunidad internacional, especialmente en cuanto pudieran afectar a la paz y a la protección y defensa de los derechos humanos, la evolución del llamado Derecho penal internacional parece orientarse más bien hacia los Tribunales internacionales y a la intervención de las Naciones Unidas, como ya hemos apuntado.»

[52] Cabe recordar que, en los últimos años, el art. 23.4 LOPJ ha sufrido dos importantes modificaciones, encaminadas ambas a reducir el ámbito de aplicación del principio de jurisdicción penal universal: LO 1/2009 y LO 1/2014.

[53] Como ha señalado CLIMENT BARBERÁ, «La justicia penal en Internet…», cit., pág. 660, las ventajas de una propuesta de derecho penal armonizado y de una justicia penal universal «son patentes desde el punto de vista de la seguridad jurídica, del decaimiento de la impunidad en Internet y de la superación de los problemas de aterritorialidad de la Red. Sin embargo, aunque los inconvenientes no se vislumbran más allá de los conflictos con las jurisdicciones nacionales, la viabilidad de esta alternativa no parece posible a corto plazo, y ello por dos razones: la primera, porque para la validez del sistema sería necesario que la totalidad de los Estados adoptaran el sistema, sin que quedaran territorios fuera del mismo a modo de *paraísos penales de Internet*. La segunda, porque aun cuando se consiguiera esta unanimidad respecto a la configuración de los delitos en Internet, no parece viable la constitución de órganos jurisdiccionales internacionales penales específicos para estos, a la vista de las dificultades que para la creación de un Tribunal Penal Internacional para los delitos contra la humanidad se vienen produciendo en la actualidad».

alternativos a la jurisdicción, como el arbitraje, la mediación y la conciliación. Tales métodos tienen, y tendrán en el futuro sin duda, una importancia capital en el terreno de los conflictos jurídicos disponibles, dado su bajo coste, su rapidez, la complejidad de las soluciones judiciales en los conflictos transnacionales, y la garantía de conocimiento especializado que proporciona un árbitro específicamente elegido para un determinado conflicto.

En el ámbito penal, hay que reconocer el impulso y la importancia que en los últimos años ha adquirido la justicia restaurativa, muy señaladamente la mediación, como sistema alternativo-complementario de solución de conflictos penales. En el marco del problema que planteamos en este trabajo —la prevención y solución de conflictos internacionales de jurisdicción en el marco de la ciberdelincuencia— los métodos consensuales de composición tienen un interés relevante. No se trata aquí de defender la mediación como sistema de solución alternativo al proceso penal; se trata de proponer el uso de sistemas autocompositivos para determinar la jurisdicción idónea en caso de concurrencia de jurisdicciones nacionales —litispendencia internacional— en la persecución y castigo de ciberdelitos.

Como veremos más adelante, a falta de normas internacionales claras sobre predeterminación de la jurisdicción idónea en materia de ciberdelincuencia, y de una instancia internacional vinculante que las imponga, no hay otra vía que la del consenso para que, en supuestos de concurrencia de jurisdicciones nacionales, pueda determinarse aquella jurisdicción que está en mejores condiciones —en términos de eficacia procesal y de protección de garantías— para asumir un proceso penal transnacional por cibercriminalidad.

Hasta el momento, las normas internacionales apuestan, en esta dirección, por un primer paso, basado en el consenso y construido sobre el intercambio de pareceres entre los Estados cuyas jurisdicciones concurren en la persecución y castigo de un determinado ciberdelito. Sin embargo, no hay que descartar que en este camino pueda avanzarse en el futuro con instrumentos como la mediación, que sin forzar una solución impuesta, añada al consenso espontáneo algunas claves de eficacia basadas en la intervención de un tercero con *auctoritas* que aproxima, sugiere y contribuye con las partes a encontrar una solución adecuada al conflicto jurisdiccional[54].

4.3. *La cooperación internacional y el juez nacional como juez internacional*

En la actualidad, la idea fundamental que hilvana las posibles estrategias de solución frente a los conflictos internacionales de jurisdicción, en términos

[54] En espacios regionales homogéneos de integración internacional existen estructuras de cooperación judicial que pueden jugar un papel importante en la solución de conflictos internacionales de jurisdicción mediante el diálogo y el consenso; así sucede, por ejemplo, con IberRed en el ámbito iberoamericano, o con Eurojust en el europeo. Sobre la intervención de Eurojust en la solución de conflictos intracomunitarios de jurisdicción penal internacional vid. art. 12.2 de la citada Decisión Marco 2009/948/JAI.

generales y señaladamente en materia de cibercriminalidad, está basada en la cooperación internacional[55]. Dichos conflictos son, en la mayoría de los casos, el producto de una visión nacional, limitada e individual del fenómeno de la criminalidad informática.

En este contexto, la cooperación internacional es el instrumento idóneo para lograr, por un lado, una armonización de los sistemas penales capaz de eliminar zonas de impunidad y unificar el lenguaje básico para la identificación de las conductas punibles[56]. Por otra parte, es la cooperación internacional la base sobre la cual se puede lograr una persecución y castigo razonablemente eficaz de la criminalidad informática desde la coordinación de la actividad judicial y policial.

Debe repararse en que la cooperación internacional ha avanzado de modo relevante en el terreno de la asistencia judicial y policial a través de medidas que permiten la colaboración en la obtención de fuentes de prueba, el intercambio de información o la entrega de detenidos. Sin embargo, no se ha avanzado tanto en la búsqueda de soluciones procesales destinadas a evitar los procedimientos penales paralelos. Plantear soluciones para este problema abre el camino para evitar no sólo duplicidades innecesarias e ineficaces para el éxito del procedimiento, sino principalmente la afectación del principio *non bis in idem,* reconocido como se sabe en los principales textos internacionales sobre derechos fundamentales y garantías penales y procesales.

En este camino, la comunidad internacional debe avanzar hacia la búsqueda de fórmulas y criterios que fortalezcan la cooperación judicial mediante la selección

[55] Los textos y acuerdos internacionales vigentes que abordan el problema de la determinación de la jurisdicción nacional competente en delitos transnacionales, basan la identificación de la jurisdicción idónea en la cooperación internacional, esto es, en el acuerdo entre las jurisdicciones concernidas sobre el lugar en el que resultará más adecuado seguir el procedimiento. Vid., entre otros, el Convenio sobre Ciberdelincuencia del Consejo de Europa, de 8 de noviembre de 2001 (art. 22); la Convención de Naciones Unidas contra la Delincuencia Organizada Transnacional (art. 15), de 15 de noviembre de 2002; la Convención de Naciones Unidas contra la Corrupción, de 31 de octubre de 2003 (art. 42); el Convenio del Consejo de Europa sobre la Lucha contra la Trata de Seres Humanos, de 16 de mayo de 2005 (art. 31); el Convenio del Consejo de Europa sobre la Prevención del Terrorismo, de 16 de mayo de 2005 (art. 14); el Convenio del Consejo de Europa sobre Protección de los Niños y contra de la Explotación y el Abuso Sexual, de 25 de octubre de 2007 (art. 25); la Decisión Marco 2002/475/JAI, del Consejo, de 13 de junio, relativa a la Lucha Contra el Terrorismo (art. 9); la Decisión Marco 2004/68/JAI del Consejo, de 22 de diciembre de 2003, relativa a la Lucha contra la Explotación Sexual de los Niños y la Pornografía Infantil (art. 8); la Decisión Marco 2008/913/JAI, del Consejo, de 28 de noviembre de 2008, relativa a la Lucha contra determinadas formas y manifestaciones del Racismo y la Xenofobia mediante el Derecho Penal (art. 9); la Decisión Marco 2009/948/JAI del Consejo, de 30 de noviembre de 2009, sobre Prevención y Resolución de Conflictos de Ejercicio de Jurisdicción en los Procesos Penales; y la Directiva 2013/40/UE del Parlamento y del Consejo, de 12 de agosto de 2013 (art. 12). Dentro de las recomendaciones y propuestas en el ámbito académico hay que citar el Conjunto de Herramientas para la Legislación sobre Ciberdelito de la Unión Internacional de Telecomunicaciones (sección 21), disponible en http://www.itu,int/ITU-D/cyb/cybersecurity/docs/itu-toolkit-cybercrime-legislation-pdf; vid. también el llamado "Proyecto Stanford para la Protección en contra de la Ciberdelincuencia y del Ciberterrorismo (Stanford Draft) (art. 5), disponible en http://www.iwar.org.uk/law/resocurces/cybercrime/stanford/cisac-draft.htm (para estos dos últimos instrumentos vid. VELASCO SAN MARTÍN, *La jurisdicción y competencia*…, cit., págs. 122 y ss).

[56] Vid CLIMENT BARBERÁ, «La justicia penal en Internet…», cit., pág. 661.

dialogada de la jurisdicción penal idónea en casos de litispendencia internacional y la búsqueda de acuerdos de reconocimiento mutuo de resoluciones judiciales adoptadas en un espacio internacional concertado en los ámbitos penal y procesal.

En concreto, la prevención de los conflictos derivados de la concurrencia jurisdiccional en materia de cibercriminalidad pasa, fundamentalmente, por una armonización racional y consensuada de los criterios de determinación de los límites y criterios de la competencia nacional en las legislaciones de los Estados. Los mecanismos de selección de la jurisdicción idónea basados en el diálogo y en el consenso no cuestionan el principio de soberanía judicial nacional; constituyen, al contrario, un ejercicio de la misma cuando son las propias autoridades competentes de los Estados las que procuran una armonización legal en materia de competencia internacional, y acuerdan, en caso de conflicto, la competencia adecuada con la mirada puesta en la eficacia de la persecución y castigo, y con respeto a las garantías internacionales sobre derechos fundamentales. Esta selección consensuada de la jurisdicción idónea conduce al reconocimiento del juez nacional como juez internacional, y al reconocimiento mutuo de las resoluciones judiciales adoptadas en aplicación de los criterios comunes de preferencia jurisdiccional[57].

En este sentido, parece razonable sostener que la persecución eficaz y coordinada de la ciberdelincuencia debe avanzar en el marco de instrumentos internacionales de cooperación que tomen como referencia fundamental dos medidas complementarias. En primer lugar, y con vocación preventiva, cabe plantear la adopción de un acuerdo sobre los criterios de atribución preferente de la competencia de la jurisdicción penal nacional en la persecución de la cibercriminalidad. En segundo lugar, como herramienta de solución de los problemas de convergencia jurisdiccional, conviene plantear la adopción de un procedimiento simplificado y consensuado para acordar, en cada caso y a través del diálogo entre las autoridades competentes concernidas, la jurisdicción idónea en casos de litispendencia internacional penal o conflictos negativos de competencia en procedimientos contra la cibercriminalidad.

Las líneas que siguen contienen un análisis de *lege data* y una propuesta de *lege ferenda*. El análisis de *lege data* se centra en la solución que ofrece el Convenio de Budapest al problema de la jurisdicción competente en materia de ciberdelincuencia. La propuesta de *lege ferenda* aporta lo que a nuestro juicio serían las líneas fundamentales para afrontar con eficacia la determinación de la jurisdicción nacional idónea en el marco de un futuro acuerdo internacional para la prevención y castigo de la ciberdelincuencia.

[57] Esta es la base de las reglas de competencia que figuran en los textos y convenios internacionales que abordan el problema de la jurisdicción penal en delitos transnacionales; un ejemplo claro sobre la fórmula de cooperación judicial internacional de determinación de la competencia en materia de delincuencia transnacional puede verse en el Informe Anual de Eurojust de 2003 (Anexo), bajo el epígrafe «Criterios para decidir: ¿Qué jurisdicción debe ser competente?».

4.4. *El modelo previsto en el Convenio sobre Ciberdelincuencia de 2001 del Consejo de Europa*

En un contexto de progresiva integración europea a través de los valores de democracia, libertad y protección de los derechos humanos cabe inscribir el proceso de tratamiento común de la criminalidad informática, liderado en sus inicios por el Consejo de Europa, que ha emitido Recomendaciones clave en la materia[58], y que han terminado por fraguar en un Convenio modelo y referente fundamental sobre la prevención y castigo de la criminalidad informática[59].

El Convenio, fechado en Estrasburgo el 25 de mayo de 2001 y presentado a la firma el 26 de noviembre de 2001, cuenta por el momento con cuarenta y siete firmas y treinta y cinco ratificaciones, habiendo entrado en vigor en un total de treinta y un Estados[60]. Su regulación constituye un importante referente en la protección internacional contra la delincuencia informática[61], que en la actualidad empieza a ser completado con otros instrumentos internacionales a nivel regional. De cualquier modo, debe destacarse su valor dentro de los esfuerzos por homogeneizar la tipificación penal de la criminalidad informática, tratando con ello de salvar uno de los principales obstáculos con lo que choca en la actualidad la persecución y castigo de esta modalidad de delincuencia[62].

A la determinación de la jurisdicción competente dedica el Convenio de Budapest el art. 22, que está basado en tres ideas fundamentales: a) la fijación de fueros comunes de atribución de competencia judicial nacional; b) el respeto a las normas internas de determinación de la competencia judicial nacional y c) la recomenda-

[58] Vid. R (89) 9, de 13 de septiembre, del Comité de Ministros del Consejo de Europa, sobre criminalidad informática; R (95) 13, de 11 de septiembre, del Comité de Ministros del Consejo de Europa, concerniente a problemas de justicia penal relacionada con las tecnologías de la información. Sobre la trayectoria europea en la prevención y persecución concertada de la ciberdelincuencia vid. RODRÍGUEZ BERNAL, «Los cibercrímenes...», cit., págs. 13 y ss.

[59] Un estudio de detalle sobre el Convenio puede consultarse en LEZERTUA, «El Proyecto de Convenio... », cit.

[60] A 20 de agosto de 2014, el Convenio cuenta con cuarenta y dos ratificaciones, siendo 11 los Estados cuya firma aún no ha venido seguida de la correspondiente ratificación. Del Consejo de Europa faltan por ratificar Andorra, Grecia, Irlanda, Leichtenstein, Luxemburgo, Mónaco, Polonia, Rusia, San Marino, Suecia y Turquía. Los países no miembros del Consejo de Europa que han ratificado el Convenio son Australia, República Dominicana, Japón, Mauritania, Panamá, Filipinas y Estados Unidos; ; vid. http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=8&DF=&CL=ENG

[61] A juicio de URBANO CASTRILLO, «Infracciones patrimoniales...», cit., pág. 153, la Convención del Consejo de Europa sobre el cibercrimen constituye el texto jurídico internacional más importante en materia de delincuencia informática, aunque la falta de ratificación por países tan importantes como China o Estados Unidos hace que su impacto sea por el momento reducido.

[62] Como ha señalado CLIMENT BARBERÁ, , «La justicia penal en Internet…», cit., pág. 662, el Convenio de Budapest «aunque presenta una alternativa modesta y no resuelve el problema global de la transnacionalidad de Internet, supone un evidente paso adelante en la línea apuntada, recoge fórmulas muy limitadas y aún confinadas en los ámbitos penales nacionales, pero presenta la gran ventaja de ser viable en el momento actual, introduciendo avances que sin duda no resuelven todos los problemas, pero mejoran sensiblemente la presente situación y aportan soluciones razonables y asumibles para los problemas más inmediatos».

ción del diálogo y del consenso como método de solución de los conflictos internacionales de jurisdicción que puedan surgir entre los Estados parte[63].

Los fueros comunes de asignación de la competencia jurisdiccional son tres. En primer lugar figura el fuero territorial, conforme al cual serán competentes para el conocimiento de los delitos previstos en el Convenio los Estados en cuyo territorio, buques o aeronaves se haya cometido el delito. El segundo criterio de atribución de la competencia nacional es la nacionalidad, de tal forma que, en relación con los delitos tipificados en el Convenio, será competente también el Estado de la nacionalidad del autor. En este caso, el delito solo será perseguible si la conducta estaba también tipificada como delito en el lugar de comisión —doble incriminación—, o si siendo delictiva en el lugar de comisión, ningún Estado alega competencia territorial sobre el mismo. En tercer lugar, será competente para el enjuiciamiento de los delitos previstos en el Convenio el Estado en el que se encuentre el presunto autor, si no resultara extraditable por razón de su nacionalidad al Estado que lo reclame[64].

[63] Un análisis de la regulación de la jurisdicción en el Convenio sobre Cibercrimen del Consejo de Europa puede verse en KASPERSEN, «Jurisdiction in the Cybercrime Convention», en *Cybercrime and Jurisdiction. A Global Survey (Ed. Bert-Jaap Koops and Susan Brenner)*, Information Technology Law Series 11 TMC Asser Press, The Hague 2006, págs. 10 y ss.(citado por VELASCO SAN MARTÍN, *La Jurisdicción y competencia*…, cit., pág. 87). Vid. también HERRERO TEJEDOR, «Convenio sobre el Cibercrimen y su aplicación en España», *E-Newsletter sobre prueba electrónica de Cybex*, núm. 36, marzo de 2008, págs. 3 a 10, y núm. 37, abril de 2008, págs. 3 a 15.

[64] Un esquema similar proponía la Decisión Marco 2005/222/JAI del Consejo, de 24 de febrero, relativa a los ataques contra los sistemas de información. En el ámbito procesal destacan las necesarias normas de reparto de competencia judicial internacional, que aparecían basadas en los principios de territorialidad, nacionalidad del autor o domicilio de la persona jurídica beneficiaria de la conducta delictiva, apelando a criterios de colaboración y cooperación a través de las redes de comunicación judicial cuando la competencia pueda recaer en los tribunales de distintos estados miembros. En caso de conflicto, la Decisión Marco recomendaba tomar en consideración tres fueros sucesivos, basados respectivamente en la territorialidad de la infracción, en la nacionalidad del autor y en el lugar de detención del autor. Como señaló RODRÍGUEZ BERNAL, «Los cibercrímenes…», cit., págs. 26 y 27, «a tenor de esta redacción, y puesto que los sistemas informáticos se hallan a menudo interconectados por redes transfronterizas, se adivinan importantes puntos de fricción. Así, bastaría la comisión parcial del delito para que un Estado aplicara su jurisdicción, siendo frecuentes los multiataques informáticos que producirían la potencial actuación de muchas jurisdicciones. Los Estados que persiguiesen a sus nacionales podrían colisionar con la jurisdicción de aquellos en cuyo territorio se hubiera cometido el delito o en cuyo territorio se domiciliase la persona jurídica administrada por el nacional perseguido por su propio país. Otras muchas combinaciones podrían darse, lo que convierte a esta regla, más que en una regla de conflicto, en una regla conflictiva». La Decisión Marco 2005/222/JAI ha sido sustituida por la vigente Directiva 2013/40/UE, del Parlamento y del Consejo, de 12 de agosto de 2013, sobre ataques contra sistemas de información. La nueva Directiva introduce algunas modificaciones significativas en materia de competencia jurisdiccional, entre las que cabe destacar tres: en primer lugar, los criterios de vinculación competencial siguen siendo tres: territorialidad, nacionalidad del autor y domicilio de la persona jurídica beneficiaria, pero los dos últimos se prevén en la Directiva de 2013 como criterios que voluntariamente pueden acoger los Estados, quedando pues el de la territorialidad como único criterio obligatorio. En segundo lugar, dentro del criterio de territorialidad —esto es, como delitos cometidos en territorio nacional— se incluyen, con acierto, tanto las conductas desarrolladas por el autor en territorio nacional con efectos fuera de él, como las conductas desarrolladas por el autor fuera del territorio nacional pero con efectos dentro del mismo. En tercer lugar, desaparecen de la regulación tanto los criterios que precisaban el orden de prelación entre las reglas de competencia —la territorialidad era preferente a la nacionalidad, y esta última lo era sobre el lugar de detención— como la recomendación de acudir a la vía

En relación con estos tres criterios de asignación competencial deben realizarse algunas observaciones[65]. Por una parte, señalar que el fuero territorial es el primero y, en principio, parece que el preferente sobre otros criterios de asignación competencial entre los Estados parte. Es preferente en cuanto que el criterio de la nacionalidad solo entra en juego si ningún Estado tiene competencia territorial sobre el mismo. (art. 22.1 d)[66]. No obstante, la preferencia parece quebrarse cuando el art. 22.4 señala que el Convenio «no excluye ninguna jurisdicción penal ejercida por una Parte de conformidad con su derecho interno», de tal forma que si el derecho interno de algún Estado no otorga preferencia al criterio de la territorialidad y el presunto autor es detenido en dicho Estado, prevalecen los criterios internos sobre los previstos en el art. 22. Junto a ello, debe notarse que el art. 22 no contiene regla alguna que identifique el lugar de comisión del delito, con lo que serán probables los supuestos de concurrencia jurisdiccional basados en la identificación del *locus delicti* con el lugar de acción y con el lugar del resultado —o con varios lugares de diferentes Estados en los que se haya producido la acción o el resultado—. Parece oportuno señalar también la omisión en el art. 22 de supuestos de exclusión de la competencia nacional derivados de hechos ya juzgados y sentenciados en otro Estado, así como de modernas referencias territoriales en la determinación de la competencia nacional, que incluyen expresamente los delitos cometidos contra sistemas informáticos situados en el territorio del Estado, independientemente de la ubicación física del autor—, o la nacionalidad de los satélites o dispositivos extraterritoriales que sirvan para realizar la conducta delictiva[67].

El segundo principio que inspira el art. 22 del Convenio está basado en el respe-

consensual para la solución de los eventuales conflictos de jurisdicción que pudieran surgir, remitiéndose la Directiva en este aspecto a lo dispuesto en la Decisión Marco de 2009 sobre solución de conflictos de jurisdicción en materia penal —apartado 11 de la exposición de motivos de la Directiva de 2013—.

[65] Sobre las críticas de la comunidad científica al art. 22 del Convenio de Budapest vid. VELASCO SAN MARTÍN, *La Jurisdicción y competencia*…, cit., pág. 89.

[66] La preferencia también deriva del carácter no disponible del fuero territorial estricto —espacio físico del Estado— frente a la disponibilidad de los criterios fijados en los fueros previstos en las letras b a d del art. 22 —delitos cometidos en buques, aeronaves o por nacionales del Estado—.

[67] Respecto del principio de territorialidad y la utilización de satélites vid. el art. 5 del Proyecto de Convenio Internacional para la Protección en contra de la Ciberdelincuencia y el Ciberterrorismo (Proyecto Stanford): «Artículo 5: Jurisdicción. 1. Cada Estado Parte en el presente Convenio deberá adoptar las medidas que sean necesarias para establecer su jurisdicción respecto de los delitos previstos en los Artículos 3 y 4 en los siguientes casos: (a) cuando el delito se comete en el territorio de ese Estado o a bordo de un buque, aeronave o satélite matriculado en ese Estado o en cualquier otro lugar bajo su jurisdicción, reconocido por el Derecho internacional». Respecto de la aplicación del criterio territorial tanto si el autor actúa desde el Estado en cuestión como si están en el Estado los sistemas informáticos de los que se sirve, vid. art. 12 de la Directiva 2013/40/UE; al establecer la competencia conforme al fuero territorial «cada Estado miembro garantizará que se incluyan en la misma los casos en que: a) el autor cometa la infracción estando físicamente presente en su territorio, independientemente de que la infracción se cometa o no contra un sistema de información situado en su territorio; b) la infracción se cometa contra un sistema de información situado en su territorio, independientemente de que el autor cometa o no la infracción estando físicamente presente en su territorio».

to de la soberanía jurisdiccional nacional, y se expresa mediante el respeto de las reglas nacionales de determinación de la extensión y límites de la jurisdicción. Se explica este principio en un contexto de recelo y desconfianza hacia los mecanismos de cesión o reconocimiento de preferencia de jurisdicciones penales de otros Estados, pero debe advertirse que es precisamente este principio el que favorecerá los conflictos internacionales de jurisdicción al establecer, de facto, la sumisión voluntaria al sistema de fueros establecidos en el Convenio, reservando siempre la posibilidad de aplicar los criterios nacionales, sean o no concordantes con los previstos en el Convenio. Cabe afirmar en este sentido que, de poco servirá la armonización penal sustantiva si esta no viene acompañada de normas homogéneas de determinación de la jurisdicción competente, puesto que son las normas procesales las que, en última instancia, garantizan una eficaz persecución y castigo de los delitos objeto de armonización.

Finalmente, el número 5 del art. 22 propone el consenso y el diálogo como método para la solución de conflictos de concurrencia jurisdiccional[68]. En concreto, dispone que cuando «varias Partes reivindiquen su jurisdicción respecto de un presunto delito contemplado en el presente Convenio, las Partes interesadas celebrarán consultas, cuando ello sea oportuno, con el fin de decidir qué jurisdicción es la más adecuada para entablar la acción penal».

Respecto de esta última previsión pueden aportarse dos observaciones. En primer lugar, la importancia que tiene la alusión indirecta a lo que en este trabajo denominamos jurisdicción idónea. Por tal cabe entender aquella jurisdicción nacional que, en un caso concreto y en concurrencia con otras jurisdicciones nacionales, está en las mejores condiciones para asumir el conocimiento de litigio con la máxima eficacia procesal y con el máximo respeto a las garantías procesales de las partes y víctimas. El concepto es útil en el campo internacional para identificar aquella jurisdicción cuya preferencia no deriva de la imposición de un

[68] Una previsión similar figura en el art. 15.5 de la Convención de Naciones Unidas contra la Delincuencia Organizada Transnacional: «Si un Estado Parte que ejerce su jurisdicción con arreglo a los párrafos 1 y 2 del presente artículo ha recibido notificación, o tomado conocimiento por otro conducto, de que otro u otros Estados Parte están realizando una investigación, un proceso o una actuación judicial respecto de los mismos hechos, las autoridades competentes de esos Estados Parte se consultarán, según proceda, a fin de coordinar sus medidas». También se apostaba específicamente por el consenso en la solución de los conflictos transnacionales de jurisdicción en materia de ciberdelincuencia en la Decisión Marco 2005/22/JAI del Consejo, de 24 de febrero, relativa a los ataques contra sistemas de información, en cuyo art, 10.4 se disponía que «Cuando una infracción sea competencia de más de un Estado miembro y cualquiera de estos Estados pueda legalmente inicial acciones judiciales por los mismos hechos, los Estados miembros de que se trate colaborarán para decidir cuál de ellos iniciará acciones judiciales contra los autores de la infracción, con el objetivo de centralizar, en la medida de lo posible, dichas acciones en un solo Estado miembro. Con este fin, los Estados miembros podrán recurrir a cualquier órgano o mecanismo creado en el marco de la Unión Europea para facilitar la cooperación entre sus autoridades judiciales y la coordinación de sus actuaciones». Como ya se indicó, la vigente Directiva 2013/40/UE, de 12 de agosto, que sustituye a la Decisión Marco 2005/22/JAI, se remite en este punto a la Decisión Marco 2009/948/JAI, de 30 de noviembre de 2009, sobre Prevención y Resolución de Conflictos de Ejercicio de Jurisdicción en los Procesos Penales.

sistema rígido de jerarquía, sino de un esquema de eficacia a partir de unas reglas orientadoras y de una fijación consensual de la competencia en caso de litispendencia internacional. En segundo lugar, la recomendación explícita de la vía del consenso es un primer paso importante para la solución de los conflictos penales de jurisdicción en materia de cibercriminalidad. No obstante, se trata de un paso todavía tímido en el Convenio de Budapest —no se señala procedimiento alguno ni compromiso expreso de los Estados para iniciarlo—, en el que se avanzará, más adelante y dentro de la Unión Europea, a través 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[69].

5. **Propuestas para un esquema de coordinación jurisdiccional internacional en la persecución y castigo eficaz de la ciberdelincuencia**

La persecución eficaz y coordinada de la ciberdelincuencia puede y debe avanzar con decisión en un espacio de cooperación internacional. Dentro de este camino, un paso importante en el marco de cualquier acuerdo internacional sobre ciberdelincuencia vendría constituido por dos medidas complementarias, destinadas a favorecer la coordinación jurisdiccional y la solución consensuada de los conflictos de concurrencia judicial. En primer lugar, y con vocación preventiva, cabe plantear la adopción de un acuerdo sobre los criterios de atribución preferente de la competencia de la jurisdicción penal nacional en la persecución de la cibercriminalidad. En segundo lugar, como herramienta de solución de los problemas de convergencia jurisdiccional que puedan surgir en la aplicación de los criterios competenciales previstos, conviene plantear la adopción de un procedimiento simplificado y consensuado para acordar, en cada caso y a través del diálogo entre las autoridades competentes concernidas, la jurisdicción idónea en casos de litispendencia internacional penal o conflictos negativos de competencia en procedimientos contra la cibercriminalidad[70].

5.1. *Reglas competenciales*

A) Criterios concertados de atribución jurisdiccional

Como es sabido, la determinación de los límites jurisdiccionales en la legislación interna de cada Estado se construye sobre criterios o vínculos de conexión

[69] Diario Oficial de la Unión Europea, L 328/42, de 15 de diciembre de 2009.

[70] El esquema del procedimiento que planteamos está tomado de la citada Decisión Marco 2009/948/JAI del Consejo, de 30 de noviembre de 2009. La propuesta que contiene este trabajo completa la Decisión marco, por una parte, al introducir los posibles conflictos negativos de jurisdicción, no previstos en el instrumento europeo. Incluye además una propuesta para el problema de los delitos conexos, la ampliación de la información procesal de intercambio en el trámite inicial, y la posibilidad de acudir a la mediación o al arbitraje, opción tampoco prevista en la referida Decisión marco.

asentados en la tradición jurídica que, con carácter general, tienen su base en la soberanía nacional, en la jurisdicción sobre los propios nacionales, en la protección de las víctimas nacionales, y en la protección de los intereses nacionales. Conscientes los Estados de la posible convergencia jurisdiccional en determinados casos, suelen graduar tales criterios introduciendo el principio de subsidiariedad en concordancia con el de reciprocidad para fueros distintos del de territorialidad[71].

Los fueros tradicionales están pensados fundamentalmente para una delincuencia territorialmente localizada, resultando excepcional y subsidiaria la competencia judicial del Estado en supuestos de extraterritorialidad. Sin embargo, la transnacionalidad es uno de los rasgos típicos de la ciberdelincuencia lo que aconseja la introducción de precisiones en la formulación de los fueros de competencia judicial internacional para evitar u orientar la solución de los supuestos de litispendencia internacional.

En este sentido, debe señalarse que la determinación de la jurisdicción idónea en materia de ciberdelincuencia ha de basarse en el principio de soberanía judicial nacional, entendido tal principio como la afirmación de la competencia penal nacional para conocer de todos los delitos previstos en un determinado acuerdo internacional cuando concurra alguno de los elementos de conexión jurisdiccional: territorio, nacionalidad de los sujetos pasivos, nacionalidad de las víctimas y protección de los intereses nacionales. No obstante, este principio de soberanía nacional debe atemperarse al reconocer, de manera preferente, la preeminencia de la competencia judicial del Estado en cuyo territorio haya sido cometido el delito. Por su parte, el respeto al principio de reciprocidad explica que los demás criterios de asignación de la competencia judicial nacional deban tener la consideración de fueros subsidiarios, en los que la asunción de la competencia depende de que el hecho no haya sido juzgado previamente en otro Estado.

Todo acuerdo internacional en esta materia debiera comenzar con una cláusula inicial en la que se afirme la competencia judicial nacional de cada Estado para el enjuiciamiento de los delitos previstos en el convenio, indicando además los criterios que definen tal asignación competencial. Tales criterios, conforme a la moderna costumbre internacional, suelen ser formulados afirmando la soberanía judicial de cada Estado respecto de los delitos[72]:

a) Cometidos dentro de su territorio nacional —cláusula que incluye buques con matrícula nacional, aeronaves que naveguen con pabellón nacional, delitos

[71] Vid., entre otros, el art. 22 del Convenio de Budapest (2001); el art. 15 de la Convención de Naciones Unidas contra la Delincuencia Organizada Transnacional, o el art. 12 de la Directiva 2013/40/UE.

[72] Vid., a título de ejemplo, la ordenación de criterios de atribución judicial de la competencia transnacional en los casos de ataques contra los sistemas informáticos prevista en el art. 10 de la derogada Decisión Marco 2005/22/JAI del Consejo, de 24 de febrero, así como las reglas competenciales que sustituyen a las indicadas en la nueva Directiva 2013/40/UE, de 12 de agosto, sobre ataques contra los sistemas informáticos.

cometidos desde satélites de titularidad nacional[73], delitos cometidos a través de sistemas informáticos cuyos soportes físicos se encuentren en territorio nacional o contra sistemas informáticos situados en territorio nacional, con independencia en los dos últimos casos del lugar desde el que físicamente actúe el autor—.

b) Cometidos por sus nacionales fuera del territorio nacional.

c) Cometidos contra sus nacionales fuera del territorio nacional —esta cláusula supone una moderna apuesta por la protección de las víctimas, que comienza a aparecer en algunos convenios internacionales[74]—.

d) Cometidos contra intereses nacionales desde fuera del territorio nacional.

e) Cometidos en beneficio de una persona jurídica con domicilio social en alguno de los de los Estados parte del acuerdo.

En función del principio de subsidiariedad, todo Estado miembro podrá decidir si aplica o no, y si solo las aplica en casos o circunstancias determinados, las normas de competencia contempladas en las letras b), c) y d) en el supuesto de que los delitos previstos en el acuerdo correspondiente se cometan fuera de su territorio[75].

Las reglas concertadas de extensión y límites de la jurisdicción nacional deben concluir con una cláusula de cierre en la que se señale que cada Estado parte del acuerdo debe adoptar las medidas necesarias para afirmar y ejercer su jurisdicción respecto de los delitos previstos en el acuerdo cuando el presunto autor se halle en su territorio y no pueda ser extraditado a otro Estado parte.

B) Criterios orientativos de preferencia jurisdiccional en caso de concurrencia

A fin de prevenir un posible conflicto de jurisdicción o para lograr un acuerdo que solucione el que haya surgido, el acuerdo debería contemplar reglas específicas que precisen el fuero preferente territorial, y que sirvan como criterios para la determinación consensuada de la jurisdicción idónea[76]. La tradicional apuesta por el *forum delicti commissi* como fuero preferente en la jurisdicción internacional

[73] La referencia a los satélites, acertada si tenemos en cuenta la arquitectura de comunicaciones que utilizan las nuevas tecnologías, aparece en el Proyecto Stanford de Convenio Internacional para la lucha contra la Cibercriminalidad y el Ciberterrorismo [art. 5.1 a)].

[74] Vid., entre otros, los arts. 15.2 a) de la Convención de Naciones Unidas contra la Delincuencia Organizada Transnacional, y 42.2 a) de la Convención de Naciones Unidas contra la Corrupción.

[75] La persecución en estos casos queda sujeta a dos condiciones: la doble incriminación y la falta de persecución en el Estado en el que se ha cometido el delito.

[76] Las aportaba, aunque de forma llamativamente escueta y condicionada en su aplicación a la voluntad de las partes, la Decisión Marco 2005/222/JAI, del Consejo, de 24 de febrero, sobre ataques contra los sistemas de información. Tales reglas se formulaban en orden consecutivo con el siguiente tenor: a) El Estado miembro en cuyo territorio se hayan cometido las infracciones; b) El Estado miembro del que sea nacional el autor y c) El Estado miembro en el que se haya encontrado al autor. El problema fundamental que este modo de afrontar el problema de la concurrencia jurisdiccional plantea no es ya que su aplicación quede a la voluntad de los Estados, sino que dicho esquema no aporta criterios imprescindibles para determinar en qué lugar ha de entenderse cometido el delito, que es el problema fundamental en la delincuencia informática transnacional. Sobre estos criterios vid. RODRÍGUEZ BERNAL, «Los cibercrímenes…», cit., pág. 27.

debe pues completarse con criterios orientadores para la concreción del lugar en que debe entenderse cometido el delito[77]. Unos criterios cuya ausencia provoca de ordinario frecuentes conflictos de jurisdicción y de competencia interna en los Estados[78].

En aquellos delitos de actividad que prevén una dinámica compleja de comisión, con conductas encadenadas que pueden ser desarrolladas en territorios de distintos Estados y con resultados también producidos en diferentes Estados, hay que acudir a la llamada teoría de la ubicuidad. Conforme al criterio de la ubicuidad, el delito puede entenderse cometido tanto en el lugar —o lugares— en que se ha desarrollado la conducta como en el lugar —o lugares— en que se haya producido el resultado, caso de que unos y otros estén situados en los territorios de distintos Estados[79].

[77] Vid. Informe de Eurojust de 2003 (Anexo), págs. 60 y ss. Para Eurojust, el principio general debe ser que 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.

[78] La práctica judicial española ofrece frecuentes ejemplos de los problemas que plantea la ausencia de una definición legal del lugar en que se entiende cometido el delito. Como es sobradamente conocido, ante laguna normativa, la jurisprudencia toma como referencia los criterios del resultado, de la actividad y de la ubicuidad, que son criterios orientativos, construidos caso a caso, para determinar en función del tipo y de la dinámica delictiva, dónde debe entenderse cometido cada delito. Sobre la aplicación de estos criterios en materia de criminalidad informática vid. CORCOY BIDASOLO, «Problemática de la persecución…», cit., págs. 31 y ss.

[79] Es el criterio que acoge la jurisprudencia española en materia de ciberdelincuencia. A la hora de determinar la competencia de los tribunales españoles en los llamados "delitos informáticos" cometidos a través de redes de comunicaciones, en los que la localización geográfica del lugar de comisión resulta especialmente difícil dada la dispersión territorial de la mayor parte de los elementos del delito —inicio de la acción delictiva, ubicación de los servidores, recepción y transmisión de la información, daños producidos a las víctimas, beneficio obtenido por el autor—, la jurisprudencia viene acogiendo pacíficamente la teoría de la ubicuidad para admitir la jurisdicción de los tribunales españoles, cuando alguno de los elementos sustanciales de la actividad delictiva —actos ejecutivos de la comisión del delito, resultado dañoso, beneficio o lucro de los autores— se haya cometido en España. Una teoría asentada sobre el parecer común del Pleno de la Sala Segunda del Tribunal Supremo a partir del acuerdo no jurisdiccional de 3 de febrero de 2005, conforme al cual «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.» Entre las sentencias del Tribunal Supremo, vid., por todas, la STS de 12 de julio de 2009, «en el motivo segundo en concreto, cuestiona la competencia de los Tribunales españoles para conocer de los delitos enjuiciados […] lo cierto es que al resultar de aplicación, para la determinación de la jurisdicción nacional competente, el principio de "ubicuidad", según el cual puede atribuirse aquella a cualquiera de los órganos territoriales de los lugares donde se cometieron actos ejecutivos del delito y en este caso, como con tanto acierto indica el Fiscal en su escrito de impugnación del Recurso, gran parte de esos actos ejecutivos de los delitos de las defraudaciones se han cometido en nuestro país, entre otros los estrictamente consumativos de los ilícitos como el hecho de quedar el dinero defraudado a disposición del sujeto activo precisamente en España, es evidente la competencia de nuestros Tribunales para conocer de este enjuiciamiento.» No han faltado sin embargo pronunciamientos de nuestros tribunales en los que la competencia se define de manera más precisa. Así sucede, por ejemplo, en los AATS de 22 de julio de 2002, de 19 de enero de 2004 o de 3 de abril de 2006, en los que se señala que el órgano judicial competente es aquel que se corresponde con el momento de la inclusión en la red de la información objeto de la causa, entendiendo por lugar de comisión del delito la ciudad en la que la sociedad mercantil infractora tenía su sede y donde confeccionó la página web desde la que se realizaron los hechos. Sobre la aplicación de la teoría de la ubicuidad para la determinación de la competencia jurisdiccional en materia de delitos informáticos, vid. ANARTE, «Incidencia de las nuevas

No obstante, dicha teoría, al entender competentes a todas las jurisdicciones en las que se desarrolla alguna parte de la acción, no termina de resolver el problema de la posible concurrencia jurisdiccional[80]. Cabría, en este sentido, precisar algo más pudiendo acordar que, en estos casos, las autoridades competentes de cada Estado deberán atender a la dinámica comisiva específica, al valor y rango de la intervención de los partícipes y, especialmente, al criterio de la acción decisiva, dominante o desencadenante[81].

Para los delitos de mera acción, en los que la conducta pueda entenderse desarrollada en territorios de diversos Estados, se propone el citado criterio de la acción relevante o determinante, entendiendo por tal la que domina la conducta, la controla, la desencadena, la coordina, la que integra la parte sustancial de la acción y localiza la decisión de la acción. Se trata de un concepto orientativo, que debe ser aplicado caso a caso (v.gr, con organizaciones criminales, acuerdo de actividades, reparto de roles, conductas en cascada...). En los delitos de mera conducta, los criterios deben completarse con una orientación pensada para la ciberdelincuencia: la acción tanto se ancla en el lugar en el que esté físicamente el sujeto, como en el lugar en los que estén los equipos o sistemas a través de los que el sujeto actúe. Se reconoce así el *modus operandi* en el ciberespacio, en el que hay una conducta física y una acción virtual, o puesta en acción virtual. Se incluye por ello en el lugar de la acción el lugar en el que estén físicamente los equipos, sistemas o terminales a través de los que el sujeto actúe o se sirva —servidores, plataformas, ordenado-

tecnologías en el sistema penal. Aproximación al Derecho Penal en la sociedad de la información», en *Derecho y conocimiento*, 1, 2002, pág. 208; vid. también DE URBANO CASTRILLO, «Infracciones patrimoniales por medios informáticos y contra la información como bien económico», en *Delitos contra y a través de las nuevas tecnologías ¿Cómo reducir su impunidad?*, Cuadernos de Derecho Judicial, Madrid, 2006, pág. 157.

[80] Es lo que sucede, por ejemplo, con el Conjunto de Herramientas para la Legislación sobre Ciberdelito de la Unión Internacional de Telecomunicaciones, en cuya sección 21, letra f, se adopta expresamente la teoría de la ubicuidad sin establecer un orden de preferencia entre los diferentes lugares en los que puede entenderse cometido el delito: «el delito se comete en cada lugar donde el infractor haya actuado (i) a través de su presencia física; (ii) a través del uso internacional de los equipos, software o datos, o (iii) en cualquier lugar en el que la acción resultante es un elemento del delito, de conformidad con las secciones 2 a 10 de esta Ley, se produjo o se habría producido de acuerdo con la comprensión del infractor». Sobre los problemas que la disposición citada puede suscitar en su aplicación práctica vid. VELASCO SAN MARTÍN, *La jurisdicción y competencia*…, cit., págs. 125 y 126.

[81] Para Eurojust, los criterios que deben tenerse en cuenta, sin una ordenación de preferencia, para la designación de la jurisdicción idónea deben ser los siguientes: el lugar de localización del acusado; el lugar de disponibilidad de los testigos y demás fuentes de prueba; el lugar en el que se pueda ejercer la jurisdicción sin dilaciones excesivas; el lugar en el que el ejercicio de la jurisdicción sea compatible con el interés de las víctimas y, finalmente, el lugar en el que resulte posible adoptar medidas cautelares eficaces para asegurar las resultas del juicio o la intervención de bienes o productos del delito. Según la propuesta contenida en el Proyecto de Convenio Stanford (art. 5.4), el orden de prioridad debiera ser el siguiente: «en primer lugar, el Estado Parte en el que el presunto delincuente estaba físicamente presente cuando se cometió el presunto delito; en segundo lugar, el Estado Parte donde se sufrió daños considerables como consecuencia del presunto delito; en tercer lugar, el Estado Parte de la nacionalidad dominante del presunto delincuente; en cuarto lugar, todo Estado Parte donde el presunto delincuente pueda estar ubicado y, en quinto lugar, cualquier otro Estado Parte con una base razonable para ejercer su jurisdicción».

res, terminales, sistemas, etc.—. Los citados instrumentos de la acción deben ser centros virtuales de actuación y no meros canalizadores de órdenes o instrucciones. Hablamos en estos casos de acción dirigida remotamente[82].

Cuando el delito sea de resultado, la aplicación de la teoría de la ubicuidad —distintos lugares en que se producen resultados, distintos lugares de acción y resultado— puede requerir criterios complementarios de orientación para la determinación de la jurisdicción idónea: ¿en el lugar de la acción o en el lugar del resultado? Siendo ambos lugares de comisión: ¿cuál resulta preferible? En estos casos no hay una solución rígida que pueda ser formulada a priori con criterios normativos. Son preferibles los criterios orientativos que, aplicados al caso concreto con sus circunstancias, ayuden a convenir la jurisdicción idónea[83].

En situaciones como las descritas podrán tenerse en cuenta, además de los ya apuntados, los siguientes criterios:

* El lugar que proporcione mayor facilidad para la investigación. En concreto, en el lugar en el que se hayan encontrado o puedan encontrarse las fuentes de prueba y, dentro de ellas, las que puedan considerarse más relevantes o decisivas[84].

* El lugar del resultado, cuando este ofrezca un referente territorial claro —quizá con más facilidad en algunos casos que la propia acción—. En casos de pluralidad de resultados se sugiere el criterio clásico del resultado de mayor gravedad.

* El lugar de residencia de la víctima, cuando el lugar del resultado y el lugar de residencia de la víctima no coincidan. La preferencia por la residencia de la víctima tiene en cuenta las facilidades de acceso a la tutela del perjudicado, además de valorar el lugar donde ha podido producirse la afectación principal al ser una pluralidad de territorios los de posible resultado —v. gr. difamación—. En los casos de pluralidad de víctimas se tendrán en cuenta los criterios combinados del lugar donde resida el mayor número de víctimas o el lugar del resultado de mayor gravedad.

* El lugar en que se haya detenido al presunto autor. Este criterio puede contri-

[82] Como señala el art. 12 de la citada Directiva 2013/40/UE, los Estados establecerán su competencia cuando, respecto de los delitos previstos en la misma, cuando: «a) el autor cometa la infracción estando físicamente presente en su territorio, independientemente de que la infracción se cometa o no contra un sistema de información situado en su territorio; b) la infracción se cometa contra un sistema de información situado en su territorio, independientemente de que el autor cometa o no la infracción estando físicamente presente en su territorio».

[83] Los criterios de determinación del orden de preferencia propuestos por el ya citado Proyecto Stanford de Convenio Internacional para la Protección frente a la Ciberdelincuencia y el Ciberterrorismo, se formulan en los siguientes términos: «Cada Estado Parte ejercerá sus derechos y cumplirá sus obligaciones en virtud del presente Convenio en la medida de lo posible de acuerdo con el siguiente orden de prioridad de la competencia: en primer lugar, el Estado Parte en el que el presunto delincuente estaba físicamente presente cuando se cometió el presunto delito; en segundo lugar, el Estado Parte donde se sufrió daños considerables como consecuencia del presunto delito; en tercer lugar, el Estado Parte de la nacionalidad dominante del presunto delincuente; en cuarto lugar, todo Estado Parte donde el presunto delincuente pueda estar ubicado y, quinto, cualquier otro Estado Parte con una base razonable para ejercer su jurisdicción».

[84] Vid. los criterios de solución de conflictos de jurisdicción en materia penal aportados por el citado Informe de Eurojust de 2003 (pág. 64).

buir a despejar el lugar idóneo para enjuiciarlo entre los lugares en que haya podido cometer la acción, o unir el lugar de resultado con el lugar de detención[85].

* El domicilio de la persona jurídica beneficiaria, de modo que podrá ser un criterio que decante la jurisdicción del lugar de la acción o del resultado si, en alguno de ellos, se encuentra, además, el domicilio de la persona jurídica.

* El último de los criterios podría ser una cláusula general que orientara la preferencia entre los diversos lugares de desarrollo de la acción, entre los diferentes lugares en que se hayan podido producir la acción y el resultado, o entre los diversos lugares en los que se hayan registrado los resultados del delito, tomando en consideración las garantías procesales, y en concreto el acceso a la tutela de las partes y el más eficaz desarrollo del proceso[86].

5.2. *Procedimiento de solución consensuada de conflictos internacionales de jurisdicción en el ámbito de la ciberdelincuencia*

Las reglas y criterios sugeridos en los apartados anteriores pueden contribuir a prevenir los conflictos de jurisdicción en el marco de un acuerdo internacional sobre ciberdelincuencia, pero no evitan que estos conflictos puedan surgir en determinados casos[87]. Es posible que, aplicando las referidas reglas y criterios en un caso concreto, dos o más Estados partes de un acuerdo internacional puedan considerarse competentes para conocer de alguno de los delitos previstos en el mismo, iniciando paralelamente acciones judiciales por los mismos hechos y contra los mismos sujetos, surgiendo entonces un problema de litispendencia internacional[88]. Parece razonable que, en tal caso y ante la falta de una autoridad judicial jerárquicamente superior, los Estados —preferiblemente las autoridades judiciales de los Estados—colaboren para decidir cuál de ellos debe asumir el procedimiento

[85] Este criterio aparecía en la derogada Decisión Marco 2005/222/JAI, relativa a los Ataques contra Sistemas de Información (art. 10.4), y antes en la Decisión Marco 2002/475/JAI, relativa al Combate contra el Terrorismo (art. 9.2). También figura como uno de los criterios propuestos por Eurojust en el ya citado Informe Anual de 2003 (pág. 63).

[86] Vid. STJUE, de 12 abril de 2012, caso Wintersteiger vs. Products 4U.

[87] Sucede con relativa frecuencia en el ámbito interno, en el que, a pesar de las normas sobre competencia territorial, surgen cuestiones de competencia derivadas de la diferente interpretación de las reglas competenciales en casos concretos. Pero, a diferencia del ámbito internacional, en los ordenamientos internos existe una autoridad judicial que resuelve de manera imperativa los conflictos de concurrencia competencial que se susciten entre los órganos judiciales nacionales. Por el momento, y salvo sectores jurídicos concretos en ámbitos regionales integrados (v.gr. UE), la cooperación, el diálogo y el acuerdo son los instrumentos de los que se vale la comunidad internacional para la solución de los conflictos de concurrencia jurisdiccional penal. Para facilitar el consenso y el acuerdo resulta fundamental, no solo una tipificación armonizada de los delitos en un determinado campo del derecho penal, sino también la aceptación de reglas y criterios consensuados de preferencia jurisdiccional, de cesión de la competencia judicial nacional y de reconocimiento mutuo de resoluciones judiciales.

[88] Por procedimientos paralelos cabe entender los procedimientos penales que se tramiten simultáneamente en dos o más Estados miembros, por los mismos hechos y seguidos contra la misma o mismas personas. A estos efectos, se entiende que la litispendencia existe desde la incoación de la fase de investigación preliminar y subsiste hasta que se dicte sentencia en primera instancia.

contra los presuntos autores del delito con el objetivo de centralizar dichas acciones, en la medida de lo posible y con respeto a los derechos y garantías internas previstas en los respectivos textos constitucionales, en la jurisdicción del Estado que se considere más idónea para el enjuiciamiento y fallo de la causa. Del mismo modo debiera procederse cuando, tras los oportunos contactos, dos o más Estados parte declinen abrir procedimiento por alguno de los delitos previstos en el acuerdo.

Ante tales supuestos, conviene incluir en las propuestas de convenios internacionales sobre persecución y castigo de la ciberdelincuencia un procedimiento consensual, flexible y simplificado para la prevención y solución de conflictos derivados, tanto de la concurrencia de jurisdicciones nacionales, como de la renuncia de las autoridades competentes a la persecución de hechos constitutivos de delitos previstos en el acuerdo[89]. Se pretende prevenir de este modo la litispendencia penal internacional en materia de ciberdelincuencia, así como el vacío en la persecución, abriendo —forzando mejor dicho— un protocolo de comunicación entre las autoridades competentes de los Estados que permita acordar, con base en criterios de eficacia procesal y protección suficiente de las garantías, la jurisdicción nacional idónea tanto en casos de conflictos positivos como negativos de jurisdicción.

A) Fundamento y estructura

El fundamento o principio sobre el que debe basarse la solución de los eventuales conflictos positivos o negativos de jurisdicciones nacionales en el ámbito de la cibercriminalidad es el consenso, esto es, la predisposición y la capacidad para alcanzar acuerdos mediante el diálogo y la transacción. El acuerdo sobre idoneidad jurisdiccional puede lograrse, en el marco de un acuerdo internacional, bien a través de contactos directos entre las autoridades competentes de los Estados, bien utilizando técnicas de mediación, o incluso de arbitraje internacional, predeterminadas estas últimas en el acuerdo correspondiente y, tal vez en un futuro, gradualmente vinculantes[90]. Ambas vías son compatibles con el principio de garantía de la

[89] La alusión al consenso para la solución de los conflictos internacionales de jurisdicción surgidos en la persecución y castigo de la ciberdelincuencia es frecuente en los acuerdos internacionales en materia de cooperación judicial penal; vid., a título de ejemplo, el art. 22 del Convenio de Budapest; el art. 15.5 de la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional; art. 42.5 de la Convención de Naciones Unidas contra la Corrupción; art. 31.4 del Convenio del Consejo de Europa sobre la Lucha contra la Trata de Seres Humanos; art. 14.5 del Convenio del Consejo de Europa contra el Terrorismo; art. 25.8 del Convenio del Consejo de Europa sobre la Protección de los Niños. Lo que ya no es tan frecuente es la regulación de un procedimiento para encauzar los contactos entre los Estados, ni la obligatoriedad, al menos, de iniciarlo en caso de conflicto, tal y como se prevé en la ya citada 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.

[90] La propia Decisión Marco 2009/948/JAI del Consejo sobre conflictos de jurisdicción en materia penal, sugiere la posibilidad de intervención de organismos encaminada a facilitar la solución del conflicto entre los Estados. Como se prevé en su art. 12.2 «Cuando no haya sido posible lograr un consenso de conformidad

soberanía jurisdiccional de cada Estado, que no implica exclusividad, y que se ejercerá con arreglo a su derecho interno, a través de las correspondientes autoridades competentes y en el marco del procedimiento que internamente establezca.

En cuanto a la estructura del procedimiento, resulta conveniente su división en dos fases. En una primera fase es necesario constatar, a través del intercambio de información procesal, la existencia de procedimientos penales paralelos en dos o más Estados parte, incoados por los mismos hechos y seguidos contra los mismos sujetos, o bien la negativa de dos o más autoridades competentes para asumir el conocimiento de una concreta noticia delictiva referida a alguno de los tipos penales recogidos en el acuerdo. Constatada la existencia de litispendencia o la negativa a asumir la competencia, debe abrirse una segunda fase que permita alcanzar un acuerdo entre las distintas autoridades competentes de los Estados miembros a fin de determinar, consensuadamente y con base en la interpretación concertada de las reglas y criterios de determinación de la jurisdicción competente que prevea el acuerdo, la jurisdicción idónea en cada caso[91].

B) Fase inicial: constatación de la litispendencia o de la existencia de conflicto negativo de jurisdicción y posible solución espontánea

La incoación del procedimiento, para la cual estarán legitimadas las autoridades competentes que cada Estado designe[92], tiene como presupuesto la noticia de una posible litispendencia o el rechazo inicial de un Estado a asumir el conocimiento del asunto[93]. La noticia de una posible litispendencia, o del rechazo inicial al ejercicio de la jurisdicción por otro Estado puede llegar a la autoridad competente a

con el art. 10, cualquiera de las autoridades competentes de los Estados miembros implicados dará traslado, si procede, del asunto a Eurojust, en caso de que Eurojust sea competente para actuar en virtud del art. 4, apartado 1 de la Decisión de Eurojust». A tal efecto, en la exposición de motivos que precede a la Decisión Marco de 2009 (14) se señala que «puesto que Eurojust está especialmente capacitado para facilitar asistencia en la resolución de conflictos de jurisdicción, el traslado de un caso a Eurojust debe ser el proceder habitual cuando no haya sido posible alcanzar un consenso».

[91] Se entiende por jurisdicción idónea aquella que está en las mejores condiciones para afrontar la persecución y castigo de una infracción determinada prevista en un convenio internacional con la máxima eficacia procesal y con el máximo respeto a las garantías procesales de las partes y las víctimas. El concepto de jurisdicción idónea se utiliza, no como un criterio excluyente ni jerárquicamente preferente para determinar la competencia, sino como valor de acuerdo basado en la idea de eficacia, de adecuación, de confianza y de reconocimiento mutuo.

[92] En los convenios internacionales de cooperación judicial es habitual distinguir entre autoridades centrales, que son los órganos que cada Estado miembro establezca para actuar como puntos únicos de contacto autorizados a fin de recibir, canalizar internamente y remitir información en relación con los procedimientos de cooperación, asistencia y comunicación previstos en el convenio, y autoridades competentes, que son las que cada Estado designe —preferentemente autoridades judiciales o miembros del Ministerio Fiscal— como facultadas para solicitar y remitir información acerca de procesos penales en curso en materia de ciberdelincuencia, así como los órganos facultados para acordar la jurisdicción idónea en casos de conflictos de jurisdicción dentro del ámbito de aplicación material del convenio

[93] Por litispendencia internacional debe entenderse la apertura y tramitación simultánea, en dos o más Estados parte del acuerdo, de dos o más procesos penales seguidos por los mismos hechos y dirigidos contra la misma o mismas personas. Por conflicto negativo de competencia judicial internacional debe entenderse el rechazo de la atribución competencia por las autoridades de los Estados requeridos para su intervención.

través de cualquiera de las diligencias que practique durante la tramitación del procedimiento, o mediante la recepción de solicitudes de asistencia judicial internacional. La primera fase del procedimiento debe pues dirigirse a constatar la incoación de procedimientos paralelos iniciados en dos o más Estados por los mismos hechos y contra los mismos sujetos, o la existencia de un conflicto negativo provocado por el inicial rechazo de dos o más Estados a ejercer su jurisdicción ante la noticia de la posible comisión de delitos previstos en el acuerdo.

Esta primera fase tendrá un doble contenido o función. En primer término, comprenderá el intercambio de la información procesal básica destinada a constatar la existencia inicial de un conflicto positivo o negativo de jurisdicción. A través de la correspondiente autoridad central, la autoridad requirente que promueva el procedimiento deberá cursar solicitud de información[94], en la que constará la identificación de la autoridad requirente, los datos básicos del procedimiento, y una justificación suficiente de la solicitud de la información[95].

Junto a ello, también la primera fase debiera permitir la adopción de un acuerdo inicial espontáneo, de tal manera que, tras un primer intercambio de información y sin más trámites, uno de los Estados concernidos reconozca la preferencia jurisdiccional del otro Estado, o asuma la jurisdicción en caso de conflicto negativo.

Pieza importante del procedimiento consensual de solución de conflictos internacionales de jurisdicción en materia de ciberdelincuencia es el trámite de incoación, que debe tener carácter obligatorio e inmediato[96]. Ante la noticia de un posible conflicto positivo o negativo de jurisdicción, las autoridades competentes de cada Estado deberán poner en marcha el procedimiento consensual de solución de conflictos mediante un doble trámite: a) dejar constancia de la noticia del

[94] Debidamente protocolizada a través de los formularios que se establezcan en los anexos al convenio.

[95] El contenido mínimo de la información solicitada que resulta necesaria para valorar la litispendencia será:

.- Hechos por los que se procede

.- Vía de recepción de la noticia delictiva

.- Sujeto o sujetos pasivos a los que se atribuye participación en los mismos

.- Identificación de las víctimas en su caso, y personación de las mismas en el procedimiento

.- Resoluciones parciales de archivo que en su caso se hayan dictado respecto de alguno o algunos de los imputados

.- Fecha de incoación del procedimiento

.- Situación personal de los imputados

.- Estado del procedimiento

.- Concurrencia de delitos conexos

La propuesta de este contenido mínimo amplía el que figura en el art. 8 de la citada Decisión Marco 2009/948.En el caso de eventuales conflictos negativos, la información se completará con la identificación de la noticia delictiva con sus circunstancias objetivas y subjetivas, así como la confirmación de la negativa del Estado requerido a ejercer su jurisdicción.

[96] Al igual que para la autoridad requirente existe obligación de solicitar información ante la noticia de una posible litispendencia internacional, o ante la convicción de la existencia de una jurisdicción nacional idónea distinta de la propia, debe existir para la autoridad requerida, como regla general, obligación de facilitar la información solicitada, o de responder a la solicitud de transmisión del procedimiento.

posible conflicto y b) cursar comunicación y petición de información al Estado o Estados concernidos a fin de verificar la existencia del conflicto y explorar, en su caso, la posible solución espontánea del mismo.

El trámite de intercambio de información procesal producirá distintos efectos en función de la posición que adopte el Estado requirente ante la respuesta que ofrezca el Estado requerido. En primer lugar, el procedimiento concluiría sin más trámites si, en caso de posible litispendencia, el Estado requerido certifica la inexistencia en su territorio de procedimiento iniciado, o si decide la incoación de procedimiento en supuestos de posible conflicto negativo de jurisdicción. En segundo lugar, si el Estado requerido confirma la existencia de procedimiento incoado en su territorio o si mantiene la negativa a incoarlo en casos de conflicto negativo, el Estado requirente habría de remitir completa la información procesal que posea e intentará un acuerdo inicial espontáneo. En su defecto, promoverá el inicio de la segunda fase del procedimiento —fase de composición— a la que nos referiremos a continuación.

Finalmente, el acuerdo debe prever que, en determinadas circunstancias, el Estado requerido pueda diferir la transmisión de la información procesal solicitada, limitar la que comunica o denegar la transmisión. Los tratados internacionales sobre cooperación judicial suelen señalar como motivos para denegar solicitudes de colaboración el peligro para la seguridad nacional, el posible perjuicio grave para la investigación o la generación de un alto riesgo para víctimas, testigos o terceras personas. Si la denegación es definitiva, el Estado requirente debe decidir si renuncia o mantiene su jurisdicción, aceptando en este segundo caso la tramitación de procedimientos paralelos. Si la denegación es temporal, o la información transmitida es limitada, deberá el Estado requirente optar[97] entre continuar el procedimiento incoado con normalidad, o suspenderlo, bien de modo inmediato (con práctica de diligencias urgentes y medidas cautelares imprescindibles), bien cuando llegue a la fase de juicio oral, quedando en ambos casos a la espera de una respuesta definitiva del Estado requerido.

C) Fase de composición y conclusión del procedimiento

Coincidiendo ambos Estados en la existencia de litispendencia o de conflicto negativo, deberán iniciar la fase de composición a fin de acordar consensuadamente la jurisdicción idónea para continuar o asumir la tramitación del procedimiento, así como las medidas concretas que, en su caso, deban disponerse para la acumulación[98].

Resulta razonable disponer que, en tanto se tramita la fase de composición, cada

[97] A la hora de tomar una decisión, deberá valorar el Estado requirente el plazo de prescripción del delito así como la obtención, conservación y disponibilidad futura de las fuentes de prueba.

[98] El acuerdo internacional debiera establecer un plazo límite para esta fase, que podría oscilar razonablemente entre los dos y los cuatro meses.

autoridad competente deba, en caso de litispendencia, continuar con la tramitación del procedimiento respectivo, adoptando las medidas de prevención necesarias para el aseguramiento del imputado y las fuentes de prueba, remitiéndose recíprocamente información sobre las medidas adoptadas en cada uno de ellos[99].

A la hora de buscar un acuerdo jurisdiccional, las autoridades competentes deberán tener en cuenta el estado de cada procedimiento, las partes personadas, la posible conexidad entre los delitos[100], y las fuentes de prueba obtenidas en cada uno de ellos, valorando especialmente la importancia de la información probatoria obtenida, su conservación y su futura eficacia de conformidad con el derecho interno respectivo.

Cuando las autoridades competentes alcancen un acuerdo sobre la jurisdicción idónea, deberán ponerlo de manifiesto a las partes en cada uno de los procedimientos para que, en función de las normas procesales internas, puedan ejercer el derecho a los recursos. Sería altamente recomendable que, en estos supuestos, se dispusiera un trámite de urgencia para la tramitación y la decisión del recurso. En estos casos, el acuerdo supondrá la acumulación de todas las causas abiertas, y sus correspondientes diligencias, ante la autoridad competente que se haya designado como jurisdicción idónea.

Si las autoridades competentes constatan la imposibilidad de llegar a un acuerdo sobre la jurisdicción idónea, deberán certificar la falta de acuerdo y poner fin al procedimiento. Esta decisión no impedirá que, con posterioridad, y a la vista de un eventual cambio de circunstancias, pueda volver a iniciarse la fase de composición a instancia de cualquiera de los Estados concernidos.

Hasta el momento, la comunidad internacional no ha previsto otro sistema para la solución de conflictos de jurisdicción en materia penal que el procedimiento de consultas, meramente apuntado en la mayor parte de los convenios internacionales sobre cooperación judicial penal, y específicamente desarrollado en la Decisión marco europea de 2009 sobre conflictos de jurisdicción penal. Como ya indicamos anteriormente, en la solución de conflictos internacionales de jurisdicción penal, señaladamente en materia de ciberdelincuencia, conviene avanzar, a corto y medio plazo, por el camino de las soluciones consensuadas, incorporando herramientas que favorezcan o impulsen el acuerdo. El recurso a la mediación o al arbitraje en caso de conflictos jurisdiccionales, apoyada en la idea del juez nacional como juez internacional, puede ser una buena opción, especialmente si viene acompañada de

[99] La tramitación de un procedimiento de solución de conflictos de jurisdicción no debe impedir, al contrario, la tramitación simultánea de solicitudes de cooperación y asistencia judicial en los términos previstos en los acuerdos internacionales que vinculen a los respectivos Estados.

[100] Cuando alguno de los procedimientos en curso incorpore delitos conexos, las autoridades competentes deliberarán sobre la posibilidad de desglosar los mismos sin ruptura de la continencia de la causa, de modo que puedan ser enjuiciados separadamente. De no ser así, podrá prosperar el acuerdo cuando la jurisdicción considerada idónea por las respectivas autoridades, sea además la competente para el enjuiciamiento de los delitos conexos.

estructuras estables de gestión del acuerdo internacional que faciliten el acceso a estos métodos de solución —v.gr. mediante la designación de mediadores o árbitros—, y verifiquen su utilización cuando haya sido establecida como vinculante.