TRABAJO FIN DE GRADO

GRADO EN DERECHO

CURSO ACADÉMICO 2018-2019

CONVOCATORIA JUNIO

TÍTULO:

CONFLICTOS DE JURISDICCIÓN EN MATERIA DE CIBERDELITOS: PROBLEMÁTICA Y SOLUCIONES

APELLIDOS/NOMBRE ESTUDIANTE: ARRAZOLA RUIZ, SARA

DNI:

DOBLE GRADO QUE CURSA: DERECHO Y RELACIONES INTERNACIONALES

APELLIDOS/NOMBRE TUTOR: ARROYO ROMERO, JAVIER

Fecha: 4 de junio de 2019.

ÍNDICE

ABREVIATURAS

Código Penal español	CP
Compañía de acceso a Internet	ISP
Constitución Española	CE
Convenio Europeo de Derechos Humanos	CEDH
Corte Penal Internacional	CPI
Derecho Internacional Humanitario	DIH
Declaración Universal de los Derechos Humanos	DUDH
Government Accountability Office (EEUU)	GAO
Infraestructura Crítica Europea	ICE
Internet Protocol	IP
Orden Europea de Investigación	OEI
Pacto Internacional de los Derechos Civiles y Políticos	PIDCP
Proveedor de red dorsal	IBP
Sistema de Nombres de Dominio	DNS
Transfer Control Protocol	TCP
Tribunal Constitucional español	TC
Tribunal de Justicia de la Unión Europea	TJUE
Tribunal Supremo español	TS
Unión de Repúblicas Socialistas Soviéticas	URSS
Unión Europea	UE/ Unión

I. Introducción

El ciberespacio definido como un espacio sin límites físicos plantea varios problemas en su funcionamiento y empleo por la ciudadanía y las instituciones que ya fueron identificados por Lessig en su obra *El código y otras leyes del ciberespacio*, más concretamente ahonda en uno de los ejes del modelo de Estado liberal actual y es el conflicto entre la libertad, entendida tanto en términos mercantiles como de derechos individuales, y la potencial capacidad regulatoria estatal, supranacional e internacional. El propio Lessig resume y futuriza ese conflicto de la siguiente forma:

"nos encontramos ante… un futuro de control ejercido en gran medida mediante las tecnologías del comercio, respaldadas por el imperio de la ley. El desafío de nuestra generación es reconciliar estas dos fuerzas."[1]

La elección del enfoque planteado por Lessig en vez de un enfoque más estrictamente tecnológico parte de la necesidad de abordar el ciberespacio, no exclusivamente como una red informática, sino desde una perspectiva jurídico-política ya que la emergencia del ciberespacio en el entramado, primero científico-universitario y después social, coincide con un momento temporal de intento fallido de transición democrática por la caída del eje comunista encabezado por la Unión Soviética (en adelante URSS) y con el inicio de la globalización entendida en términos de interrelación, interdependencia e interconexión entre los agentes de la escena internacional. En definitiva, el ciberespacio se presentaba como un lugar de libertad frente a la incapacidad de los Estados no liberales por liberarse de la clase política heredada del *Politburó* o, en otras palabras,

"justo cuando comenzaba a declinar la euforia postcomunista, emergió en Occidente otra «nueva sociedad» que muchos consideraron tan apasionante como las nuevas sociedades de la Europa postcomunista."[2]

La naturaleza del ciberespacio y su intangibilidad ha determinado la existencia de dificultades jurídicas en lo que a su conceptualización como fenómeno jurídico y al tratamiento que debe hacerse de las conductas asociadas a este nuevo espacio de interacción se refiere. Hay dos ejes sobre los que recaen dichas dificultades: la superación del territorio nacional como referencia y la inmaterialidad de los intercambios de

[1] LESSIG, L.: *El código 2.0*, Ed. Traficantes de sueños, Madrid, 2009, página 24.
[2] *Íbidem*, página 32.

información que en él y a través de él tienen lugar. Estas características han supuesto un desafío en todas las disciplinas del Derecho, desde el área de Derecho privado debido al aumento de las transacciones y contratos efectuados por esta vía, hasta el área del Derecho público tanto en su vertiente nacional como internacional. Un área especialmente sensible ha sido la del Derecho Penal, concretamente, en su vertiente procesal ya que a las dificultades inherentes a procesos con características de transnacionalidad, ha incorporado problemas derivados de la falta de claridad y homogeneidad del Derecho sustantivo que inciden de forma negativa sobre la delimitación del objeto del proceso tanto a efectos de impulso del mismo, como a efectos de cumplimiento de la garantía procesal plasmada en el principio *non bis in ídem;* y problemas de investigación primero, y de actividad probatoria en otras fases del proceso, vinculados a la incapacidad de aportar indicios y pruebas dotados del carácter físico que exige la legislación del procedimiento penal tradicional. Sin dicha delimitación del objeto procesal, tampoco puede delimitarse la jurisdicción competente en tanto en cuanto, los principios de atribución de la misma en materia de ciberdelincuencia se topan con una pluralidad de criterios, una pluralidad de conexiones difusas y una ausencia de órdenes de prelación.

Teniendo en cuenta estas cuestiones, el presente trabajo se estructura de la siguiente forma: un primer capítulo dedicado al estudio del ciberespacio, de sus características, de su funcionamiento y de los debates jurídicos que suscita su naturaleza; un segundo capítulo dedicado al tratamiento jurídico-procesal del fenómeno y dividido en tres secciones; una primera dedicada a los problemas de identificación del objeto del proceso penal en los casos de ciberdelincuencia derivados de la ausencia de homogeneidad y claridad en la tipificación del fenómeno; una segunda sección que versa sobre la incidencia de la transnacionalidad y la intangibilidad en la actividad investigadora; y, finalmente una tercera sección dedicada especialmente a los conflictos de jurisdicción que se plantean una vez identificado el objeto y a las opciones planteadas por la doctrina y en algunos instrumentos internacionales.

La metodología empleada será la del estudio de una revisión bibliográfica de doctrina jurídica, justificada en la ausencia de una actividad legislativa y judicial extensa en la materia; de instrumentos internacionales, destacando el plano delimitado por Naciones Unidas, especialmente, la Oficina de Naciones Unidas contra la Droga y el Delito; la normativa del Consejo de Europa y las disposiciones desarrolladas en el seno del Espacio de Libertad, Seguridad y Justicia de la Unión Europea.

II. El concepto de ciberespacio

La primera de las cuestiones que debe ser abordada es la del espacio donde tienen lugar los conocidos como delitos informáticos o ciberdelitos. Se trata de un espacio de dimensiones ilimitadas, sin delimitaciones físicas, fundamentado en el intercambio de datos y que emplea un lenguaje basado en bits, dígase, en combinaciones de 0 y 1 que han ampliado sus posibilidades pasando de representar únicamente números y texto hasta poder crear imágenes y gráficos; en definitiva, se trata de una realidad de tipo virtual que puede, y de hecho cada vez lo hace más intensamente, interferir en el categorizado como mundo analógico. Supone, siguiendo el título de la obra de Terceiro, el paso del *homo sapiens al homo digitalis*[3], y, en términos sociales se traduce en la conversión de una sociedad analógica en una sociedad digital, dígase, según Negroponte, en una sociedad que puede ser expresada en términos de 0 y 1.[4] En términos más técnicos, la llegada del ciberespacio supuso el abandono de un sistema de red ligado a la telefonía y monodireccional hacia un sistema de código abierto basado en la transmisión y en el intercambio de paquetes de datos.

Lo cierto es que, a pesar de que el concepto de ciberespacio o de internet como red de redes tiene un componente ilimitado y abstracto, se apoya en estructuras físicas y localizables para su funcionamiento, y más concretamente, en un entramado de computadores unidos mediante cables de fibra óptica, dígase, un cable de vidrio capaz de transmitir energía lumínica a una velocidad y con una resistencia que supera a todos los sistemas de telecomunicaciones anteriormente desarrollados por el hombre.[5] Esta primera dimensión de Internet recibe el nombre de capa de infraestructuras y telecomunicaciones y está formada esencialmente por elementos objeto de derechos de propiedad e infraestructuras críticas como las antenas, los satélites, los cables o la fibra óptica.

La segunda dimensión es la conformada por los estándares y servicios técnicos y es un campo de actuación esencialmente privado donde destacan el sistema de transmisión de la información conocido como protocolo TCP/IP y la dirección IP.

[3] TERCEIRO, J.B.: *Sociedad digital: del homo sapiens al homo digitalis,* Ed. Alianza Editorial, Madrid, 1996.
[4] NEGROPONTE, N.: *Being digital,* Ed. Vintage books, Nueva York, 1996.
[5] *Íbidem,* página 70.

El primero es el protocolo básico para el tráfico, envío, reconstrucción e intercambio de datos en Internet. Está formado por la combinación del *Transfer Control Protocol* (en adelante TCP) y *Internet Protocol* (en adelante IP). Está compuesto por diferentes etapas de actuación protocolaria:

- Transporte: los datos digitales son distribuidos en distintos paquetes de bits a los que se les asigna un orden para su transmisión.
- Red: supone asignar a cada paquete de datos una dirección de destino. Tendrá que atravesar un número de nodos, dígase de dispositivos conectados a la red (internet) que sirven como punto de enlace para varios equipos informáticos, que no puede ser superior al tiempo de vida asignado en el momento de indicar el destino de los datos.
- Aplicación: supone en primer lugar, la unificación de los distintos paquetes de bits en los que se dividió la información en la fase de transporte, y, en segundo lugar, la conversión de los datos en información comprensible para el usuario.

Este protocolo permite la comunicación entre dispositivos de diversa naturaleza, con sistemas operativos distintos y que se encuentren ubicados en la misma o en distinta red, dando así a la Internet esa posibilidad de alcance global o en términos técnicos esa superación de la red local a favor de la red extensa.

La segunda, es un número único de identificación en red asignado a un equipo. Está formada por 128 bits actualmente y compuesta por un número de red y un número de nodo. Existen dos direcciones IP: una IP de carácter público que es la que se asigna al router ofrecido por una compañía que da acceso al usuario base a Internet (conocida como compañía ISP), dígase, de comercialización de acceso a la red que depende jerárquicamente de un proveedor de red dorsal (llamado compañía IBP), es decir, de una red de fibra óptica privada y propia; y una IP privada para cada dispositivo conectado a ese router. La dirección IP tiene otra utilidad y es la de identificar los servidores, dígase, los lugares de almacenamiento de las webs y demás contenidos como correos electrónicos o archivos de Internet; esa nomenclatura se sustituye por el conocido como nombre de dominio a través de un sistema de nombres de dominio (en adelante DNS).

En definitiva, el funcionamiento de ese ente inmaterial que es el ciberespacio depende de un apoyo o sustento de carácter físico que combina la presencia de agentes

públicos y privados para permitir que la información viaje de forma fraccionada a través de las redes disponibles, en atención al nivel de saturación, hasta una IP de destino donde será recopilada y traducida. Es un entramado poco jerarquizado y caracterizado, según la Asociación Derechos Digitales, por 2 cuestiones:

En primer lugar, por la descentralización, dígase, no hay un nodo central por lo que es estructuralmente resistente frente a los ataques que, consecuentemente, no podrán afectar a la totalidad de la red. Surge, en esta dimensión física de la red que se está abordando, el problema de las conocidas como infraestructuras críticas. Es un campo especialmente sensible ya que los focos de los que parte la mayor parte del abastecimiento mundial de internet se ubican únicamente en 4 estados: Estados Unidos, especialmente en Nueva York y Virginia, Alemania, con especial hincapié en Frankfurt, Holanda, en concreto en Ámsterdam y, finalmente, en Reino Unido, concretamente en su capital, Londres[6] (a pesar de que, según el último informe de la Unión Internacional de las Telecomunicaciones emitido en septiembre de 2017, un 48% de la población mundial tiene acceso a internet[7]). Estas infraestructuras están sometidas, según el GAO, a riesgos de triple naturaleza, los estrictamente físicos derivados tanto de acciones humanas como de desastres naturales, los estrictamente tecnológicos derivados de acciones cibernéticas maliciosas, y los mixtos.[8] Si se toma como referencia el marco ofrecido por la Unión Europea (en adelante UE/ Unión) se aprecia la importancia de estas infraestructuras tanto a nivel nacional como a nivel regional y supranacional ya que su protección se inserta dentro de la Estrategia Europea de Lucha Contra el Terrorismo y ha sido objeto de regulación por la vía de las directivas. En concreto, la Directiva 2008/114/CE del Consejo, de 8 de diciembre de 2008[9], sobre la identificación y designación de infraestructuras críticas europeas y la evaluación de la necesidad de mejorar su protección, define lo que se entiende por infraestructura crítica,

[6] PEÑA OCHOA, P.: *¿Cómo funciona Internet? Nodos críticos desde una perspectiva de los derechos. Guía para periodistas,* Editado por ONG Derechos digitales, Santiago de Chile, 2013, página 9. Disponible versión ebook en: https://www.derechosdigitales.org/wp-content/uploads/Como-funciona-internet-ebook.pdf

[7] ITU: *Gráfico sobre el porcentaje de uso de internet por regiones,* World Telecommunication Indicators Database, septiembre de 2017.

[8] GAO: *Internet infrastructure. Challenges in developing a public/private recovery plan,* United States Government Accountability Office (GAO-08-212T), Statement of G. C. Wilshusen, Octubre de 2007, página 2. Disponible en: https://www.gao.gov/new.items/d08212t.pdf

[9] Directiva 2008/114/CE del Consejo, de 8 de diciembre de 2008, sobre la identificación y designación de infraestructuras críticas europeas y la evaluación de la necesidad de mejorar su protección. Disponible en: https://www.boe.es/buscar/doc.php?id=DOUE-L-2008-82589

"el elemento, sistema o parte de este situado en los Estados miembros que es esencial para el mantenimiento de funciones sociales vitales, la salud, la integridad física, la seguridad, y el bienestar social y económico de la población y cuya perturbación o destrucción afectaría gravemente a un Estado miembro al no poder mantener esas funciones."

Y por infraestructura crítica europea o ICE, *"la infraestructura crítica situada en los Estados miembros cuya perturbación o destrucción afectaría gravemente al menos a dos Estados miembros."* Esta directiva se aplica específicamente a los sectores de la energía y del transporte, es decir, ya deja delimitado, a pesar de que son los Estados miembros quienes deben identificar las ICE con arreglo al procedimiento establecido, un ámbito de aplicación material positivo, dicho de otra forma, qué sectores son, por su propia naturaleza, críticos. Las tipologías más relevantes de ataques que sufren estas infraestructuras están vinculadas, atendiendo al Estudio sobre la Criminalidad realizado por el Gabinete de coordinación y estudios de la Secretaría de Estado de Seguridad dependiente del Ministerio del Interior de España en el año 2016, a los virus y troyanos, los accesos no autorizados, la denegación del servicio, los escaneos de red, el fraude, el spam y el robo de información.[10]

La segunda de las características identificadas por la Asociación Derechos Digitales es la neutralidad, es decir, sólo importa el volumen de los datos y no su procedencia, dígase, ante la presencia de dos paquetes de datos de igual dimensión, la actuación de la red es similar. Este es el componente esencial del ciberespacio, la información y la posibilidad de manejarla de forma remota, *quasi* impersonal y flexible.

Retomando a Lessig, el ciberespacio se articula como un espacio de libertad (o de anarquía) y se plantea el problema de su regulación o lo que algunos autores denominan "ética del ciberespacio" ya que, dentro de ese manejo de la información caracterizado por la flexibilidad, cabe un abanico de actividades que incluye desde conductas lícitas a comportamientos que, aún con ausencia de tipificación o incapacidades de investigación/persecución, tendrían un componente de ilicitud si se trasladasen al espacio físico. Unida esa cuestión al creciente número de usuarios y

[10] MINISTERIO DEL INTERIOR DE ESPAÑA: *Estudio sobre la cibercriminalidad en España*, Gabinete de coordinación y estudios de la Secretaría de Estado de Seguridad, 2016, página 25. Disponible en: http://www.interior.gob.es/documents/10180/5791067/Estudio+Cibercriminalidad+2016.pdf/456576b2-9ce8-4f3c-bbcc-ca0dbf3bb3cf

transacciones efectuadas a través de la red, determina lo que Geist ya anunciaba, *"puede que los Estados hayan querido quedarse al margen en la etapa incipiente de la Internet comercial, pero eso se acabó."*[11] Se trata, en definitiva, de seguir las líneas de Locke entendiendo que el conflicto entre libertinaje y libertad radica en que *"no se trata de una libertad sin límites sino del fin de la libertad porque se ha llevado a la libertad fuera de todo orden y se ha producido una negación de sí misma."*[12] En palabras del filósofo Fernando Savater se trata de cubrir una necesidad, la de protección de la libertad y del equilibrio del binomio conformado por la libertad y la seguridad entendida en términos materiales y jurídicos, partiendo del mismo enfoque global que tiene el objeto de regulación:

"*cualquier política de ciber vigilancia debería dotarse de normas claras (tanto legales como deontológicas) y tendría que estar acordada, al menos, entre los estados que comparten planteamientos democráticos semejantes."*[13]

Las principales necesidades regulatorias son, entonces, siguiendo la línea de Gil Navalón: definir los límites de la intervención estatal en el ciberespacio, proteger los derechos de propiedad e intimidad, identificar qué tipos delictivos son o pueden ser realizados a través del ciberespacio, crear tipos nuevos que respondan a conductas que únicamente puedan ser realizadas en red, y delimitar el método de aplicación de los conceptos procesales penales, especialmente en lo concerniente a los conflictos de jurisdicción.[14] Esta perspectiva adopta un enfoque sustentado en la protección del Estado de Derecho y de las garantías procesales; sin embargo, sus detractores adoptan un enfoque basado en la inviolabilidad de los derechos y libertades fundamentales concibiéndolos de modo absoluto tal y como muestra el texto de la conocida como Declaración de Independencia del Ciberespacio:

"Gobiernos del Mundo Industrial ... no son bienvenidos entre nosotros. No tienen ninguna supremacía donde nos juntamos...El Ciberespacio está fuera de sus fronteras. Estamos creando un mundo donde cualquiera, en cualquier sitio, puede expresar sus

[11] GEIST, M.: *Cyberlaw 2.0*, Boston College Law Review, núm. 44, 2003, pp. 323-358, página 330. Disponible en: https://lawdigitalcommons.bc.edu/cgi/viewcontent.cgi?article=2227&context=bclr
[12] LÓPEZ ZAMORA, P.: *El ciberespacio y su ordenación*, Ed. Tirant Lo Blanch, Difusión jurídica y temas de actualidad, Valencia, 2006, página 94.
[13] SAVATER, F.: *Deontología de la ciberseguridad*, Fundación para la Libertad, 28 de julio de 2013. Disponible en: http://paralalibertad.org/deontologia-de-la-ciberseguridad/
[14] GIL NAVALÓN, R.: *El vacío legal del ciberespacio*, Revista de Aeronáutica y Astronáutica, nº817, octubre de 2012, pp. 849-852.

creencias, sin importar lo singulares que sean, sin miedo a ser coaccionado al silencio o al inconformismo. Sus partidarios no consideran que ningún Estado ni Organización deba participar en la regulación, al considerar que el ciberespacio es un espacio de libertad."[15]

Niega la sujeción del ciberespacio a cualquier orden jurisdiccional y la posibilidad incluso de la conocida como autorregulación; se concibe la red como un ente anárquico en el sentido etimológico del término griego, dígase, sin gobierno, y autónomo. Así pues, tampoco acepta la categorización que de los derechos se hace tanto internacional como constitucionalmente, es decir, no promulga lo expresado por el Tribunal Constitucional español (en adelante TC) en la sentencia 2/82, de 29 de enero, *"no existen derechos ilimitados";* afirmación que viene refrendada por el artículo 29.2 de la Declaración Universal de los Derechos Humanos (en adelante DUDH) y por el artículo 18 del Convenio de Roma (en adelante CEDH).

Esta última tendencia concibe el ciberespacio como un lugar no físico, exento y al margen de las jurisdicciones ordinarias que han venido siendo tradicionalmente delimitadas en atención al principio de territorialidad, tanto en términos de derecho internacional ya que la territorialidad es la base misma del Estado, como en términos de enjuiciamiento penal ya que es el principio competencial principal. Si bien no puede negarse a esta segunda tendencia la concepción del ciberespacio como un ente carente de una territorialidad única, no es correcto entenderlo como extraterritorial en tanto en cuanto existen componentes físicos ubicados territorialmente y una capacidad de acción e influencia en puntos tangibles del mundo analógico; por ello, es preferible su categorización como multiterritorial, siguiendo la tesis defendida por Almonacid[16], no negando ni su naturaleza abierta, puesto que el ciberespacio es un espacio único de encuentro con independencia de la ubicación física del usuario, ni la necesidad de convertirlo en un lugar libre, que no libertario, donde los derechos se vean garantizados.[17]

[15] PERRY BARLOW, J.: *Declaración de independencia del ciberespacio.* Disponible (en español) en: https://nomadasyrebeldes.files.wordpress.com/2012/05/manifiesto_de_john_perry_barlow-1.pdf m

[16] ALMONACID LAMELAS, V. y SANCLIMENT CASADEJÚS, X.: *El impacto de las TIC en la configuracion clásica del Derecho. Especial referencia al principio de territorialidad,* CEF, nº4, mayo-agosto 2016, pp. 11-32, página 13. Disponible en: tecnologia-ciencia-educacion.com/judima/index.php/TCE/issue/download/15/10

[17] Discurso de Bert Koenders, ministro de Asuntos Exteriores del Gobierno de los Países Bajos, en la IV Conferencia Global sobre ciberespacio: *"el reto principal de las sociedades del siglo XXI es cómo hacer que internet sea libre, abierto y seguro."*

III. La ciberdelincuencia como fenómeno jurídico. Su tratamiento procesal

1. Problemas en la identificación del objeto del proceso.

La primera precisión que debe realizarse es de carácter terminológico y obedece a la necesidad de identificación del objeto del proceso una vez incoado un procedimiento penal. El objeto procesal no es otra cosa que el *tema decidendi*, dígase, los hechos sobre los que versará el procedimiento y su correspondiente calificación jurídica. La delimitación del objeto se realiza en lo que se denomina fase preliminar y supone corroborar la existencia del hecho, su relevancia jurídico-penal y la posibilidad de imputación del mismo a un sujeto; es decir, supone el desarrollo de actividades de investigación tendentes a delimitar la ocurrencia del hecho, y en su caso, las circunstancias en que tuvo lugar, la posibilidad de encuadre de dicha conducta en un tipo penal y la atribución de dichos actos a uno o varios sujetos de forma, en fase preliminar, presunta. Esos tres ejes que delimitan el objeto procesal como fundamento mismo del procedimiento penal son los que plantean dificultades en el marco de la ciberdelincuencia ya que es difícil rastrear la forma de ejecución de la conducta, no existe una tipificación completa del fenómeno y no siempre es posible encontrar al sujeto físico. De esos tres ejes, el que mayores problemas plantea en el plano del ciberdelito, es el del encaje de la conducta en un tipo penal ya que sólo teniendo una conducta típica descrita penalmente es posible desarrollar una actividad investigadora y de corroboración eficaz en términos jurídicos de los hechos que conformarán el objeto procesal. En este sentido, es necesario partir de una primera diferenciación entre las amenazas o empleos ilícitos que se hacen de la red y que pueden agruparse bajo la nomenclatura de ciberdelitos si se opta por la perspectiva de la ciudadanía, o de ciberataques si el potencial afectado es el Estado en su condición de soberano e inviolable.

En el primero de los sentidos es necesario hacer las siguientes precisiones a efectos de determinar cuál será el objeto del proceso:

El término ciberdelincuencia es el empleado en un instrumento jurídico de referencia en la materia como es el Convenio sobre la Ciberdelincuencia del Consejo de Europa, también conocido como Convenio de Budapest firmado en noviembre de 2001, si bien es cierto que dentro del citado convenio también hay un uso del concepto de delito

informático. De la propia articulación del Convenio puede desprenderse que ciberdelincuencia se refiere al fenómeno de la posibilidad de comisión de delitos o actos criminales a través de sistemas informáticos[18], es decir, siguiendo la literalidad del Convenio, se trata de actos criminales realizados a través de un *"dispositivo aislado o conjunto de dispositivos interconectados o relacionados entre sí, siempre que uno o varios de ellos permitan el tratamiento automatizado de datos en ejecución de un programa"*[19]; mientras que delito informático hace referencia a conductas específicas que suponen *"la introducción, alteración, borrado o supresión de datos informáticos"*[20], su falsificación o la *"interferencia en el funcionamiento de un sistema informático."*[21]

El concepto de delito informático tiene un contenido, entonces, restringido y tanto es así que, siguiendo a la profesora Corcoy, el bien jurídico protegido por esos tipos es únicamente de carácter patrimonial y/o socioeconómico.[22] Esta restricción del término delito informático a determinados tipos tiene su fundamento en lo vaticinado por Casabona:

"en puridad no puede hablarse de un delito informático, sino de una pluralidad de ellos, en los que encontramos como única nota común su vinculación de alguna manera con los computadores, pero ni el bien jurídico protegido agredido es siempre de la misma naturaleza ni la forma de comisión del -hecho delictivo o merecedor de serlo- presenta siempre características semejantes (...) Por eso es preferible hablar de delincuencia informática o delincuencia vinculada a las tecnologías de la información."[23]

Si se combina lo expuesto por Corcoy y Casabona y se pone en relación con lo señalado por Tiedemann, según el cual, ciberdelincuencia incluye las posibles amenazas a la esfera privada del ciudadano y, además, los daños patrimoniales producidos[24], la

[18] Definición de ciberdelincuencia del artículo 2.1 del Convenio Iberoamericano de Cooperación sobre Investigación, Aseguramiento y Obtención de Prueba en materia de Ciberdelincuencia del 2014. Disponible en: https://www.mec.gub.uy/innovaportal/file/52706/1/ciber_convenio.pdf
[19] Articulo 1 apartado a) del Convenio sobre la Ciberdelincuencia del Consejo de Europa (Convenio de Budapest) del 2001. Disponible en: https://www.oas.org/juridico/english/cyb_pry_convenio.pdf
[20] Artículo 7, *íbidem.*
[21] Artículo 8, *íbidem.*
[22] CORCOY BIDASOLO, M.: *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*, Eguzkilore, nº21, 2007, pp. 7-32, página 8. Disponible en: https://www.ehu.eus/documents/1736829/2176629/01+Corcoy.indd.pdf
[23] ROMEO CASABONA, C. M.: *Poder Informático y Seguridad Jurídica: la función tutelar del Derecho Penal ante las nuevas tecnologías de la información*, Ed. Fundesco, Madrid, 1988, página 47.
[24] TIEDEMANN, K.: *Poder informático y delito*, Ed. Ariel, Barcelona, 1985.

conclusión es que el concepto de delito informático no abarca la totalidad del fenómeno de la criminalidad en red, pero puede emplearse para referirse a una tipología de delitos cometidos a través de sistemas informáticos como son aquellos que atentan contra derechos patrimoniales. Debe tratarse de una conducta que recaiga sobre un sistema informático en sus componentes internos o *software*, dígase, que genere interferencias en los sistemas de gestión de la información[25]; dicho de otra forma, si la conducta recae sobre el elemento físico o *hardware* se podrá insertar en un tipo tradicional, en tanto en cuanto es un elemento patrimonial tangible y una conducta que no atenta contra el componente que otorga la especificidad a los delitos informáticos que es la capacidad de *"procesamiento y transmisión automatizados de datos y la confección y/o utilización de programas para tales fines*." [26]Este es, en esencia, el sentido que el Convenio de Budapest da al concepto de delito informático en sus artículos 7 y 8, dígase, lo que un sector de la doctrina entiende como criminalidad informática en sentido estricto y que es toda aquella amalgama de conductas ilícitas en las que el objeto material es un sistema informático en su dimensión interna[27], o, en otras palabras, la capacidad de gestión de la información.

No obstante, aún admitiendo esa premisa, existe otro debate doctrinal que versa sobre el bien jurídico protegido si esa es la consideración que se tiene del delito informático, más concretamente, el debate se centra en establecer si es un único bien jurídico protegido o son varios:

En la primera de las posiciones, lo único que caracterizaría al delito informático frente a los delitos patrimoniales tradicionales, sería la forma de comisión, es decir, se trataría de delitos de medios comisivos determinados, que, por tanto, exigirían necesariamente el empleo de dispositivos o sistemas informáticos.

La segunda de las perspectivas se plantea si hay una concurrencia de bienes jurídicos protegidos, es decir, junto al ineludible contenido patrimonial del delito, sitúa un bien jurídico supraindividual que es descrito como *"la confianza en el funcionamiento de los sistemas informatizados."*[28] El fundamento de esta perspectiva radica en que

[25] MIRÓ, F.: *El cibercrimen. Fenomenología y criminología de la delincuencia en el ciberespacio,* Ed. Marcial Pons, Madrid, 2012, página 308.
[26] ROMEO CASABONA, C. M.: *Poder informático y…, op. cit.,* página 43.
[27] MIRÓ, F.: *El cibercrimen…, op. cit.*
[28] CORCOY BIDASOLO, M.: *Problemática de la persecución…, op. cit.,* página 10.

entiende que la base de cualquier tipo de interacción, con independencia del espacio donde ésta tenga lugar, es la confianza.[29]

Acotar de esa forma el concepto de delito informático implica ampliar el sentido de cibercriminalidad. Ha tenido 3 acepciones: la más genérica de todas ellas es la que permitía emplear el término para referirse a todo tipo de conducta delictiva, tradicional o no, en la que interviniese de una u otra forma un componente informático o sistema de telecomunicaciones; por otro lado, se ha empleado como sinónimo de criminalidad informática en sentido amplio, es decir, ha aludido a todas aquellas conductas que encajaban en tipos tradicionales y cuya única diferenciación era la del empleo de dichos sistemas[30]; y finalmente, el término ciberdelincuencia se ha acotado y comprende todas aquellas conductas delictivas que recayendo sobre o empleando medios informáticos sean realizadas a través de Internet.[31]

Esa triple configuración permite plantear dos cuestiones:

La primera de ellas es la diferenciación, siguiendo la evolución del término, entre ciberdelincuencia y criminalidad informática. Si se toma como referencia el 10º Congreso de las Naciones Unidas sobre Prevención del Delito y Tratamiento del Delincuente, ciberdelincuencia se refiere a cualquier conducta de carácter ilícito que se comete a través de un sistema informático o red o herramienta similar, incluyendo la posesión ilícita y la distribución de información no autorizada por medio de dichos mecanismos[32]; sin embargo, en la Propuesta de Convenio Internacional para la Protección contra la Ciberdelincuencia y el Terrorismo se exige que para hablar de ciberdelincuencia se emplee un cibersistema.[33] Así pues, la perspectiva de Naciones Unidas encaja mejor en el espectro más amplio que abarca la criminalidad informática, mientras que el llamado

[29] GUTIÉRREZ, M. L.: *Fraude informático y estafa,* Ed. Centro de Publicaciones del Ministerio de Justicia, Madrid, 1991, página 266.
[30] MATA y MARTÍN, R.: *Delitos cometidos mediante sistemas informáticos (estafas, difusión de materiales pornográficos, ciberterrorismo,* Cuadernos Penales Jose María Lidón (Universidad de Deusto), nº4, 2007, pp. 129-171, página 131.
[31] CÁRDENAS, C.: *El lugar de comisión de los denominados ciberdelitos,* Política Criminal, nº6, 2008, pp. 1- 14, página 2. Disponible en: http://repositorio.uchile.cl/bitstream/handle/2250/126580/Ellugardecomisiondelosdenominadosciberdelitos.pdf?sequence=1&isAllowed=y
[32] ONU: *Crimes related to computer networks, Background paper for the workshop on crimes related to the computer network*,10th UN Congress on the Prevention of Crime and the Treatment of Offenders, 2000, A/CONF.187/10, página 5. Disponible en: https://www.unodc.org/documents/congress//Previous_Congresses/10th_Congress_2000/017_ACONF.187.10_Crimes_Related_to_Computer_Networks.pdf
[33] SOFAER, A. D. y GOODMAN, S. E.: *The transnational dimensión of Cyber Crime and Terrorism,* Ed. Hoover Institution Press, Standford, 2001, página 225.

Proyecto Standford se refiere a una restricción terminológica del concepto acotándolo al empleo de la red (Internet).

La segunda de ellas es la de si la ciberdelincuencia plantea la necesidad de protección de nuevos bienes jurídicos, o bien, nuevas formas de protección de bienes jurídicos tradicionales; en otras palabras, se trata de dilucidar si *"la confidencialidad, la integridad y la disponibilidad de los sistemas informáticos, redes y datos informáticos"*[34] es un conjunto de bienes jurídicos de naturaleza novedosa, o si, por el contrario, se trata de una nueva forma de atacar bienes jurídicos tradicionales como la intimidad, la privacidad, la indemnidad sexual, la libertad o el patrimonio.[35]

La consecuencia de esta ausencia de consenso sobre los términos y con ello, la imposibilidad de emplearlos como conceptos jurídicos determinados deriva en que la persecución penal de este tipo de conductas deba hacerse a través de una tipificación expresa y específica, dicho de otra forma, la distinción de las conductas en el derecho penal sustantivo se hace por tipología.[36]

Si se toma como referencia el ordenamiento jurídico español se aprecia que el procedimiento de tipificación de esta tipología delictiva es complejo. Siguiendo el eje cronológico, a pesar de haber firmado el citado Convenio de Budapest en noviembre de 2001, el instrumento no fue ratificado hasta octubre del 2010[37], 9 años después de su firma (aunque la ratificación más tardía fue la de Mónaco en marzo 2017, 3 Estados aun no lo han ratificado y Rusia no lo ha firmado)[38] coincidiendo con el desarrollo de la Ley Orgánica 5/2010 de 22 de junio que modificaba el marco penal español permitiendo una primera asunción de las obligaciones de tipificación contenidas en el instrumento internacional. La última reforma de su Código Penal (en adelante CP) operada a través de la Ley Orgánica 1/2015 de 30 marzo, que entró en vigor el 1 de julio del mismo año, es una respuesta a otra obligación internacional, en concreto, la comunitaria de implementar el contenido de la Directiva 2013/40/UE de 12 de agosto de 2013 relativa a los ataques

[34] Preámbulo Convenio de Budapest, *op. cit.*
[35] LORDOÑO, F.: *Los delitos informáticos en el proyecto de reforma en actual trámite parlamentario,* Revista Chilena de Derecho Informático, nº4, 2004, pp. 171-190, página 173. Disponible en: https://revistas.uchile.cl/index.php/RCHDI/article/view/10679
[36] GERCKE, M.: *Comprensión del ciberdelito: fenómeno, dificultades y respuesta jurídica,* UIT, 2014, página 20. Disponible en: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/Cybercrime2014_S.pdf
[37] Ratificación del Convenio de Budapest por España publicado el 17 de septiembre de 2010 en el BOE nº 226 de 2010. Disponible en: http://www.boe.es/boe/dias/2010/09/17/pdfs/BOE-A-2010-14221.pdf
[38] Chart of signatures and ratifications of Treaty 185 "Convention on Cybercrime", status as of 16/01/2019. Disponible en: https://www.coe.int/web/conventions/full-list/-/conventions/treaty/185/signatures

contra los sistemas de información y por la que se sustituye la Decisión marco 2005/222/JAI del Consejo, que viene a reforzar las obligaciones contenidas en el Convenio del Consejo de Europa (organización internacional de cooperación de la que son miembros todos los integrantes de la Unión Europea) y más específicamente, el primero de los objetivos del Convenio según Morón Lerma, dígase, la armonización del Derecho Penal sustantivo (artículos 2 a 13).[39] En este sentido, según Rovira, lo que tiene lugar es una suerte de conjunción entre las dos ideas que en el debate doctrinal se plantean entorno a la naturaleza de la criminalidad informática, dígase, se combina

"la conceptualización genérica del ciberdelito como delitos tradicionales ya implantados en el Código Penal y con la única diferenciación en su comisión, (...) y por otro lado, la superación de las nociones conceptuales tipificadas hasta el momento y la aparición de nuevos intereses de protección penal como la información y los datos en sí mismos."[40]

El Convenio identifica 4 tipos de delitos relacionados con los sistemas informáticos que en la legislación española han sido regulados siguiendo las líneas identificadas en la Estrategia de Seguridad Nacional de 2013 (en adelante ESN), dígase, partiendo de que la delincuencia informática se caracteriza por el fácil acceso[41], la capacidad de actuar como si no existiesen fronteras[42], el bajo coste y la minimización de los riesgos[43]:

- Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos (artículos 2 a 6 del Convenio): los artículos 197 y 197 bis del CP contemplan el acceso e interceptación ilícita contenido en el Convenio ya que incluyen, tanto el apoderamiento de datos sin autorización accediendo de forma ilegítima a un sistema informático, como la intercepción de transmisiones privadas de datos. En el caso español se combina la regulación de la confidencialidad del propio sistema con el derecho a la intimidad personal. El artículo 197 ter tipifica la modalidad que el Convenio califica como abuso de

[39] MORÓN LERMA, E. y RODRÍGUEZ PUERTA, M.: *Traducción y breve comentario del Convenio sobre Cibercriminalidad*, Revista de derecho y proceso penal, nº 7, 2002, pp.167-200, página 169.
[40] ROVIRA DEL CANTO, E.: *Nuevas formas de ciberdelincuencia intrusiva: el hacking y el grooming*, Iuris: actualidad y práctica del Derecho, nº 160, 2011, pp. 36-44, página 40.
[41] PRESIDENCIA DE GOBIERNO: *Estrategia de seguridad nacional. Un proyecto compartido. 2013*, Departamento de Seguridad Nacional, 2013, NIPO 002130347, página 42. Disponible en: http://www.lamoncloa.gob.es/documents/seguridad_1406connavegacionfinalaccesiblebpdf.pdf
[42] *Íbidem* página 18.
[43] *Íbidem* página 33.

dispositivo, dígase, el empleo de un sistema informático para la intrusión en otro sistema con vistas a cometer cualquiera de los delitos anteriores.

- Delitos informáticos (artículos 7 y 8 del Convenio): los artículos 264 y 264 bis del CP tipifican la conducta del fraude informático contenida en el Convenio, sancionando a quien interfiere en un sistema informático alterando los datos y generando con ello un perjuicio de tipo patrimonial ya que dichos artículos están incluidos en el capítulo IX, relativo a los daños, dentro del título XIII relativo a los delitos contra el patrimonio y el orden socio-económico.

- Delitos relacionados con el contenido a su vez subdivididos en dos secciones:

  - Delitos relacionados con la pornografía infantil (artículo 9 del Convenio): el artículo 183 ter CP ofrece la descripción de un delito de mera actividad que exige el empleo de tecnologías de la información para contactar con un menor de 16 años de cara a concertar un encuentro que derivaría en la comisión de un delito contra la indemnidad sexual o a obtener material pornográfico. El artículo 189 sanciona la conducta de difusión de material pornográfico de menores por cualquier medio (189.1 apartado b) y el acceso a dicho material a través de tecnologías de la información (189.5).

  - Delitos relacionados con infracciones de la propiedad intelectual y derechos afines (artículo 10): el artículo 270.2 CP sanciona las violaciones que a través de la prestación de servicios informáticos se hagan de los derechos de propiedad intelectual; no obstante, incluye un matiz no presente en el Convenio de Budapest como es el ánimo de lucro para considerarlo infracción de carácter penal.

- Delitos relativos a los actos de naturaleza racista y xenófoba cometidos por medio de sistemas informáticos: no están incluidos en el Convenio porque no fue posible alcanzar un acuerdo, pero sí se contemplan en el Protocolo adicional del Convenio sobre la Ciberdelincuencia firmado en enero de 2003 y ratificado por España en enero de 2015. El artículo 510 CP contempla la comisión de delitos de odio y enaltecimiento de la violencia por motivos discriminatorios, en concreto, los mismos motivos contenidos en el agravante genérico del artículo 22 apartado 4º, e incluye una agravación específica cuando, según el tenor literal

del artículo 510.4, *"los hechos se hubieran llevado a cabo a través de un medio de comunicación social, por medio de Internet o mediante el uso de tecnologías de la comunicación."* En este sentido, también es relevante la introducción de lo contenido en la Resolución 2178 del Consejo de Seguridad de Naciones Unidas a través de los artículos 575.2 y 578.2 que contemplan respectivamente el auto adoctrinamiento terrorista en red siempre que se acceda al contenido radical desde territorio español, y el enaltecimiento o justificación pública de actos tipificados como terroristas a través de los medios citados en el 510.4. Se introduce aquí un criterio de atribución de la jurisdicción española en base al principio de territorialidad.

Se trata de una regulación más extensa que la contenida en otros Estados miembros, como por ejemplo, Alemania, donde únicamente hay una protección penal del patrimonio respecto a los delitos informáticos[44], o Reino Unido, donde existe una extensa regulación del acceso ilícito en la *Compute Misuse Act* de 1990, con especial mención al desarrollo de programas para modificar o suprimir datos contenidos en otros equipos, y de los daños materiales que puedan causarse por dichos medios en la *Serious Crime Act* de 2015.[45]

Pasando a la segunda de las categorías, es decir, a la perspectiva de ataques en red sufridos por y entre Estados, es importante abordar el concepto no definido de ciberguerra y los posibles empleos del ciberespacio como método bélico no regulado ni previsto por las normas del Derecho Internacional Humanitario (en adelante DIH). A primera vista se plantean dos problemas: en primer lugar, lo ya apreciado por Goldsmith, es decir, la posibilidad de que *"un Estado podría emprender una operación cibernética que otro clasificara como acto de guerra, incluso cuando la primera nación no tuviera la intención de emprender semejante acción."*[46] En definitiva, la cuestión es delimitar cuando un ciberataque encaja en la definición de ataque incluida en el artículo 49 del Protocolo Adicional I de los Convenios de Ginebra de 1949; la solución parece pasar por entender

[44] MINISTERIO DE JUSTICIA y MINISTERIO DE INDUSTRIA, ENERGÍA Y TURISMO (España): *Análisis de derecho comparado sobre ciberdelincuencia, ciberterrorismo y amenazas al menor*, red.es, Madrid, octubre del 2015, página 27. Disponible en: http://cnec.university/wp-content/uploads/2016/07/AN%C3%81LISIS%20DE%20DERECHO%20COMPARADO%20SOBRE%20CIBERDELINCUENCIA%2C%20CIBERTERRORISMO%20Y....pdf

[45] *Ibidem*, página 48-51.

[46] GJELTEN, T.: *Extending de Law of War to ciberspace*, programa de radio del 22 de septiembre del 2010 en la NPR. Transcripción disponible en: http://www.npr.org/templates/story/story.php?storyId=130023318

que cualquier ciberataque que tenga lugar en un contexto de conflicto armado en el sentido expresado por los mismos convenios, ya sea nacional o internacional, será considerado un ataque y que cualquier ciberataque que determine la obtención de una ventaja militar estratégica siguiendo lo establecido en el artículo 52.2 del protocolo citado, también podrá ser categorizado como acción bélica. Esta última consideración plantea la segunda de las dificultades que el ciberespacio inserta en el marco del DIH y de la soberanía y es el de la aplicación del artículo 50 de la Carta de Naciones Unidas, es decir, la legítima defensa. La doctrina mayoritaria parece estar de acuerdo en que todo aquel ciberataque que tenga una consecuencia destructiva y de carácter físico entra en el ámbito de aplicación del citado artículo siempre y cuando se cumplan el resto de requisitos, véase, gravedad, inmediatez e intrusión; en consecuencia, un ciberataque que recaiga sobre ICE tendrá esta categorización o, en otras palabras, cuando el ciberataque coincida con la definición propuesta por Barat-Ginies, será presupuesto válido para la legítima defensa, es decir, cuando se trate de *"una operación cibernética ofensiva o defensiva de la que se espera que pueda causar pérdidas de vidas humanas, lesiones a las personas y daños o destrucciones de bienes."*[47] Sin embargo, en el marco de otro tipo de acciones como el ciberespionaje, la respuesta del DIH es más permisiva que sancionadora en tanto en cuanto no hay una prohibición expresa al efecto.

En cualquier caso, en este segundo supuesto actuarían las normas sobre resolución de conflictos del Derecho Internacional Público y los problemas derivados de una ausencia de regulación y categorización de las conductas realizadas a través de la red por y/o entre Estados con finalidades políticas, supondrían, no una incapacidad o dificultad para configurar el objeto procesal puesto que no existiría como tal, sino simplemente una falta de consenso a la hora de resolver la disputa internacional, la posibilidad de acudir, de darse las condiciones exigidas para ello a la Corte Internacional de Justicia para la interpretación de un hipotético tratado internacional sobre ciberataques, y, en el caso del DIH, sanciones por parte del Consejo de Seguridad.

[47] BARAT-GINIES, O.: *Informe jurídico del CCD CoE, El Manual de Tallin sobre la Aplicación del Derecho Internacional a la Ciberguerra. Informe final a 22 de noviembre de 2012*, traducción nº 13-063 realizada por el Gabinete de Traductores e intérpretes del Estado Mayor del Ejército de Tierra, Madrid, 2013, página 28.

2. Incidencia de la transnacionalidad de la ciberdelincuencia en las diligencias de investigación.

Las dificultades en la tipificación sustantiva del fenómeno de la criminalidad informática que proceden de las propias fórmulas de comisión de estos delitos plantean problemas en su perseguibilidad en términos procesales, es decir, aún siendo capaces de tipificar expresamente el fenómeno y dar cumplimiento al principio procesal *nullum crimen, nulla poena sine lege*, también denominado principio de legalidad, refrendado por el artículo 14 del Pacto Internacional de los Derechos Civiles y Políticos (en adelante PIDCP), el artículo 7 del CEDH y el artículo 9.3 de la Constitución española (en adelante CE), existen dificultades en su persecución penal derivadas de la naturaleza y medios comisivos de estos delitos, de ahí, que el establecimiento de medidas procesales y el esclarecimiento de las normas de Derecho Procesal Internacional sea el segundo eje temático que Morón Lerma identifica en el Convenio de Budapest (artículos 14 a 35).[48] En términos estrictamente procesales, las dificultades en la delimitación del objeto procesal y la ausencia de una certeza jurídica plena acerca del encaje de la conducta en red en un tipo penal, deja en la misma situación a la extensión y límites del ejercicio de la jurisdicción, a la atribución de competencia y a la elección del tipo de procedimiento.

Entre las dificultades que entraña la persecución y el enjuiciamiento de los delitos relacionados con las nuevas tecnologías, uno de los ejes centrales de los desafíos procesales son las consecuencias derivadas de la dimensión internacional del fenómeno, tanto en el plano físico- estructural, dígase, porque el camino empleado para el intercambio de datos se selecciona en atención al nivel de saturación de los disponibles y el óptimo puede implicar la salida del país de origen incluso aun cuando el destino de la información se encuentre dentro del mismo territorio nacional de salida; como en el plano del *iter criminis*, ya que el autor, la víctima y los medios comisivos pueden estar ubicados en distintas jurisdicciones. La concurrencia de varias jurisdicciones plantea inconvenientes tanto en el plano de la competencia para enjuiciar y del criterio a emplear (personalidad activa, personalidad pasiva, universalidad, territorialidad), como en el plano de la ley aplicable y del principio de doble incriminación; estas deficiencias pueden

[48] MORÓN LERMA, E. y RODRÍGUEZ PUERTA, M.: *Traducción y breve comentario…, op. cit.,* página 169.

ser empleadas por los propios autores[49] que recurren a cometer los delitos desde lo que se conoce como "refugios seguros" o estados con legislación escasa, débil o inexistente en materia de ciberdelincuencia[50] y que en términos procesales se traduce en la existencia de *fórum shopping* o *"ampliación del principio de oportunidad en el ejercicio de la acción penal."*[51] A título ejemplificante, en el año 2000 ocurrió el caso del bautizado por la prensa internacional como virus *I love you* que consistía en un gusano, dígase, un virus informático que se propagaba a través del correo electrónico cuando el usuario receptor del mensaje con asunto *I love you* abría el fichero adjunto. Los efectos principales eran el empleo de toda la agenda de direcciones de correo electrónico del usuario infectado para reproducir el virus, la posibilidad de modificar los ficheros de los ordenadores infectados y la capacidad de descargar un troyano que recogía toda la información personal y confidencial del usuario del dispositivo para enviarla a una cuenta de correo ubicada también en Filipinas[52], donde en ese momento, *"el desarrollo y la difusión intencionales del programa informático dañino no estaban debidamente penalizados* ."[53] Hasta el año 2009, Filipinas no comenzó a redactar legislación nacional en materia de ciberdelincuencia siguiendo el contenido del Convenio de Budapest y atendiendo a recomendaciones internacionales[54] que incidían en la importancia de realizar labores de convergencia legislativa en la materia a nivel mundial entendiendo que: en primer lugar, existe una normalización de los protocolos informáticos que hace análoga la situación de acceso a Internet en Occidente, Asia y África; en segundo lugar, hay una homogeneización en cuanto a los tipos de dispositivos y las características técnicas que se comercializan a lo largo y ancho del globo; y, en tercer lugar, la, antagónica, ausencia

[49] LEWIS, J.A.: *Computer spionage. Titan rain and China,* Technology and Public Policy Program, Center for Strategic and International Studies, diciembre 2005, página 1. Disponible en: http://cybercampaigns.net/wp-content/uploads/2013/05/Titan-Rain-Moonlight-Maze.pdf

[50] GERCKE, M.: *Comprensión del ciberdelito…, op. cit.,* página 92.

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

[52] DE ALZAGA, P. y PASTOR, E.: *El virus del amor colapsa ordenadores de todo el mundo,* Diario del Navegante, 5 de mayo del 2000. Disponible en: https://www.elmundo.es/navegante/2000/05/05/ailofiu_virus.html

[53] ONU: *Novedades recientes en el uso de la ciencia y la tecnología por los delincuentes y por las autoridades competentes en la lucha contra la delincuencia, incluido el delito cibernético,* Documento de trabajo preparado por la Secretaría, 12º Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal, 22 de enero de 2010, página 5. Disponible en: https://www.unodc.org/documents/crime-congress/12th-CrimeCongress/Documents/A_CONF.213_9/V1050385s.pdf

[54] GERCKE, M.: *El ciberdelito: guía para los países en desarrollo,* División de Aplicaciones TIC y Seguridad del Departamento de Políticas y Estrategias, Sector de Desarrollo de la Telecomunicaciones, UIT, Ginebra, abril del 2009, página 106. Disponible en: https://www.itu.int/dms_pub/itu-d/oth/01/0B/D010B0000073301PDFS.pdf

de un consenso internacional acerca de la tipificación penal de las conductas informáticas consideradas ilícitas que limita las capacidades de investigación y enjuiciamiento al ser un criterio de enjuiciabilidad la doble incriminación, dígase, la apreciación de la conducta como delito en las jurisdicciones implicadas y la identidad en su tipificación.[55] Esta dificultad se plantea en los casos donde es posible identificar algún tipo de conexión territorial; sin embargo, delimitar esta última cuestión es cada vez más complejo ya que delincuente, equipo y víctima pueden encontrarse en distintas jurisdicciones y/o ser múltiples. Una de las principales dificultades es la planteada por la posibilidad de automatización y diversificación de los recursos que agilizan todos los procesos de intercambio de datos magnificando la capacidad invasiva de los agentes maliciosos cibernéticos y permitiendo la creación de lo que se conoce como redes robot, dígase, un conjunto de sistemas informáticos que realizan ataques de la misma o distinta naturaleza contra los mismos objetivos pero que son irrastreables como conjunto operativo. La pertenencia de un dispositivo a una red robot no tiene porqué ser conocida por el usuario del mismo, sino que se parte de una serie de ataques iniciales que tienen como objetivo la creación de dicha red robot y que permite llevar a cabo ataques de grandes magnitudes como los sufridos por Estonia en 2007.[56]

El seguimiento del rastro e identificación de los autores es otras de las trabas jurídicas principales ya que la red está fuertemente respaldada por el anonimato personal en el sentido de que el elemento objeto de rastreo es la dirección IP pero no el usuario que está detrás y debido a la tecnología del encriptado que emplea algoritmos para convertir un texto en ilegible.[57] En palabras de Robles Carrillo, la investigación de la delincuencia en la red viene dificultada por la deslocalización subjetiva, funcional, espacial e instrumental.[58]

En resumidas cuentas, la actividad investigadora está vinculada al hallazgo de indicios de carácter físico y en el caso de la ciberdelincuencia estos son múltiples,

[55] NACIONES UNIDAS: *Novedades recientes en el uso…, op. cit.,* página 6.
[56] MCGUINNESS, D.: *Cómo uno de los primeros ciberataques rusos de la historia transformó a un país,* BBC, 6 de mayo de 2017. Disponible en: https://www.bbc.com/mundo/noticias-39800133
[57] LOWMAN, S.: *The effect on file and disc encryption on computer forensics,* Lowmanio, enero de 2010, página 1. Disponible en: https://www.lowmanio.co.uk/share/The%20Effect%20of%20File%20and%20Disk%20Encryption%20on%20Computer%20Forensics.pdf
[58] ROBLES CARRILLO, M.: *El ciberespacio: presupuestos para su ordenación jurídico-internacional,* Revista Chilena de Derecho y Ciencia Política, volumen 7, nº1, enero-abril del 2016, pp. 1-43, página 15 y ss.

deslocalizados e inexactos. Las diligencias de investigación tradicionales tendentes a la obtención de las fuentes de información como puede ser la entrada y registro a lugar cerrado, o el registro de libros y papeles, tienen limitaciones ya que suelen encontrarse ubicados físicamente en otras jurisdicciones y porque carecen del carácter de especialidad que tiene la delincuencia informática. Se han desarrollado diligencias específicas para el acceso y cotejo de la información contenida en dispositivos electrónicos, no obstante, su rastreo o su recuperación en caso de borrado está sujeta también a disponibilidad profesional y tecnológica y a las mismas limitaciones territoriales que las diligencias tradicionales incluso siendo posible el acceso remoto; dígase, que técnicamente sea posible la realización de diligencias a distancia que recaigan sobre los elementos físicos de la criminalidad en red, no supone la ausencia de necesidad de tramitación de las investigaciones transnacionales por los procedimiento judiciales de carácter ordinario que suponen añadir a las garantías que en términos de derechos del investigado se formulan como requisitos indispensables para la realización de diligencias especialmente invasivas, tales como los principios de proporcionalidad, idoneidad, necesidad y excepcionalidad, un requisito de especialidad o de vinculación de la diligencia a determinadas tipologías penales, y una serie de requisitos procedimentales vinculados a las peticiones entre jurisdicciones y no a las propias diligencias investigadoras. En definitiva, aún existiendo acuerdos de asistencia jurídica mutua, éstos no suelen contemplar el delito informático dentro de sus supuestos de acción. Si atendemos a las disposiciones del Convenio de Budapest, este dedica gran parte del preámbulo a recalcar la necesidad de integrar la delincuencia informática dentro de los acuerdos de cooperación judicial internacional en materia penal, y el título tercero de su tercer capítulo a regular los principios generales que deben regular la asistencia mutua; ahora bien, lo hace en términos orientativos ya que la normativa reguladora de esta asistencia es, según reza el artículo 25.4, la normativa interna y/o otros acuerdos internacionales, y su ejercicio está sujeto al cumplimiento del principio de doble incriminación entendido en términos de identidad sustantiva, dígase, exige que la conducta por la que se solicita la asistencia esté tipificada como delito en el Estado receptor de la solicitud, y no así la incardinación del tipo en la misma naturaleza delictiva.[59]

El contexto más propicio para este tipo de cooperación es el ofrecido por el Espacio de Libertad, Seguridad y Justicia Europeo sustentado, según el artículo 82.1 del

[59] Artículo 25.5 del Convenio de Budapest, *op. cit.*

Tratado de Funcionamiento, en los principios de reconocimiento mutuo y aproximación. Los avances más recientes en la materia son, por un lado, la creación dentro de Eurojust, tradicionalmente vinculado solamente a las infracciones que atentan contra *"los intereses financieros de la Unión"*[60], de la Red Judicial Europea de Ciberdelincuencia en el año 2016 para facilitar el intercambio de información entre Eurojust y Europol[61]; y, por otro lado, la Directiva 2014/41/CE del Parlamento Europeo y del Consejo de 3 de abril de 2014, relativa a la orden europea de investigación en materia penal que concibe la orden europea de investigación (en adelante OEI) como *"una resolución judicial emitida o validada por una autoridad judicial de un Estado miembro («el Estado de emisión») para llevar a cabo una o varias medidas de investigación en otro Estado miembro («el Estado de ejecución») con vistas a obtener pruebas."*[62] La emisión de la OEI procede, según el artículo cuarto de la misma Directiva, siempre que se refiera a una infracción conforme al derecho interno del solicitante que pueda originar o haya originado un procedimiento penal y siempre que se cumpla con los principios de adecuación y proporcionalidad.[63] En principio, el artículo 9, delimita un reconocimiento y ejecución automático de la OEI emitida de conformidad con los citados principios; no obstante, en materia de delincuencia informática, y atendiendo a la conjugación entre el anexo "D" de la Directiva y el artículo 11 que contempla las causas de denegación, hay una posibilidad de no reconocimiento de una OEI dictada en relación a delitos informáticos cuando la conducta no sea constitutiva de delito en el Estado de ejecución[64]; en otras palabras, cuando no se de cumplimiento al principio de doble incriminación en el sentido anteriormente expuesto como consecuencia de una mala aproximación de la normativa penal, no habrá asistencia judicial en este contexto.

En esencia, la ausencia de una actividad tipificadora consensuada y próxima en materia de ciberdelincuencia, complica las actividades investigadoras transnacionales, y con ello, el seguimiento de los procesos. Es paradójico que esta dificultad investigadora tenga lugar en una tipología delictiva novedosa cuando el límite impuesto a las acciones

[60] Cooperación judicial en materia penal: http://www.europarl.europa.eu/factsheets/es/sheet/155/la-cooperacion-judicial-en-materia-penal

[61] EUROJUST: *Informe Anual 2016,* página 31. Disponible en: http://eurojust.europa.eu/doclibrary/corporate/eurojust%20Annual%20Reports/Annual%20Report%202016/AR2016_ES.pdf

[62] Artículo 1 de la Directiva 2014/41/CE del Parlamento Europeo y del Consejo de 3 de abril de 2014. Disponible en: https://www.boe.es/doue/2014/130/L00001-00036.pdf

[63] Artículo 6 de la Directiva 2014/41/CE,…, *op. cit.*

[64] Artículo 11.1 apartado g) *Íbidem.*

de aproximación penal procesal en el ámbito europeo es el respeto a las tradiciones y sistemas jurídicos de los Estados miembros.

Todas estas dificultades resumidas por Davara de la siguiente forma derivan en la ausencia de un criterio único y unificado para establecer el anclaje de la red con alguna dimensión del mundo físico sea la estrictamente territorial como base de la jurisdicción penal, o la personal en atención a los principios de personalidad activa y pasiva:

"la intangibilidad de la información como valor fundamental de la nueva sociedad y bien jurídico a proteger; el desvanecimiento de teorías jurídicas tradicionales como la relación entre acción, tiempo y espacio; el anonimato que protege al delincuente informático; la dificultad de recolectar pruebas de los hechos delictivos de carácter universal del delito informático; las dificultades físicas, lógicas, y jurídicas del seguimiento, procesamiento y enjuiciamiento en estos hechos delictivos; la doble cara de la seguridad, como arma de prevención de la delincuencia informática y, a su vez, como posible barrera en la colaboración con la justicia. Todas ellas son cuestiones que caracterizan a este nuevo tipo de delitos y que requieren –entre otras- respuestas jurídicas. Firmes primeros pasos ya que se están dando a niveles nacionales, quedando pendiente una solución universal que, como todo producto farmacológico que se precie, se encuentra en su fase embrionaria de investigación y desarrollo."[65]

[65] DAVARA, M. A.: *Factbook del Comercio Electrónico*, Ed. Arazandi (2ª edición), Pamplona, 2002.

3. Conflictos internacionales de jurisdicción en materia de ciberdelincuencia. Posibilidades.

Los posibles conflictos de jurisdicción internacional que tienen lugar en materia de persecución de la criminalidad informática parten de la paradoja identificada por Mata, consistente en que el tratamiento de los datos informatizados es un factor criminológico de doble cara, dígase, hay una facilidad en su acceso, obtención y uso lesivo que se traduce en una dificultad para la determinación del autor y los medios de prueba[66] en tanto en cuanto es una red de comunicación global sujeta de forma simultánea a varias jurisdicciones limitadas por el factor territorial frente a la citada multiterritorialidad que caracteriza a la red y que a efectos de la persecución de la ciberdelincuencia se traduce en plurijurisdiccionalidad.[67]

Siguiendo a Morales, Internet ha sido capaz de desarrollar un sistema de comunicación y transmisión de datos de carácter universal[68] frente a la incapacidad político-gubernativa de optar, bien por el establecimiento de una homogeneización o legislación internacional a efectos, cuanto menos conceptuales en el sentido de unificar las tipologías previstas en el derecho penal sustantivo con vistas a dotar a la persecución penal de la criminalidad en red de seguridad jurídica y conocimiento de la acusación, pero también a efectos de establecer los criterios de determinación del foro competencial; o bien por la creación de una suerte de autoridad internacional encargada del enjuiciamiento de los delitos de dicha naturaleza, vía que, por otra parte, y atendiendo a la escasa credibilidad que actualmente tiene la Corte Penal Internacional como sede del Derecho Penal Internacional, parece ser la menos realista.

Los sistemas tradicionales de determinación de la jurisdicción competente a través del criterio del *forum delicti commissi* se encuentran, en el caso de la ciberdelincuencia, con la posibilidad de autorías conjuntas transnacionales, de duplicidades en los terminales, de sujetos pasivos no sólo grupales sino también transnacionales, y de

[66] MATA y MARTÍN, R. M.: *Delincuencia informática y derecho penal*, Ed. Edisofer, Madrid, 2001, página 17.
[67] MUÑOZ MACHADO, S: *La regulación de la red. Poder y Derecho en Internet*, Ed. Taurus, Madrid, 2000, página 221.
[68] MORALES GARCÍA, O.: *Criterios de atribución de responsabilidad penal a los prestadores de servicios e intermediarios de la sociedad de la información*, Cuadernos de Derecho Judicial, nº9 (dedicado a "Delincuencia informática: problemas de responsabilidad), 2002, pp. 179-240, página 237.

deslocalización, es decir, divergencias entre el lugar de situación del equipo, el lugar de control del equipo por el autor y el lugar de situación de los proveedores de servicios y servidores. Esa multiplicidad de anclajes físicos supone desde el punto de vista procesal obstáculos que desde el plano del enjuiciador se manifiestan en dificultades en la instrucción del proceso por la limitación territorial del alcance de la actividad investigadora frente a la transnacionalidad de la criminalidad en red[69]; desde el plano de los procesados en una posible merma de la garantía procesal formulada por el principio *non bis in ídem* en el caso de los conflictos de jurisdicción positivos; y desde el plano del orden público y las víctimas, en una ausencia de actividad punitiva y/o reparadora en el caso de los conflictos negativos de jurisdicción por la concurrencia de diversos criterios atributivos de competencia que la diversifican.

Tomando como referencia a la Fiscal de la Sala de Cooperación Internacional, Morán Martínez[70], los delitos relacionados con Internet cumplen con varias de las posibles razones que, de forma individual y no concurrente como en esta tipología delictiva, determinan la existencia de conflictos de jurisdicción:

- Comisión de la infracción penal en varios Estados.
- Empleo de medios tecnológicos.
- Uso de criterios de atribución jurisdiccional y competencial de carácter extraterritorial.

Otro factor que según Morán Martínez puede derivar en la existencia de conflictos positivos de jurisdicción es la consideración del criterio de la ubicuidad, según el cual, el delito se entiende cometido tanto en el lugar de producción del resultado como en el lugar de la ejecución siguiendo la doctrina expresada por el TJUE en el caso Wintersteiger.[71] Este criterio es visto como una parte de la doctrina como el ideal para solucionar la cuestión de los conflictos negativos de jurisdicción ya que supondría que siempre existiría

[69] LEZERTUA RODRÍGUEZ, M: *El proyecto de Convenio sobre cibercrimen de Consejo de Europa: proteger el ejercicio de derechos fundamentales en las redes informáticas*, Cuadernos europeos de Deusto, nº 25, 2001, pp. 83-118, página 92.
[70]MORÁN MARTÍNEZ, R. A.: *Conflictos de jurisdicción, n bis in ídem y transferencia de procedimientos*, Módulo VI, Tema 19, 5ª Edición, Red Europea de Formación Judicial, 2013, página 9. Disponible en: http://www5.poderjudicial.es/cvcp12-13/CVCP13-19-ES.pdf
[71] Sentencia del Tribunal de Justicia de la Unión Europea (Sala Primera) de 19 de abril de 2012 relativa al C-523/10. Disponible en: http://curia.europa.eu/juris/document/document.jsf;jsessionid=162F93D927771F84AA2A723D605DAD6A?text=&docid=121744&pageIndex=0&doclang=ES&mode=lst&dir=&occ=first&part=1&cid=9688423

algún tipo de conexión territorial que impidiese la inhibición competencial.[72] No obstante, es la posibilidad de la multiplicidad de conexiones la que lo inserta como un criterio que determina la existencia de conflictos positivos de jurisdicción una vez se ha avanzado en actividad instructora, de ahí que el principio de ubicuidad sea útil a efectos de determinar un primer foro competencial, dígase, un *fórum praeventionis c*ompetente para realizar la investigación pertinente pero que no tiene porque ser el foro definitivo.[73]

El criterio expresado el 3 de febrero del año 2005 por el Tribunal Supremo español reunido en pleno no jurisdiccional que conjuga ubicuidad con *prior in tempore, potior in iure*, podría, o al menos pretende, resolver los conflictos positivos de jurisdicción derivados de la aplicación primaria del criterio de la ubicuidad:

"el delito se comete en todas las jurisdicciones en 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 instruir la causa."[74]

Si se emplea como ejemplo el caso de las transferencias bancarias entre distintos puntos, dígase un tipo de estafa informática consistente en la transferencia no consentida de activos patrimoniales, puede observarse que el criterio de la ubicuidad se plasma en las distintas soluciones jurisprudenciales ya que entienden como competente tanto a la jurisdicción del lugar de posibilidad de disposición de los fondos estafados, como a la del lugar donde tiene lugar la causación del perjuicio, dígase, donde se ubica el banco perjudicado. Está dejando, sin embargo, al margen de estas dos opciones, en primer lugar, el supuesto en que el autor se encuentre en un tercer lugar y vinculando las posibilidades de persecución y enjuiciamiento de este delito informático a criterios tradicionales relacionados con el lugar del perjuicio causado y el lugar de disponibilidad que es donde se manifiesta el ánimo de lucro que caracteriza a los delitos económicos; y, en segundo lugar, el hecho de que dicha tipología delictiva puede tener dos modalidades, bien la

[72] HUNGRIA, N.: *Comentários ao Código Penal,* Volumen I, Tomo I, Ed. Forense, Río de Janeiro, 1976, página 162.
[73] Auto del Tribunal Supremo de España de 21 de enero de 1998 (cuestión 3550/1997). Disponible en: http://www.poderjudicial.es/search/contenidos.action?action=contentpdf&databasematch=TS&reference=893254&links=ubicuidad&optimize=20060309&publicinterface=true
[74] Acuerdo de 3 de febrero de 2005 del Tribunal Supremo español reunido en pleno no jurisdiccional. Disponible en: http://www.poderjudicial.es/cgpj/es/Poder-Judicial/Tribunal-Supremo/Jurisprudencia-/Acuerdos-de-Sala/Acuerdos-de-3-de-febrero-de-2005-sobre--1--Principio-de-ubicuidad---2--Clausulas-de-reserva-de-dominio-y-prohibicion-de-enajenar---3--Principio-de-minimos-psicoactivos-en-relacion-al-art--368-CP

conocida como *phishing*, que implica el uso de las direcciones de correos electrónicos para simular ser un banco y que el cliente, y posterior víctima, introduzca sus claves de acceso en un servidor falso, y la llamada *pharming,* que consiste en la manipulación y falsificación de la página web del banco para que cada cliente que acceda entregue sus datos a los autores del delito[75]. Obviar esa posibilidad de daños de carácter masivo y transnacional implicaría la existencia de múltiples procesos paralelos de idéntica naturaleza en el caso de recurrir tanto al criterio del banco perjudicado como al del lugar de disponibilidad de lo estafado ya que este puede ser también múltiple; parecería más acertado optar, bien por un criterio de unificación de los procedimientos por estafas informáticas masivas en una única jurisdicción, cuestión que parece poco probable tanto por la inexistencia de un tribunal internacional especializado en delitos informáticos, como por los requisitos que permitirían la acumulación de la causa ante un órgano jurisdiccional único, a saber, trascendencia económica relevante o complejidad en la instrucción[76]; o bien, por el establecimiento de obligaciones en materia de cooperación judicial, especialmente en lo concerniente a la realización de investigaciones conjuntas y al intercambio de información.[77]

En el caso del delito cibernético, el principio de ubicuidad parece resolver, también, la cuestión planteada por los llamados lugares de tránsito, dígase, todas aquellas jurisdicciones por las que la información transita sin dejar una consecuencia jurídica ilícita o reprochable. Esos lugares de tránsito son relevantes a efectos investigadores ya que será necesaria una búsqueda informática transfronteriza para rastrear el origen de la información dañina. Descartar los lugares de mero tránsito a través de nodos como jurisdicciones competentes encuentra su fundamento en una legislación vinculada a Internet como es la relativa a la protección de los datos de carácter personal; siguiendo el Reglamento UE 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016[78],

[75] Artículo 248.2 apartado a) del Código Penal español. Disponible en: https://www.boe.es/buscar/pdf/1995/BOE-A-1995-25444-consolidado.pdf

[76] ORTIZ PRADILLO, J.C.: *Determinación de la jurisdicción y competencia para la investigación y enjuiciamiento de los daños informáticos*, Ponencia de 23 de mayo de 2016 en el Centro de Estudios Jurídicos del Ministerio de Justicia, página 11. Disponible en: https://www.fiscal.es/fiscal/PA_WebApp_SGNTJ_NFIS/descarga/ponencia%20Ortiz%20Pradillo%20Juan%20Carlos.pdf?idFile=cd54640d-efbe-4839-bb98-27f9b0c17d67

[77] Decisión nº 854/2005/CE del Parlamento Europeo y del Consejo, de 2 de mayo de 2005, relativa al interés de fomentar un uso más seguro de Internet y las nuevas tecnologías en línea

[78] Reglamento 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de esos datos y por el que se deroga la Directiva 95/46/CE. Disponible en: https://www.boe.es/doue/2016/119/L00001-00088.pdf

se mantiene la idea expresada en el artículo 4.1 apartado c) de la Directiva 95/46/CE del Parlamento Europeo y del Consejo de 24 de octubre de 1995[79], según el cual cuando se empleen medios situados en un Estado miembro por un responsable de tratamiento de datos que no se encuentre en territorio comunitario y esto sea a meros efectos de tránsito por el territorio de la Unión, no será de aplicación la normativa comunitaria en la materia ni por tanto, competente su jurisdicción. El actual reglamento, a pesar de no mantener dicha disposición de forma literal, sigue contemplando dicha exclusión ya que dentro de la definición que realiza del tratamiento de datos en su artículo 4 apartado 2, no incluye el tránsito como supuesto de tratamiento.

Esa dicotomía entre el lugar de comisión y el lugar del resultado apareció muy bien reflejada en el conocido como caso Yahoo Inc[80], en el cual se planteaba una disputa jurisdiccional entre Francia y Estados Unidos atendiendo a las siguientes circunstancias: Yahoo tiene su sede social en California y ofrece servicios de búsqueda y alojamiento de información accesibles a través de diversos servidores. Ciudadanos estadounidenses, acogiéndose a la Primera Enmienda de su constitución, estaban publicando contenido calificado como nazi y accesible a través del servidor ubicado en Francia (yahoo.fr), lugar en el que dichas conductas son constitutivas de un delito de odio. Por un lado se plantea, entonces, a quién corresponde el enjuiciamiento de los hechos, jurisdicción estadounidense por ser la de la sede social y el servidor de publicación, o Francia por ser uno de los lugares de acceso a la información a través de su servidor nacional; y por otro lado, se plantea la cuestión de la responsabilidad de las plataformas de alojamiento de información en tanto que personas jurídicas, y de sus directivos, en relación a la información subida por los usuarios, debate que, por otra parte, es de actualidad en materia de propiedad intelectual.

A falta de un criterio de resolución de conflictos positivos de jurisdicción en este ámbito por la sensibilidad que este representa al ser una manifestación clásica de soberanía el ejercicio del *ius puniendi*, y teniendo en cuenta que el instrumento normativo de referencia, dígase, el Convenio del Consejo de Europa únicamente dedica un artículo,

[79] Directiva 95/46/CE del Parlamento Europeo y del Consejo de 24 de octubre de 1995 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. Disponible en: https://www.acave.travel/sites/default/files/comunitario-Directiva%2095-46-CE.pdf

[80] FLORES PRADA, I.: *Prevención y solución de conflictos internacionales de jurisdicción en materia de ciberdelincuencia*, Revista Electrónica de Ciencia Penal y Criminología, nº17, 2015, pp. 1-42, página 13 y ss. Disponible en: http://criminet.ugr.es/recpc/17/recpc17-21.pdf

concretamente, el número 22, al tratamiento de la cuestión de la jurisdicción, la doctrina ha desarrollado varios posibles sistemas, cada uno con sus limitaciones:

En lo concerniente a las previsiones del Consejo de Europa, el Convenio de Budapest se limita al empleo del criterio del lugar de la comisión, sin especificar si éste es el de la ejecución material del delito o el de la materialización del (o de los) resultados lesivos. Emplea el criterio base de la territorialidad entendiendo esta en los términos de territorio nacional según las normas de Derecho Internacional Público, aeronaves o buques con el pabellón del Estado en cuestión. Incorpora también el criterio de la personalidad activa estableciéndolo en segundo lugar en orden de prelación y siempre que se de cumplimiento al principio de doble incriminación. El único sistema que contempla para la resolución de conflictos positivos de jurisdicción es, según su artículo 22.5, la realización de consultas entre dichas jurisdicciones, en consonancia con los criterios ya expresados en otros acuerdos y resoluciones internacionales como el Convenio del Consejo de Europa sobre la prevención del terrorismo, firmado en Varsovia en 2005 (artículo 14[81]) o el Convenio de Naciones Unidas del año 2000 contra la delincuencia organizada transnacional (artículo 15)[82].

El primer bloque de propuestas doctrinales, por otra parte, tiene como base teórica el modelo de resolución de conflictos de jurisdicción para crímenes transnacionales elaborado por Zeis: un primer enfoque representado por Sinn, entiende que debe recurrirse al establecimiento de un orden de prelación de criterios de atribución competencial que prevea supuestos de un único Estado afectado y supuestos de pluralidad de afectados; por el contrario, el enfoque planteado por Hecker pretende combinar los clásicos criterios atributivos de competencia basados en las conexiones territoriales del criterio de ubicuidad, con circunstancias de corte material que se aplican en el contexto del Derecho Internacional Privado y que tienen relación con los intereses de la víctima o del acusado o la cuantía y comparativa entre daños.[83]

[81] Convenio del Consejo de Europa para la prevención del terrorismo, firmado en Varsovia en 2005. Disponible en: https://eurlex.europa.eu/legalcontent/ES/TXT/PDF/?uri=CELEX:22018A0622(01)&from=ES

[82] Convenio de Naciones Unidas del año 2000 Contra la Delincuencia Organizada Transnacional. Disponible en: https://www.unodc.org/documents/treaties/UNTOC/Publications/TOC%20Convention/TOCebook-s.pdf

[83] D'AVILA, F.R. y LEONHARDT DOS SANTOS, D.: *Derecho penal y ciberdelitos. Breves aproximaciones dogmáticas,* Revista Pensamiento Penal, nº1, 2016, pp. 1-14, página 6. Disponible en: http://www.pensamientopenal.com.ar/system/files/2016/12/doctrina44615.pdf

El segundo bloque propone la aplicación del principio de universalidad que supone una ampliación extraterritorial de la manifestación de soberanía que es el *ius puniendi* partiendo de una idea bien expresada por el Tribunal Constitucional de España en la STC 102/2002,

"el fundamento último de esta norma atributiva de competencia radica en la universalidad de la competencia jurisdiccional de los Estados y de sus órganos para el conocimiento de ciertos hechos sobre cuya persecución y enjuiciamiento tienen interés todos los Estados, de forma que su lógica consecuencia es la concurrencia de competencias, o, dicho de otro modo, de Estados competentes, respecto de las actuaciones indicadas."[84]

Recurrir a este principio como fundamento de la jurisdicción para el enjuiciamiento de los delitos informáticos, tal y como se expresó en el seno del duodécimo Congreso de las Naciones Unidas sobre justicia penal y prevención del delito[85], supondría vulnerar la propia configuración que de este principio de universalidad se hizo en los Principios de Princeton de 2001 entendiendo que se trata de

"una jurisdicción penal sustentada exclusivamente en la naturaleza del delito, con prescindencia del lugar en que éste se haya cometido, la nacionalidad del autor presunto o condenado, la nacionalidad de la víctima o todo otro nexo con el Estado que ejerza esa jurisdicción."[86]

Es decir, supondría el empleo de un principio sustentado en el bien jurídico objeto de protección, para el enjuiciamiento de una serie de tipos delictivos basados en el método y forma de comisión y que pueden atentar contra bienes jurídicos de diversa naturaleza. Esto implica que el principio de justicia universal no se repute adecuado como título atributivo de jurisdicción para conocer de delitos vinculados a la red; sin embargo, no debe descartarse en su totalidad ya que una de las condiciones que lo integran es el

[84] Sentencia del Tribunal Constitucional español nº 102/2000 de 10 de abril de 2000. Recurso de amparo 4.077/98, página 5. Disponible en: https://www.boe.es/diario_boe/txt.php?id=BOE-T-2000-9227

[85] ONU: *A Cyberspace Treaty - a United Nations Convention or Protocol on cybersecurity and Cybercrime*, Documento A/CONF.213/IE/7 preparado por Stein Schjolberg, 12º Congreso de la ONU sobre Justicia Penal y Prevención del Delito, celebrado en Salvador, Brasil, del 12 al 19 de abril de 2010. Disponible en: http://www.cybercrimelaw.net/documents/UN_12th_Crime_Congress.pdf

[86] ASAMBLEA GENERAL DE NACIONES UNIDAS: *Nota verbal de fecha 27 de noviembre de 2001 dirigida al Secretario General por las Misiones Permanentes del Canadá y de los Países Bajos ante las Naciones Unidas y anexo con los principios de Princeton sobre la jurisdicción universal*, Quincuagésimo sexto período de sesiones Tema 164 del programa, Establecimiento de la Corte Penal Internacional, 4 de diciembre de 2001, principio primero, página 14. Disponible en: https://digitallibrary.un.org/record/457330/files/A_56_677-ES.pdf?version=1

conocido como principio a*ut dedere aut judicare* que, tal y como se enuncia en los citados Principios de Princeton que clarifican el criterio de universalidad, supone que el Estado que tendría atribuida la competencia inicial siguiendo unos principios de prelación, procese al autor o, de lo contrario, lo entregue al siguiente Estado competente en atención al mismo orden y criterios expresados anteriormente. En línea con la cuestión de las garantías judiciales, la justicia universal tal y como está configurada internacionalmente plantea una excepción al principio *non bis in ídem* cuando hayan tenido lugar *"enjuiciamientos fictos o penas irrisorias dimanadas de una condena u otras actuaciones de imputación de la responsabilidad."*[87] Aplicada esta excepción a la criminalidad informática, supondría que la ausencia de un enjuiciamiento efectivo ya sea por ausencia de cumplimiento de los criterios de independencia e imparcialidad judicial, por empleo político de la criminalidad informática y del aparato judicial o por ausencia de una tipificación de los delitos vinculados a la red en el Estado competente en atención al primero de los criterios, permitiría el ejercicio de la jurisdicción por el siguiente competente. Conjugando esta posibilidad con el estricto significado procesal del principio *non bis in ídem,* que implica la prohibición de desarrollo de dos procesos penales de objeto semejante siempre que exista uno con una resolución a la que se le atribuya efecto de cosa juzgada, y no así la prohibición de litispendencia o multiplicidad de persecuciones penales con identidad de objeto y sujetos[88], sería posible el desarrollo de actividades cuanto menos instructoras paralelas a procedimientos ficticios o irrisorios en otras jurisdicciones.

El citado criterio *aut dedere aut judicare* es el que se emplea en un ámbito especialmente sensible como son los delitos contra la indemnidad sexual ya que el titular de dicho bien jurídico es un sujeto especialmente protegido por el Derecho como es el niño. El fundamento de dicha protección radica en la Convención para los Derechos del Niño. En el marco de la Unión, la preocupación sobre la protección del menor en la red ya se manifestó con la Decisión Marco 2004/68/JAI del Consejo, de 22 de diciembre de 2003[89], en la que se incluía una definición de sistema informático en su artículo primero

[87] ASAMBLEA GENERAL: *Nota verbal de fecha 27 de noviembre…, op. cit.,* principio noveno, página 16.
[88] Sentencia del Tribunal Constitucional español nº 159/1987 de 26 de octubre de 1987. Disponible en: http://hj.tribunalconstitucional.es/en/Resolucion/Show/891
[89] 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. Disponible en: https://www.boe.es/buscar/doc.php?id=DOUE-L-2004-80095

y tres criterios atributivos de jurisdicción en su artículo octavo que, en orden de prelación se presentaban de la siguiente forma: territorialidad por comisión total o parcial del delito dentro del territorio de un Estado miembro, personalidad activa con independencia del lugar de comisión y provecho de una persona jurídica establecida en territorio comunitario. En cuanto al primero de los criterios, la inclusión de la parcialidad de actividad ejecutiva delictiva en el territorio de un Estado miembro como criterio atributivo de competencia supone la necesidad de establecer un segundo criterio como puede ser el temporal en el caso de que exista un conflicto positivo de jurisdicción, o como puede ser la nacionalidad del autor o de la víctima en el caso de conflictos de carácter negativo; en cuanto al segundo, consolida el criterio referido anteriormente según el cual, en el caso de conflictos negativos en atención al primero de los criterios de la Decisión, la nacionalidad del autor actuaría e, igualmente, supone una obligación de extradición según el apartado tercero del artículo 8, en el caso de no existir opción o capacidad de enjuiciamiento. Estos criterios se mantienen en el artículo 17 de la Directiva (UE) nº 2011/92, del Parlamento Europeo y del Consejo, 13 diciembre 2011, relativa a la lucha contra los abusos sexuales y la explotación sexual de los menores y la pornografía infantil y por la que se sustituye la Decisión marco 2004/68/JAI del Consejo.[90] A pesar de ser el ámbito de la infancia una vertiente jurídica especialmente garantista, en materia de ciberdelincuencia vinculada a la corrupción del menor y su exhibición, no puede hablarse de criterios claros de atribución competencial, sino que es, quizás, el ámbito de los daños el que ofrece una mayor claridad en términos jurisdiccionales, especialmente a través de la derogada Decisión Marco 2005/222/JAI del Consejo de 24 de febrero de 2005 relativa a los ataques contra los sistemas de información y sustituida por Directiva 2013/40/UE del Parlamento Europeo y del Consejo, de 12 de agosto de 2013, relativa a los ataques contra los sistemas de información, puesto que aclara terminología incluida en la Decisión Marco 2004/68 recurriendo, de nuevo, al principio de ubicuidad que se manifiesta así como la solución más empleada, a pesar de la existencia de otros enfoques como los expuestos y de sus limitaciones.

Lo más relevante de esa normativa de daños es la precisión contenida en su artículo 10.4 que, incluía por primera vez en materia de ciberdelincuencia un orden expreso de prelación entre los criterios: ubicuidad, estimando lugar de comisión tanto el

[90] Decisión marco 2004/68/JAI, …, *op. cit.*

de la teoría de la actividad como el de la teoría del resultado[91]; personalidad pasiva y lugar de captura del autor.[92] La Directiva de 2013 permite la inclusión del criterio de la residencia habitual del autor en el territorio de un Estado miembro como habilitante para el ejercicio de su jurisdicción penal.[93] La especificidad del objeto de aplicación de esta Decisión, y de la posterior Directiva que la sustituye, circunscrito a las actividades delictivas que causan daños en los sistemas informáticos, dígase, a los delitos informáticos en el sentido del Convenio de Budapest, limita el alcance de dicho orden de prelación, pero no evita que pueda servir como modelo.

[91] Decisión Marco 2005/222/JAI del Consejo de 24 de febrero de 2005 relativa a los ataques contra los sistemas de información. Disponible en: https://www.boe.es/doue/2005/069/L00067-00071.pdf
[92] *Ibidem.*
[93] Directiva 2013/40/UE del Parlamento Europeo y del Consejo, de 12 de agosto de 2013 relativa a los ataques contra los sistemas de información y por la que se sustituye la Decisión Marco 2005/222/JAI del Consejo de 24 de febrero de 2005. Disponible en: https://www.boe.es/doue/2013/218/L00008-00014.pdf

IV. Conclusiones

La cuestión de la criminalidad informática plantea varios desafíos en lo referente a su configuración y entendimiento desde un punto de vista jurídico ya que supone la aparición de un espacio multiterritorial, global, incorpóreo y con una capacidad de evolución y desarrollo muy rápida que afecta a múltiples disciplinas del Derecho. Al margen de los posibles derechos materiales y sustantivos que puedan verse involucrados, esa dimensionalidad del ciberespacio crea conflictos de jurisdicción por varias razones:

1. La ausencia de una autoridad que reúna la característica principal de la red, dígase, su globalidad tanto en términos de extensión de sus facultades como de su composición. Partiendo de ello, algunos autores plantean la posibilidad de constitución de una suerte de Tribunal Penal Internacional con competencia en delincuencia informática, no obstante, y a la vista de lo expuesto a lo largo del trabajo, deben plantearse algunas conclusiones y problemáticas relativas a esta propuesta ya que si bien resolvería el problema de la jurisdicción competente, crearía otro tipo de dificultades que tienen que ver con los principios y bases del propio Derecho Internacional tanto en su vertiente tratadista como en su vertiente material y procesal. En términos de Derecho Originario, la asunción de la competencia de un tribunal internacional es siempre voluntaria para los Estados soberanos y no basta con la mera firma del tratado constitutivo, sino que debe también pasar por el proceso interno de ratificación. En ese mismo sentido, nada garantizaría, y de hecho es poco probable que ocurriese a la vista del ejemplo de la CPI, que la totalidad de los Estados aceptasen este hipotético tribunal especializado y se correría el riesgo, más acrecentado que actualmente, de la existencia de refugios seguros en tanto en cuanto la comisión del delito o su incidencia en Estados no adheridos al tribunal supondría la ausencia de un procedimiento único e incluso la inexistencia de un derecho sustantivo homogéneo. Además, la materia propiamente penal es especialmente sensible a efectos de soberanía y más aún cuando, en el caso de la ciberdelincuencia, no existe una protección de los denominados bienes jurídicos de la Humanidad sino una afectación de bienes jurídicos de carácter individual y sin dicha trascendencia universal.

Igualmente, y siguiendo la línea del *ius puniendi* como manifestación de soberanía, la constitución del tribunal pasaría por una homogeneización sustantiva del fenómeno de la criminalidad en red que no ha sido posible de forma completa ni siquiera en el espacio de integración por antonomasia que es la UE y su espacio de Libertad, Seguridad y Justicia.

2. La ausencia de limitaciones territoriales en el traspaso de la información frente a las delimitaciones fronterizas que enfrenta el ejercicio de la jurisdicción, unida a la capacidad de evolución del fenómeno frente a la lentitud que caracteriza el avance del Derecho. En otras palabras, la multiterritorialidad de la red y la homogeneización de su sistema de funcionamiento a lo largo del globo choca de frente con un mundo dividido en espacios jurisdiccionales sujetos a limitaciones fronterizas y procedimentales. La criminalidad en la red ha demostrado una rápida capacidad de avance, mutación y alcance frente a la ausencia de una capacidad tipificadora, ya no internacional, sino estatal que lleve el mismo ritmo o alcance y que consiga abarcar el fenómeno en buena parte o en su totalidad. En este aspecto, las posibles soluciones que pueden proponerse a la luz de lo expuesto pasarían por una flexibilización de la actividad jurídica, bien en el sentido de optar por procesos legislativos más ágiles, bien en el sentido de una figura de juez más próxima a la del derecho anglosajón. En la primera de las alternativas se pierden los matices técnicos que parece necesitar la tipificación de la ciberdelincuencia, y en la segunda, se compromete la seguridad jurídica; sin embargo, cabe plantearse en este punto que un fenómeno multidisciplinar y con amplia capacidad de mutación, a pesar de su aspecto tecnológico y sus múltiples variantes, puede no requerir necesariamente una tipificación sistemática, sino una de corte general con agravantes y atenuantes que otorguen al tipo las especificidades propias del fenómeno; en esencia, supone plantearse que la regulación de tipos tradicionales como el hurto o el homicidio contempla una actividad genérica que deriva en un resultado lesivo y no las diversas e inabarcables formas en que puede cometerse el citado delito. De la misma forma, dichos tipos tienen agravantes y atenuantes propios vinculados a su propia naturaleza, y tipos agravados por razón de los medios y/o formas empleados o de las características de la víctima. ¿Es este modelo extrapolable a los delitos

informáticos? Sí, siempre y cuando la tipificación de estos tipos se realice teniendo en cuenta el bien jurídico afectado y el medio empleado. En cuanto al bien jurídico, la aproximación realizada al fenómeno permite concluir que a pesar de poder teorizar acerca de la existencia de un bien jurídico propio y específico de la ciberdelincuencia y vinculado a la actividad en red, la realidad es que, en busca de la efectividad en su persecución, debe optarse por la protección de los bienes jurídicos tradicionales, especialmente intimidad, integridad moral, patrimonio, libertad e indemnidad sexual y libertad tanto en su aspecto de capacidad de decisión como en su aspecto de capacidad de movilidad, y prever un tipo de afectación de estos bienes jurídicos a través del empleo de la metodología ofrecida por la red y el ciberespacio.

3. La capacidad de crear nuevas formas de delincuencia no previstas por el Derecho tradicional vinculado a la prueba de carácter físico: hay un difícil encaje de la criminalidad informática en los sistemas penales nacionales en tanto en cuanto es un área especialmente técnica que requiere de una comprensión de su funcionamiento tecnológico previa a su tipificación, y en tanto en cuanto, escapa a los sistemas procesales penales tradicionales basados en pruebas físicas y tangibles. A pesar de la existencia de anclajes de la red al mundo físico, el empleo delictivo de los mismos supone, en la mayor parte de los casos, una suerte de juego y engaños a través de dichos enlaces analógicos que derivan en incapacidad para delimitar de forma concreta y/o única dichas conexiones físicas; además, la propia esencia de Internet radica en la transmisión continua de información que, a efectos del mundo físico, es inexistente. Así pues, en busca de una efectividad en la persecución del fenómeno, es necesario ponderar entre, por un lado, el derecho a la sanción y el derecho a la reparación de la víctima, y por otro, el derecho a la presunción de inocencia, sin que ello signifique desnaturalizar nuestro sistema penal y/o minusvalorar cualquiera de los citados derechos. La posibilidad de rastrear los delitos vinculados a la ciberdelincuencia ha creado una diferenciación respecto a otras categorías delictivas, dígase, retomando el ejemplo de tipos tradicionales como el homicidio o el hurto, la reconstrucción de los hechos no es exacta con carácter general, sino que determinadas pruebas y algunos indicios ayudan a construir una radiografía de lo que pudo ser el *iter criminis*;

sin embargo, parece que a los delitos vinculados a la tecnología se les exige un mayor refuerzo en la verificación de los pasos y hechos delictivos. No hay que obviar que el empleo de medios tecnológicos permite ese rastreo, pero al mismo tiempo, es un trabajo largo, arduo y complejo que vinculado al sistema penal sólo ralentiza y minimiza su eficacia.

Si se trasladan estas conclusiones a la característica de la transnacionalidad, puede desprenderse lo siguiente:

4. Esas características de diversificación y volatilidad de la red determinan que se considere la necesidad de flexibilizar los criterios procesales que permiten la determinación de la jurisdicción competente, entendiendo que no es posible establecer una regla de carácter rígido capaz de abordar de forma eficaz el espectro de posibilidades de la criminalidad informática. Así, la delimitación de la jurisdicción idónea pasaría, en ausencia de normativa en la materia, por criterios de carácter tangible que serían aplicados en atención a las circunstancias del caso, tales como: el lugar de situación del autor en el momento de comisión de los hechos, el lugar donde tiene lugar el resultado lesivo de mayor gravedad, el lugar de detención del autor o el lugar de residencia de la víctima. El empleo de dichos criterios genera varios inconvenientes ya previstos por el grupo intergubernamental de expertos de la Oficina de Naciones Unidas contra la Droga y el Delito reunidos en Viena del 17 al 21 de enero de 2011(armonización, Derecho Penal sustantivo, investigación, cooperación, prueba electrónica y responsabilidad):
    a. Ausencia de seguridad jurídica y cumplimiento de las garantías procesales por cuanto que, siguiendo lo expresado por el TJUE en el ya citado caso Wintersteiger, los criterios que delimitan la jurisdicción y la prioridad en el ejercicio de la misma para los supuestos que implican transnacionalidad, deben ser claros y precisos.
    b. Necesidad de cooperación investigadora y judicial transnacional: la cooperación judicial y policial internacional es un terreno que ha visto progresos en las últimas décadas, no obstante, en términos de delimitación de la jurisdicción competente en materia de ciberdelincuencia, no se afronta tanto el problema de la existencia de una cooperación o traspaso real de información, como el de la eficacia

que, en términos procesales y no materiales, tienen estos sistemas de cooperación. El problema que tiene lugar en este área es que la cooperación suele aparecer cuando hay dos procedimientos paralelos, dígase, suele generar situaciones de litispendencia que encajan en la doctrina del núcleo esencial común en tanto en cuanto hay una identidad sustancial entre lo juzgado en ambos procedimientos y un riesgo de conculcación del principio *non bis in ídem*, además de la posibilidad de dictar resoluciones contradictorias por ausencia de homogeneidad en la tipificación sustantiva del fenómeno y de una propuesta de *lege ferenda* en la materia.

c. Necesidad de delimitación un orden de prelación o de preferencia o criterios alternativos para la resolución de conflictos positivos de jurisdicción y de implementación de algún tipo de obligación internacional para los conflictos negativos de jurisdicción: al margen de la solución que pasaría por el establecimiento de un orden de prelación delimitado en atención a la conjugación entre los clásicos criterios atributivos de jurisdicción y ligados a la territorialidad, con criterios sustraídos del ámbito del Derecho Privado y que aluden a los daños y a la situación de la víctima; un sistema alternativo sería el empleo de la mediación o el arbitraje, siguiendo la línea expresada en la normativa ya referenciada que, prevé conversaciones entre las jurisdicciones competentes con vistas a solucionar el conflicto positivo. Supondría, en definitiva, ir un paso más allá del consenso y someter la resolución del conflicto a un tercero con autoridad y capaz de dictaminar una resolución vinculante para las partes en el conflicto de jurisdicción obligando siempre a uno de ellos a conocer de la cuestión y determinando las obligaciones cooperativas del resto. La composición idónea de dicho tercero sería la de un órgano colegiado compuesto por dos autoridades judiciales década uno los Estados implicados (puesto que son quienes mejor aproximación a sus derechos internos pueden aportar) y autoridades judiciales de terceros Estados hasta superar en un miembro a las de los Estados implicados; teniendo en cuenta que dichos terceros deben ser representativos de los

sistemas penales involucrados y otorgar una visión lo más profunda posible y cercana a la de las partes en conflicto.

En esencia, el mayor desafío que la ciberdelincuencia impone a nuestros sistemas de Derecho, y especialmente al Derecho continental, es el de su rigidez; característica que se reputa manifiestamente más intensa en áreas como la penal y la procesal. Partiendo de esta idea, y en términos de enjuiciamiento penal, la ciberdelincuencia muestra dos facetas:

5. En primer lugar, y en algunas de sus manifestaciones, no es más que una vía distinta de atentar contra bienes jurídicos ya protegidos, dígase, se trata más bien de una nueva forma de medios comisivos que de una nueva forma de delincuencia en sí misma. Así pues, lo esencial a efectos de su persecución y enjuiciamiento penal no es tanto su configuración en el Derecho sustantivo, que podría pasar por contemplar, para tipos delictivos que no exijan un contacto físico efectivo, la posibilidad de su comisión a través de medios electrónicos, sino la capacidad probatoria. Si se utiliza como ejemplo la clásica prueba documental, no tiene sentido equiparar a los sistemas informáticos y a la información que contienen con un documento notarial por cuanto que lo que define la autenticidad de un fichero informatizado es la rastreabilidad de su autor. Si uno se posiciona en el más sencillo de los escenarios, dígase, una única víctima y un autor rastreable, ese rastro puede atravesar varias y diversas jurisdicciones nacionales; suponiendo que el criterio atributivo de competencia fuese, bien el lugar de producción de los daños, bien el de la nacionalidad de la víctima, la posibilidad de llegar a determinar el *iter criminis* o la identidad concreta de la persona física situada enfrente del sistema informático, se antoja, cuanto menos, improbable, impidiendo con ello la formación del objeto procesal. Desde un punto de vista teórico, la cooperación judicial internacional es la mejor de las soluciones ya que incoado un procedimiento y percibiéndose en su fase investigadora un componente informático y transnacional, debería ser plausible la emisión de una petición de cooperación judicial que derivase en la apertura de diligencias investigadoras en los Estados involucrados. Desde un punto de vista, ya no sólo político, sino también material, el incremento de la criminalidad en red paralizaría los sistemas judiciales y de cooperación. Lo ideal sería una categorización delictiva partiendo de acuerdos ya existentes: por ejemplo, en

el plano de delitos de naturaleza económica, el criterio cuantitativo discriminaría qué procedimientos pueden movilizar dichos recursos de cooperación; en el área de los delitos de naturaleza sexual, la vulnerabilidad internacionalmente reconocida a colectivos como las mujeres y la infancia permitiría la cooperación en dichas circunstancias.

6. En segundo lugar, genera conductas nuevas que hacen necesaria la inclusión de títulos específicos dentro de los códigos penales nacionales que contemplen la protección del bien jurídico denominado seguridad informática por cuanto que, y acudiendo, de nuevo, al plano internacional, el empleo de medios informáticos es una forma de desarrollar el contenido del artículo 19 de la DUDH en un mundo globalizado. Esta propuesta de categorizar un espectro de la delincuencia informática como una tipología delictiva propia y autónoma, encuentra su fundamento en la necesidad de adaptación de los derechos a la información y a la libertad de expresión, a las sociedades digitalizadas. Esta perspectiva se aleja de aquellos delitos que derivan en daños patrimoniales y/o físicos para proteger otro tipo de intereses como la integridad de los datos, la inviolabilidad de las identidades o los delitos de peligro en red que seguirían la configuración clásica de un delito de peligros, es decir, sanción de la peligrosidad *ex ante*. Esta configuración soluciona también problemas de enjuiciamiento y perseguibilidad puesto que está sancionando aquellas conductas que producen una sensación de desconfianza o inseguridad en el usuario hacia el uso de Internet, y descartando la necesidad de que se produzca un daño efectivo a los bienes jurídicos tradicionales. Situar en este momento la barrera penal supone no tener que abordar el tema de la pluralidad de víctimas o diversificación de los daños ya que el potencial afectado será el servidor en concreto o dominio que ve su cuota de usuarios mermada.

Bibliografía

1. Libros:

- ASENCIO MELLADO, J.M.: *Derecho procesal penal,* Ed. Tirant lo Blanch, Madrid , 2015.

- BARAT-GINIES, O.: *Informe jurídico del CCD CoE, El Manual de Tallin sobre la Aplicación del Derecho Internacional a la Ciberguerra. Informe final a 22 de noviembre de 2012,* traducción nº 13-063 realizada por el Gabinete de Traductores e intérpretes del Estado Mayor del Ejército de Tierra, Madrid, 2013.

- DAVARA, M. A.: *Factbook del Comercio Electrónico*, Ed. Arazandi (2ª edición), Pamplona, 2002.

- FEYERABEND, P.K.: *Contra el método*, Ed. Ariel, Barcelona, 1974.

- GIMENO SENDRA, V.: *Derecho Procesal Penal,* Ed. Civitas, Madrid, 2015.

- GUTIÉRREZ, M. L.: *Fraude informático y estafa,* Ed. Centro de Publicaciones del Ministerio de Justicia, Madrid, 1991.

- HUNGRIA, N.: *Comentários ao Código Penal,* Volumen I, Tomo I, Ed. Forense, Río de Janeiro, 1976.

- LESSIG, L.: *El código 2.0,* Ed. Traficantes de sueños, Madrid, 2009.

- LÓPEZ ZAMORA, P.: *El ciberespacio y su ordenación*, Ed. Tirant Lo Blanch, Difusión jurídica y temas de actualidad, Valencia, 2006.

- MATA y MARTÍN, R. M.: *Delincuencia informática y derecho penal*, Ed. Edisofer, Madrid, 2001.

- MIRÓ, F.: *El cibercrimen. Fenomenología y criminología de la delincuencia en el ciberespacio*, Ed. Marcial Pons, Madrid, 2012.

- MUÑOZ MACHADO, S: *La regulación de la red. Poder y Derecho en Internet*, Ed. Taurus, Madrid, 2000.

- NEGROPONTE, N.: *Being digital,* Ed. Vintage books, Nueva York, 1996.

- ORMAZÁBAL SÁNCHEZ, G.: *Proceso penal con implicaciones extranjeras y principio de legalidad en el ámbito de la Unión Europea*, en VV.AA., *La Justicia y la Carta de Derechos Fundamentales de la Unión Europea*, Ed. Colex, Madrid, 2008.

- ROMEO CASABONA, C. M.: *Poder Informático y Seguridad Jurídica: la función tutelar del Derecho Penal ante las nuevas tecnologías de la información*, Ed. Fundesco, Madrid, 1988.

- SOFAER, A. D. y GOODMAN, S. E.: *The transnational dimensión of Cyber Crime and Terrorism*, Ed. Hoover Institution Press, Standford, 2001.

- TERCEIRO, J.B.: *Sociedad digital: del homo sapiens al homo digitalis,* Ed. Alianza Editorial, Madrid, 1996.

- TIEDEMANN, K.: *Poder informático y delito*, Ed. Ariel, Barcelona, 1985.

2. Estudios y guías electrónicas:

- GAO: *Internet infrastructure. Challenges in developing a public/private recovery plan*, United States Government Accountability Office (GAO-08-212T), Statement of G. C. Wilshusen, Octubre de 2007. Disponible en: https://www.gao.gov/new.items/d08212t.pdf

- GERCKE, M.: *Comprensión del ciberdelito: fenómeno, dificultades y respuesta jurídica*, UIT, 2014. Disponible en: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/Cybercrime2014_S.pdf

- GERCKE, M.: *El ciberdelito: guía para los países en desarrollo*, División de Aplicaciones TIC y Seguridad del Departamento de Políticas y Estrategias, Sector de Desarrollo de la Telecomunicaciones, UIT, Ginebra, abril del 2009. Disponible en: https://www.itu.int/dms_pub/itu-d/oth/01/0B/D010B0000073301PDFS.pdf

- MINISTERIO DE JUSTICIA y MINISTERIO DE INDUSTRIA, ENERGÍA Y TURISMO (España): *Análisis de derecho comparado sobre ciberdelincuencia, ciberterrorismo y amenazas al menor*, red.es, Madrid, octubre del 2015. Disponible en: http://cnec.university/wp-content/uploads/2016/07/AN%C3%81LISIS%20DE%20DERECHO%20COMP

ARADO%20SOBRE%20CIBERDELINCUENCIA%2C%20CIBERTERRORISMO%20Y....pdf

- MINISTERIO DEL INTERIOR DE ESPAÑA: *Estudio sobre la cibercriminalidad en España,* Gabinete de coordinación y estudios de la Secretaría de Estado de Seguridad, 2016. Disponible en: http://www.interior.gob.es/documents/10180/5791067/Estudio+Cibercriminalidad+2016.pdf/456576b2-9ce8-4f3c-bbcc-ca0dbf3bb3cf

- MORÁN MARTÍNEZ, R. A.: *Conflictos de jurisdicción, n bis in ídem y transferencia de procedimientos,* Módulo VI, Tema 19, 5ª Edición, Red Europea de Formación Judicial, 2013. Disponible en: http://www5.poderjudicial.es/cvcp12-13/CVCP13-19-ES.pdf

- PEÑA OCHOA, P.: *¿Cómo funciona Internet? Nodos críticos desde una perspectiva de los derechos. Guía para periodistas,* Editado por ONG Derechos digitales, Santiago de Chile, 2013. Disponible versión ebook en: https://www.derechosdigitales.org/wp-content/uploads/Como-funciona-internet-ebook.pdf

- PRESIDENCIA DE GOBIERNO: *Estrategia de seguridad nacional. Un proyecto compartido. 2013,* Departamento de Seguridad Nacional, 2013, NIPO 002130347. Disponible en: http://www.lamoncloa.gob.es/documents/seguridad_1406connavegacionfinalaccesiblebpdf.pdf

3. Artículos académicos:

- ALMONACID LAMELAS, V. y SANCLIMENT CASADEJÚS, X.: *El impacto de las TIC en la configuracion clásica del Derecho. Especial referencia al principio de territorialidad,* CEF, nº4, mayo-agosto 2016, pp. 11-32. Disponible en: tecnologiacienciaeducacion.com/judima/index.php/TCE/issue/download/15/10

- CÁRDENAS, C.: *El lugar de comisión de los denominados ciberdelitos,* Política Criminal, nº6, 2008, pp. 1- 14. Disponible en: http://repositorio.uchile.cl/bitstream/handle/2250/126580/Ellugardecomisiondelosdenominadosciberdelitos.pdf?sequence=1&isAllowed=y

- CORCOY BIDASOLO, M.: *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,* Eguzkilore, nº21, 2007, pp. 7-32. Disponible en: https://www.ehu.eus/documents/1736829/2176629/01+Corcoy.indd.pdf

- D'AVILA, F.R. y LEONHARDT DOS SANTOS, D.: *Derecho penal y ciberdelitos. Breves aproximaciones dogmáticas,* Revista Pensamiento Penal, nº1, 2016, pp. 1-14. Disponible en: http://www.pensamientopenal.com.ar/system/files/2016/12/doctrina44615.pdf

- FLORES PRADA, I.: *Prevención y solución de conflictos internacionales de jurisdicción en materia de ciberdelincuencia,* Revista Electrónica de Ciencia Penal y Criminología, nº17, 2015, pp. 1-42. Disponible en: http://criminet.ugr.es/recpc/17/recpc17-21.pdf

- GEIST, M.: *Cyberlaw 2.0,* Boston College Law Review, núm. 44, 2003, pp. 323-358. Disponible en: https://lawdigitalcommons.bc.edu/cgi/viewcontent.cgi?article=2227&context=bclr

- GIL NAVALÓN, R.: *El vacío legal del ciberespacio,* Revista de Aeronáutica y Astronáutica, nº817, octubre de 2012, pp. 849-852.

- GONZÁLEZ HURTADO, J.A.: *Delincuencia informática: daños informáticos del artículo 264 del Código Penal y propuesta de reforma,* Tesis doctoral, Departamento de Derecho Penal de la Universidad Complutense de Madrid, Madrid, 2013. Disponible en: https://eprints.ucm.es/23826/1/T34976.pdf

- LEWIS, J.A.: *Computer spionage. Titan rain and China,* Technology and Public Policy Program, Center for Strategic and International Studies, diciembre 2005. Disponible en: http://cybercampaigns.net/wp-content/uploads/2013/05/Titan-Rain-Moonlight-Maze.pdf

- LEZERTUA RODRÍGUEZ, M: *El proyecto de Convenio sobre cibercrimen de Consejo de Europa: proteger el ejercicio de derechos fundamentales en las redes informáticas,* Cuadernos europeos de Deusto, nº 25, 2001, pp. 83-118.

- LORDOÑO, F.: *Los delitos informáticos en el proyecto de reforma en actual trámite parlamentario,* Revista Chilena de Derecho Informático, nº4,

2004, pp. 171-190. Disponible en: https://revistas.uchile.cl/index.php/RCHDI/article/view/10679

- LOWMAN, S.: *The effect on file and disc encryption on computer forensics,* Lowmanio, enero de 2010. Disponible en: https://www.lowmanio.co.uk/share/The%20Effect%20of%20File%20and%20Disk%20Encryption%20on%20Computer%20Forensics.pdf

- MATA y MARTÍN, R.: *Delitos cometidos mediante sistemas informáticos (estafas, difusión de materiales pornográficos, ciberterrorismo,* Cuadernos Penales Jose María Lidón (Universidad de Deusto), nº4, 2007, pp. 129-171.

- MORALES GARCÍA, O.: *Criterios de atribución de responsabilidad penal a los prestadores de servicios e intermediarios de la sociedad de la información,* Cuadernos de Derecho Judicial, nº9 (dedicado a "Delincuencia informática: problemas de responsabilidad), 2002, pp. 179-240.

- MORÓN LERMA, E. y RODRÍGUEZ PUERTA, M.: *Traducción y breve comentario del Convenio sobre Cibercriminalidad*, Revista de derecho y proceso penal, nº 7, 2002, pp.167-200.

- ORTIZ PRADILLO, J.C.: *Determinación de la jurisdicción y competencia para la investigación y enjuiciamiento de los daños informáticos,* Ponencia de 23 de mayo de 2016 en el Centro de Estudios Jurídicos del Ministerio de Justicia. Disponible en: https://www.fiscal.es/fiscal/PA_WebApp_SGNTJ_NFIS/descarga/ponencia%20Ortiz%20Pradillo%20Juan%20Carlos.pdf?idFile=cd54640d-efbe-4839-bb98-27f9b0c17d67

- ROBLES CARRILLO, M.: *El ciberespacio: presupuestos para su ordenación jurídico-internacional,* Revista Chilena de Derecho y Ciencia Política, volumen 7, nº1, enero-abril del 2016, pp. 1-43.

- ROVIRA DEL CANTO, E.: *Nuevas formas de ciberdelincuencia intrusiva: el hacking y el grooming,* Iuris: actualidad y práctica del Derecho, nº 160, 2011, pp. 36-44.

- SANZ PASCUAL, J.: *¿Una sociedad digital?,* Manual Formativo ACTA nº010, 1998, pp. 29-36. Disponible en: https://www.acta.es/medios/articulos/comunicacion_e_informacion/010027.pdf

4. Documentos de alcance jurídico:

a. Consejo de Europa:

- Chart of signatures and ratifications of Treaty 185 "Convention on Cybercrime", status as of 16/01/2019. Disponible en: https://www.coe.int/web/conventions/full-list/-/conventions/treaty/185/signatures

- Convenio del Consejo de Europa para la prevención del terrorismo, firmado en Varsovia en 2005. Disponible en: https://eurlex.europa.eu/legalcontent/ES/TXT/PDF/?uri=CELEX:22018A0622(01)&from=ES

- Convenio sobre la Ciberdelincuencia del Consejo de Europa (Convenio de Budapest) del 2001. Disponible en: https://www.oas.org/juridico/english/cyb_pry_convenio.pdf

b. Normativa y decisiones comunitarias:

- Decisión nº 854/2005/CE del Parlamento Europeo y del Consejo, de 2 de mayo de 2005, relativa al interés de fomentar un uso más seguro de Internet y las nuevas tecnologías en línea

- 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. Disponible en: https://www.boe.es/buscar/doc.php?id=DOUE-L-2004-80095

- Decisión Marco 2005/222/JAI del Consejo de 24 de febrero de 2005 relativa a los ataques contra los sistemas de información. Disponible en: https://www.boe.es/doue/2005/069/L00067-00071.pdf

- Directiva 2008/114/CE del Consejo, de 8 de diciembre de 2008, sobre la identificación y designación de infraestructuras críticas europeas y la evaluación de la necesidad de mejorar su protección. Disponible en: https://www.boe.es/buscar/doc.php?id=DOUE-L-2008-82589

- Directiva 95/46/CE del Parlamento Europeo y del Consejo de 24 de octubre de 1995 relativa a la protección de las personas físicas en lo que

respecta al tratamiento de datos personales y a la libre circulación de estos datos. Disponible en: https://www.acave.travel/sites/default/files/comunitario-Directiva%2095-46-CE.pdf

- Directiva 2013/40/UE del Parlamento Europeo y del Consejo, de 12 de agosto de 2013 relativa a los ataques contra los sistemas de información y por la que se sustituye la Decisión Marco 2005/222/JAI del Consejo de 24 de febrero de 2005. Disponible en: https://www.boe.es/doue/2013/218/L00008-00014.pdf

- Directiva 2014/41/CE del Parlamento Europeo y del Consejo de 3 de abril de 2014. Disponible en: https://www.boe.es/doue/2014/130/L00001-00036.pdf

- EUROJUST: *Informe Anual 2016*, página 31. Disponible en: http://eurojust.europa.eu/doclibrary/corporate/eurojust%20Annual%20Reports/Annual%20Report%202016/AR2016_ES.pdf

- Reglamento 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de esos datos y por el que se deroga la Directiva 95/46/CE. Disponible en: https://www.boe.es/doue/2016/119/L00001-00088.pdf

c. Normativa española:

- Código Penal español. Disponible en: https://www.boe.es/buscar/pdf/1995/BOE-A-1995-25444-consolidado.pdf

- Ratificación del Convenio de Budapest por España publicado el 17 de septiembre de 2010 en el BOE nº 226 de 2010. Disponible en: http://www.boe.es/boe/dias/2010/09/17/pdfs/BOE-A-2010-14221.pdf

d. Resoluciones y acuerdos judiciales:

- Acuerdo de 3 de febrero de 2005 del Tribunal Supremo español reunido en pleno no jurisdiccional. Disponible en: http://www.poderjudicial.es/cgpj/es/Poder-Judicial/Tribunal-Supremo/Jurisprudencia-/Acuerdos-de-Sala/Acuerdos-de-3-de-febrero-de-2005-sobre--1--Principio-de-ubicuidad---2--Clausulas-de-reserva-de-dominio-y-

prohibicion-de-enajenar---3--Principio-de-minimos-psicoactivos-en-relacion-al-art--368-CP

- Auto del Tribunal Supremo de España de 21 de enero de 1998 (cuestión 3550/1997). Disponible en: http://www.poderjudicial.es/search/contenidos.action?action=contentpdf&databasematch=TS&reference=893254&links=ubicuidad&optimize=20060309&publicinterface=true

- Sentencia del Tribunal Constitucional español nº 102/2000 de 10 de abril de 2000. Recurso de amparo 4.077/98. Disponible en: https://www.boe.es/diario_boe/txt.php?id=BOE-T-2000-9227

- Sentencia del Tribunal Constitucional español nº 159/1987 de 26 de octubre de 1987. Disponible en: http://hj.tribunalconstitucional.es/en/Resolucion/Show/891

- Sentencia del Tribunal de Justicia de la Unión Europea (Sala Primera) de 19 de abril de 2012 relativa al C-523/10. Disponible en: http://curia.europa.eu/juris/document/document.jsf;jsessionid=162F93D927771F84AA2A723D605DAD6A?text=&docid=121744&pageIndex=0&doclang=ES&mode=lst&dir=&occ=first&part=1&cid=9688423

e. Resoluciones y estudios de Naciones Unidas:

- ASAMBLEA GENERAL DE NACIONES UNIDAS: *Nota verbal de fecha 27 de noviembre de 2001 dirigida al Secretario General por las Misiones Permanentes del Canadá y de los Países Bajos ante las Naciones Unidas y anexo con los principios de Princeton sobre la jurisdicción universal*, Quincuagésimo sexto período de sesiones Tema 164 del programa, Establecimiento de la Corte Penal Internacional, 4 de diciembre de 2001. Disponible en: https://digitallibrary.un.org/record/457330/files/A_56_677-ES.pdf?version=1

- Convenio de Naciones Unidas del año 2000 Contra la Delincuencia Organizada Transnacional. Disponible en: https://www.unodc.org/documents/treaties/UNTOC/Publications/TOC%20Convention/TOCebook-s.pdf

- ONU: *A Cyberspace Treaty - a United Nations Convention or Protocol on cybersecurity and Cybercrime*, Documento A/CONF.213/IE/7 preparado por Stein Schjolberg, 12º Congreso de la ONU sobre Justicia Penal y Prevención del Delito, celebrado en Salvador, Brasil, del 12 al 19 de abril de 2010. Disponible en: http://www.cybercrimelaw.net/documents/UN_12th_Crime_Congress.pdf

- ONU: *Crimes related to computer networks, Background paper for the workshop on crimes related to the computer network*,10th UN Congress on the Prevention of Crime and the Treatment of Offenders, 2000, A/CONF.187/10. Disponible en: https://www.unodc.org/documents/congress//Previous_Congresses/10th_Congress_2000/017_ACONF.187.10_Crimes_Related_to_Computer_Networks.pdf

- ONU: *Novedades recientes en el uso de la ciencia y la tecnología por los delincuentes y por las autoridades competentes en la lucha contra la delincuencia, incluido el delito cibernético,* Documento de trabajo preparado por la Secretaría, 12º Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal, 22 de enero de 2010. Disponible en: https://www.unodc.org/documents/crime-congress/12th-CrimeCongress/Documents/A_CONF.213_9/V1050385s.pdf

f. Varios:

- Convenio Iberoamericano de Cooperación sobre Investigación, Aseguramiento y Obtención de Prueba en materia de Ciberdelincuencia del 2014. Disponible en: https://www.mec.gub.uy/innovaportal/file/52706/1/ciber_convenio.pdf

5. Páginas web:

- DE ALZAGA, P. y PASTOR, E.: *El virus del amor colapsa ordenadores de todo el mundo,* Diario del Navegante, 5 de mayo del 2000. Disponible en: https://www.elmundo.es/navegante/2000/05/05/ailofiu_virus.html

- GJELTEN, T.: *Extending de Law of War to ciberspace,* programa de radio del 22 de septiembre del 2010 en la NPR. Transcripción disponible en: http://www.npr.org/templates/story/story.php?storyId=130023318

- Cooperación judicial en materia penal: http://www.europarl.europa.eu/factsheets/es/sheet/155/la-cooperacion-judicial-en-materia-penal

- MCGUINNESS, D.: *Cómo uno de los primeros ciberataques rusos de la historia transformó a un país*, BBC, 6 de mayo de 2017. Disponible en: https://www.bbc.com/mundo/noticias-39800133

- PERRY BARLOW, J.: *Declaración de independencia del ciberespacio.* Disponible (en español) en: https://nomadasyrebeldes.files.wordpress.com/2012/05/manifiesto_de_john_perry_barlow-1.pdf m