DOI: 10.14718/NovumJus.2017.11.1.2

LOS RETOS PROCESALES DE LA CRIMINALIDAD INFORMÁTICA DESDE UNA PERSPECTIVA ESPAÑOLA

Lorena Arocena Alonso
Iñaki Esparza Leibar
Universidad del País Vasco/Euskal Herriko Unibertsitatea

Resumen

Dada su cotidianeidad, la criminalidad informática adquiere un papel muy importante y valioso en la sociedad del siglo XXI. No se pueden obviar las características intrínsecas de los delitos informáticos, pues demandan un tratamiento procesal específico en comparación con los delitos convencionales. Sin embargo, aunque la analogía ha sido la protagonista en esta materia durante un largo período en España, llegan nuevos tiempos con el Convenio sobre cibercriminalidad y la Ley Orgánica 13/2015, cuyos ejes conductores son la capacitación de todos los operadores jurídicos y la cooperación internacional.

Palabras clave: delitos informáticos, capacitación, cooperación internacional, tutela judicial efectiva, debido proceso, tratamiento procesal específico.

Los autores: Lorena Arocena Alonso es abogada. Correo electrónico: lorenaarocena@gmail.com
Iñaki Esparza Leibar es doctor en Derecho. Catedrático de Derecho Procesal en la Facultad de Derecho de la Universidad del País Vasco/Euskal Herriko Unibertsitatea. Correo electrónico: inaki.esparza@ehu.eus

Recibido: 23 de agosto de 2016; ***evaluado:*** 18 de noviembre de 2016; ***aceptado:*** 5 de diciembre de 2016.

DOI: 10.14718/NovumJus.2017.11.1.2

THE PROCEDURAL CHALLENGES OF CYBERCRIMINALITY FROM A SPANISH PERSPECTIVE

Lorena Arocena Alonso
Iñaki Esparza Leibar
Universidad del País Vasco/Euskal Herriko Unibertsitatea

Abstract

Given its everyday nature, cybercriminality plays an important and relevant role in 21st-century society. The intrinsic characteristics of cybercrimes cannot be ignored, as they require a specific procedural treatment in comparison with conventional crimes. Nevertheless, although analogy has been the protagonist in this matter for a long time in Spain, new times are coming with the Convention on Cybercrime and Organic Law 13/2015, whose guiding principles are the training of all legal operators and international cooperation.

Keywords: cybercrimes, training, international cooperation, effective judicial protection, due process, specific procedural treatment.

About the authors: Lorena Arocena Alonso is a lawyer. Email: lorenaarocena@gmail.com
Iñaki Esparza Leibar has a PhD in Law. Professor of Procedural Law at the Faculty of Law of the Universidad del País Vasco/Euskal Herriko Unibertsitatea. Email: inaki.esparza@ehu.eus

Received: August 23, 2016; ***evaluated:*** November 18, 2016; ***accepted:*** December 5, 2016.

Introducción

El presente artículo forma parte de la investigación que se llevó a cabo para confeccionar un trabajo de grado para la Universidad del País Vasco/Euskal Herriko Unibertsitatea, en el que Iñaki Esparza Leibar tuvo el papel de director.[1]

La necesidad de abordar esta materia es consecuencia de que la sociedad avanza y evoluciona y, junto a ella, ha de hacerlo el Derecho. Esta es la premisa de la que partimos a la hora de abordar los delitos informáticos, una realidad candente fruto de las nuevas tecnologías. A partir de su constante transformación, nos encontramos con los primeros problemas, pues el factor humano es el principal obstáculo para adaptar tanto la ley como la jurisprudencia a los nuevos cambios sociales,[2] lo que termina traduciéndose en tipos penales abiertos e indeterminación.

La delincuencia también se nutre de los cambios sociales. En consecuencia, además de brindarnos múltiples facilidades e información, las nuevas tecnologías también configuran nuevas oportunidades para la comisión de delitos. Esto no quiere decir que a la vez surjan nuevos bienes jurídicos que proteger, ya que la tendencia general es a que se vean afectados los bienes jurídicos tradicionales, mediante un elemento en particular: la aplicación de las nuevas tecnologías.[3]

Tal es la relevancia de los delitos informáticos que es la tercera potencia delictiva y afecta a más de 500 millones de personas. El desconocimiento y la inconsciencia con los que se utilizan las nuevas herramientas dan lugar a que millones de usuarios no sepan llevar a cabo actuaciones sencillas de prevención.

> Cuando nos mandan mensajes de estos que van en cadena, que hay que reenviar para tener un día de suerte o apoyar a una fuerza política, podemos estar contribuyendo a facilitar la obtención de datos personales como nuestro

1 Para consultar el documento completo se puede acudir al Repositorio Institucional de la Universidad del País Vasco/Euskal Herriko Unibertsitatea>Docencia>F. Derecho>Trabajos académicos-Grado Derecho. Fue publicado el 18 de julio de 2016, con el título *La odisea procesal de la criminalidad informática*, a nombre de Lorena Arocena Alonso. Asimismo, se puede acceder mediante el enlace http://hdl.handle.net/10810/18654

2 José María Álvarez-Cienfuegos Suárez, "Aspectos procesales en relación con la investigación de delitos informáticos", *Revista Catalana de Seguretat Pública*, núm. 3 (1998): 27.

3 Ignacio Benítez Ortuzar, "Informática y delito. Aspectos penales relacionados con las nuevas tecnologías" en *Reforma del Código Penal. Respuestas para una sociedad del siglo XXI*, comp. Lorenzo Morillas Cueva, María José Cruz Blanca y Gonzalo Quintero Olivares (Madrid: Dykinson, 2009), 112.

> número de teléfono o correo haciendo un flaco favor a nuestra persona, que a saber las consecuencias según en manos de quien caiga.[4]

La distancia, la instantaneidad, la comisión de delitos en masa, el componente internacional, la cualificación necesaria para cometerlos o el anonimato en la autoría son algunas de las características que se identifican con los delitos informáticos.[5] Estos rasgos indican la necesidad de una cooperación policial y judicial, si se pretende conseguir que los delitos informáticos no queden impunes. Como producto de esta colaboración internacional, tenemos el Convenio sobre Ciberdelincuencia, del Consejo de Europa del 23 de noviembre de 2001; un primer paso en esta área, pero no definitivo.[6]

Lo que hay que tener claro es que el especial medio que sirve como herramienta para la comisión de los delitos informáticos nos obliga a conceptualizar una específica línea de investigación y enjuiciamiento, en aras de no procurar la impunidad de estos delitos.[7] El resultado es que los delitos informáticos se catalogan dentro del Derecho informático, que es el conjunto de normas que regula todas las relaciones que tengan que ver con la informática.[8]

El desconocimiento ha sido la causa de tantos años de impunidad y de desorientación. No hay que olvidar que Internet es mucho más grande que lo que un simple usuario puede llegar a pensar, pues la parte que se ve no es más que "la punta del iceberg". En este sentido, hay que hablar de deep web (también conocida como Internet profunda o hidden web, entre otros), el lugar a donde los motores de búsqueda como Google o Yahoo no pueden llegar y almacena un 80% del contenido real de Internet. Por supuesto, es el medio que utilizan muchos ciberdelincuentes para evitar dejar rastro y hacer que su persecución sea más dificultosa, si se carecen de los medios y los conocimientos adecuados.[9]

---

4 Chinchilla, Antonia. "Ciberdelincuencia: ojo al dato". http://diario-informacion.vlex.es/vid/ciberdelincuencia-ojo-dato-523529010 (acceso marzo 8, 2017). Por su parte, San Juan, Vozmediano y Vergara indican que la percepción de inseguridad parece ser mayor respecto del hecho de ser víctima de un robo en la calle, pese a ser más probable ser víctima de un delito informático. César San Juan, Laura Vozmediano y Ana Vergara, "Miedo al delito en contextos digitales: un estudio con población urbana", *Eguzkilore*, núm. 23 (2009): 178.

5 Eloy Velasco Núñez, *Delitos cometidos a través de Internet: cuestiones procesales* (Madrid: La Ley, 2010), 47.

6 Benítez Ortuzar, "Informática y delito", 112-114.

7 María Concepción Rayón Ballesteros y José Antonio Gómez Hernández, "Cibercrimen: particularidades en su investigación y enjuiciamiento", *Anuario Jurídico y Económico Escurialense*, núm. 47 (2014): 211.

8 Leyre Hernández Díaz, "El delito informático", *Eguzkilore*, núm. 23 (2009): 227-228.

9 A pesar de las dificultades de persecución que entraña la Deep Web por su inexpugnabilidad, la Operación Internacional Onymous parece haber abierto brechas importantes en la misma. Arantzazu López-Barberá,

Dada la complejidad que supondría llevar a cabo también el análisis de los aspectos procesales de los delitos informáticos cometidos en la deep web, nos centraremos en la surface web o Internet superficial.

En resumen, el hecho de que hayan tenido que transcurrir tantos años para avanzar en la regulación de la investigación de los delitos informáticos de la Internet superficial no nos deja en un buen lugar, si la meta es conseguir que no haya impunidad ni siquiera en la deep web.

1. Justificación de un tratamiento procesal específico

Las características propias de los delitos informáticos conllevan ciertas singularidades en su tratamiento procesal, como pone de relieve Velasco Núñez. No en vano uno de los rasgos más representativos de esa peculiaridad reside en la nota de internacionalidad. Esto conlleva la necesaria colaboración entre los Estados para poder acumular los delitos y evitar que desaparezcan pruebas, así como aplicar agravaciones genéricas[10] y agravaciones específicas.[11] De otra forma sería imposible apreciar el *modus operandi* del delincuente y, además, puesto que los delitos informáticos suelen tener una pena inferior a cinco años, esta medida también previene que se venzan los plazos de prescripción que, debido a la pena, van a ser cortos.[12]

Dadas las incógnitas que rodean a los delitos informáticos, como la ocultación de la autoría mediante diferentes técnicas, el proceso para conseguir resultados es lento y depende mucho de la prueba pericial técnica, complementada con otras actuaciones intermedias como pantallazos, análisis de los archivos, etc., múltiples factores que conllevan "menor eficacia, resumida en el aserto certísimo de que obliga a investigaciones muy complejas, caras e intrusivas, para ser finalmente castigados con poca pena".[13]

"Deep web' o Internet profundo", *Seguritecnia: Revista Decana Independiente de Seguridad*, núm. 407 (2014): 96-97; *El País*, "Golpe policial a la 'Deep Web", http://el-pais.vlex.es/vid/golpe-policial-deep-web-543508626 (acceso marzo 8, 2017).

10 Con agravaciones genéricas, hemos de pensar sobre todo en la agravación por delito continuado del Artículo 74 del Código Penal. Velasco Núñez, *Delitos cometidos a través de Internet*, 49.

11 Ejemplo de agravación específica en relación con los delitos informáticos es la recogida en el Artículo 250.4 del Código Penal, ya que en atención a la especial gravedad de la estafa, basados en el valor de su defraudación, esta se considera estafa de especial gravedad. Velasco Núñez, *Delitos cometidos a través de Internet*, 49.

12 Velasco Núñez, *Delitos cometidos a través de Internet*, 48-50.

13 Velasco Núñez, *Delitos cometidos a través de Internet*, 50.

1.1. Principios que orientan la persecución de los delitos informáticos

El Artículo 22[14] del Convenio sobre cibercriminalidad aboga en primer lugar por la territorialidad, salvo en algunos casos excepcionales en los que permite que se aplique el principio de personalidad. Sin embargo, la nota de transnacionalidad de los delitos informáticos dificulta el empleo del principio de territorialidad *stricto sensu*.[15] El resultado ha sido que los Estados han procurado ampliar el criterio seguido por el Convenio con base en otros delitos y dar lugar a diversas teorías o versiones sobre la competencia para enjuiciar los delitos informáticos.

1.1.1 Ubicuidad

En los delitos informáticos hay que partir de la premisa de que muchas veces quedan afectados varios países. Esto resulta de que en múltiples ocasiones el delincuente comete el hecho delictivo desde un lugar del mundo y la consecuencia se presenta en otra parte.[16] Esta situación ha planteado muchos debates sobre el foro y el juez competente, ya que la víctima solo suele saber que ha sido atacada; no sabe quién es el autor y mucho menos desde dónde ha actuado.

Por si estos fueran pocos problemas, el autor puede cometer el hecho delictivo desde un ordenador que ni siquiera está fijo:

> […] y que puede redireccionar a través de diversos servidores ubicados no sólo en lugares sino incluso países diversos, o a través de servicios de Internet, que además de estar en localizaciones en ocasiones alejadas entre sí, producen efectos en muchos y muy diversos emplazamientos geográficos, las más de las veces llegando a ocupar diverso ámbito internacional.[17]

Cuando se abordó la cuestión sobre el órgano jurisdiccional que iba a ser competente, con base en otros delitos convencionales, una parte de la doctrina propuso la teoría de la acción. Según esta, el juez competente debía de ser aquel del lugar desde donde se ha cometido el hecho delictivo. Estaríamos, por tanto, ante un concepto

[14] "Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para afirmar su jurisdicción respecto de cualquier delito previsto con arreglo a […]". Consejo de Europa, *Convenio sobre la Ciberdelincuencia* (Budapest, 23 de noviembre de 2001), art. 22.1.

[15] José Luis de la Cuesta Arzamendi y Norberto J. de la Mata, coords., *Derecho Penal Informático* (Madrid: Civitas, 2010), 247-248.

[16] Velasco Núñez, *Delitos cometidos a través de Internet*, 55.

[17] Velasco Núñez, *Delitos cometidos a través de Internet*, 56.

de "acción" cuya interpretación dista de la tradicional, pues hay que entenderla como realización parcial de la misma —no acción típica completa—, que sería lo que habilitaría para enjuiciar la causa. Se admitiría como lugar de comisión de los hechos aquel en el que esté ubicado el servidor, que es a donde el autor manda los datos para almacenarlos.[18]

Sin embargo, en Derecho el consenso no es tan fácil. Otra parte de la doctrina abogaba porque el juez competente sea aquel del lugar en donde se hubieran producido los resultados, puesto que hasta entonces no habría ningún tipo de perjuicio. El "resultado" se ha de entender como afección del bien jurídico protegido. Esto se traduce en que cualquier Estado puede manifestar que los juzgados de su jurisdicción son competentes por el simple hecho de que se ha producido un "peligro abstracto" de un bien jurídico que es susceptible de protección en su ordenamiento jurídico.[19]

Para evitar discusiones vanas que no iban a llegar a ningún lado en una materia en la que la inmediatez en la actuación es fundamental, el Tribunal Supremo[20] tomó cartas en ella. El Tribunal concluyó, consciente de su nota de internacionalidad, que los delitos informáticos se producen en todos los lugares donde se exteriorizan sus consecuencias; esto abarca tanto el lugar de comisión como el de resultado.[21]

Con esa postura, el Tribunal Supremo se posicionó a favor del principio de la ubicuidad y, por tanto, puede ser competente cualquier juzgado de instrucción en cuyo partido judicial se hubiera manifestado alguna parte del hecho criminal. Dicho de otra forma, serían competentes los juzgados y tribunales españoles si el hecho delictivo se comete desde el territorio nacional o si se lleva a cabo desde fuera, pero tiene consecuencias o resultados en el territorio. Basta con que algún elemento pueda relacionarse con la circunscripción española para que esta pueda ser competente.[22] La decisión del Tribunal Supremo aboga por el principio de ubicuidad, la cual compartimos porque es la mejor alternativa para evitar que los delitos informáticos queden impunes.

---

18 De la Cuesta Arzamendi y De la Mata, coords., *Derecho Penal Informático*, 249-250.

19 De la Cuesta Arzamendi y De la Mata, coords., *Derecho Penal Informático*, 250.

20 "El delito se comete en todas las jurisdicciones en las que se haya realizado algún elemento del tipo. En consecuencia, el Juez de cualquiera de ellas que primero haya iniciado las actuaciones procesales, será en principio competente para la instrucción de la causa". Tribunal Supremo, Sala General, *Acuerdo no jurisdiccional de 3 de febrero de 2005*.

21 Velasco Núñez, *Delitos cometidos a través de Internet*, 56.

22 De la Cuesta Arzamendi y De la Mata, coords., *Derecho Penal Informático*, 250-252.

Esta regla no es más que una pauta inicial acorde con el Artículo 15 Ley de Enjuiciamiento Criminal, pues si en el transcurso de la investigación se averigua el lugar concreto desde donde se ha cometido el hecho delictivo, entonces, de acuerdo con el mismo Artículo, cabe la inhibición a favor del competente según las reglas del Artículo 14.

Es necesario hacer una serie de precisiones respecto a la distribución competencial de los procesos de pornografía infantil. Puede darse el caso de que existan diversos usuarios y que cada uno se ubique en diferentes partidos judiciales. En este supuesto, el Tribunal Supremo[23] respalda la idea de que se tramiten tantas causas como imputados, salvo que pueda demostrarse fehacientemente estar ante un supuesto de codelincuencia.[24]

Ya se opte por la acción, por el resultado o por ambas, las tres vías tienen sus ventajas y desventajas, lo que muestra la complejidad y dificultad de la persecución efectiva de los delitos informáticos y el trabajo que se ha de realizar para diluir esferas de impunidad a causa de lagunas en la penalidad.

1.1.2. Universalidad

Ha quedado claro que una de las características principales de los delitos informáticos suele ser su nota de internacionalidad. Sin embargo, si vamos a la legislación que regula el funcionamiento del Poder Judicial en el ordenamiento jurídico español, encontraremos que no se consideran delitos de persecución universal, ya que no se recogen en el listado del Artículo 23.4 de la Ley Orgánica del Poder Judicial, pues la relación de delitos recogidos afecta a bienes jurídicos concretos que necesitan de una persecución reforzada a consecuencia de su propia naturaleza.

Por justicia universal se entiende la ampliación de excepciones respecto a la aplicación de la territorialidad de la ley penal.[25] La única forma de que entre en juego el principio de universalidad en relación con los delitos informáticos es vincularlos con los recogidos en el precepto citado. Por ejemplo, si el sabotaje informático se asocia con el terrorismo, podría ser de persecución universal.

[23] Audiencia Nacional, Sala de lo Penal, *Sentencia 14/2001, de 10 de marzo*, M. P. Rosa María Arteaga Cerrada.
[24] Velasco Núñez, *Delitos cometidos a través de Internet*, 56-57.
[25] De la Cuesta Arzamendi y De la Mata, coords., *Derecho Penal Informático*, 248.

Según Velasco Núñez, la crítica que se puede hacer a esto es que los delitos informáticos, que atacan la seguridad en la Red, al final afectan un bien jurídico que es de protección supranacional y, en consecuencia, se les debería aplicar también la nota de universalidad.[26]

Al igual que con la teoría de la ubicuidad, la pornografía infantil merece una serie de especificaciones. Este delito informático es de persecución universal por una doble vía dentro del ordenamiento jurídico español. La primera es la del Artículo 23.4.k) LOPJ, relativa a delitos contra la libertad e indemnidad sexual cometidos sobre víctimas menores de edad, siempre y cuando se cumplan los requisitos establecidos en el mismo. La otra vía es la del Artículo 189.1 b) del Código Penal referente al tráfico de material pornográfico infantil, independientemente de que su origen sea extranjero o desconocido. Si la procedencia del material es desconocida, sobre la base del Artículo 65.1 e) LOPJ deberían ser competentes los juzgados centrales de instrucción de la Audiencia Nacional. Sin embargo, se prefiere la aplicación del principio de ubicuidad y que conozca la causa aquel juez que la haya conocida primero.[27]

1.1.3. Cosa juzgada y non bis in ídem

Dado el carácter transnacional de los delitos informáticos, a la hora de dilucidar la competencia también se han de tener en cuenta las reglas de Derecho Procesal Penal Internacional.

En aras del principio del juez predeterminado por la ley y del derecho a un juicio justo con todas sus garantías, hay que tener siempre muy presente que queda prohibido que se castigue por los mismos hechos a la misma persona en diferentes ordenamientos jurídicos. Se trata de evitar el *bis in ídem*, sin perjuicio de que hasta que se dilucide el tema de la competencia —en nuestro caso, los juzgados españoles— puedan seguir investigando[28] respecto a hechos delictivos que no se están enjuiciando en ningún otro Estado, para evitar que se pierdan pruebas. Si los juzgados españoles no son los competentes, se procede a la acumulación a favor del Estado que mejor foro tiene.

[26] Velasco Núñez, *Delitos cometidos a través de Internet*, 58.
[27] Velasco Núñez, *Delitos cometidos a través de Internet*, 58-59.
[28] Audiencia Nacional, Sala de lo Penal. *Sentencia 14/2001*; Tribunal Supremo, Sala General. *Acuerdo no jurisdiccional de 3 de febrero de 2005*.

El proceso penal tiene dos fases: la de investigación y la del juicio oral. Lo explicado se predica respecto a la fase de investigación. Sin que pueda ser de otra forma, en el juicio oral hay que favorecer el mayor número de garantías posible y eso solo se consigue si dicho juicio es único y se evitan los dobles enjuiciamientos.

Ante esta situación, podríamos plantearnos cómo se informan los jueces de si la causa que están investigando sobre un delito informático también se está enjuiciando fuera del territorio nacional. Esta labor está encomendada a organismos internacionales[29] que hacen la función de intermediarios entre los jueces para una eficaz coordinación.

La competencia suele atribuirse al Estado que esté en mejores condiciones para garantizar los derechos fundamentales de todo aquel que tenga que intervenir en el procedimiento. Asimismo, se valoran elementos[30] para estimar su idoneidad.

También podría darse el caso de que al hecho delictivo se le aplicara el principio de jurisdicción universal. Ante esta situación, la inacción por parte del Estado donde ocurren los hechos no es óbice para que conozca la causa cualquier otro juzgado de otro Estado que tenga buenas condiciones. Por supuesto, siempre y en todo caso, con respeto por el principio de *non bis in ídem* para evitar que haya dobles enjuiciamientos.[31]

1.2. Personal especializado

Desde su creación, Internet ha sido un escenario complejo que ha provocado que el Derecho se vea desbordado por la velocidad a la que avanza. Esta novedad conlleva dejar el pasado atrás y seguir la estela de pilares y planteamientos nuevos. La primera dificultad con la que nos encontramos es que los juristas tardan en

[29] Por ejemplo, Eurojust para la Unión Europea. Para más información, puede verse la página web oficial: http://www.eurojust.europa.eu/Pages/home.aspx

[30] Los elementos que se tienen en consideración son "las obligaciones convencionales bilaterales y multilaterales entre los países implicados; la naturaleza y gravedad intrínseca del delito; el lugar de su comisión (principio de territorialidad); la nacionalidad del autor (principio de personalidad activa); la nacionalidad de las víctimas (principio de personalidad pasiva); los intereses nacionales afectados (principio real o de protección de los intereses esenciales de un Estado); disponibilidad de las pruebas materiales del delito, lugar de su obtención y posibilidades de su detección y transmisión; residencia o presencia del acusado, o su lugar de refugio o detención; lugar donde están los testigos; lugar donde se encuentran las víctimas; prioridad en razón de la fecha de comienzo de las investigaciones; coincidencia del idioma oficial del Tribunal y mayoría de pruebas personales y documentales, y conveniencia de las partes procesales". Velasco Núñez, *Delitos cometidos a través de Internet*, 61-62.

[31] Velasco Núñez, *Delitos cometidos a través de Internet*, 59-63.

comprender los problemas que entraña la tecnología y cuando se entienden, la elaboración de instrumentos normativos que resuelvan los problemas en torno a la persecución de los delitos informáticos es muy lenta y, en consecuencia, entran en vigor para quedar obsoletos en poco tiempo.[32]

Si se parte de la premisa de que la cooperación es la única vía para atajar la cibercriminalidad, a todo lo señalado habría que añadir que la experiencia en delitos informáticos no es la misma en diferentes Estados. Si a eso le sumamos el hecho de que la cooperación entre ellos dista de ser la ideal, nos encontramos con lugares de impunidad en unos delitos con un marcado carácter transnacional.

No podemos pasar por alto que para el rastreo de los delitos informáticos se necesitan ciertos conocimientos técnicos de toda la cadena de personal implicado en el asunto, desde la policía hasta el juez. Tan es así, que tanto el Cuerpo Nacional de Policía como la Guardia Civil y Fiscalía se han visto en la necesidad de poner en marcha secciones especializadas para investigar los delitos informáticos y llevar a cabo una territorialización de esta especialización.[33]

1.2.1. En el ámbito policial

Los delitos informáticos tienen la dificultad añadida de que resulta difícil saber de dónde proviene el hecho delictivo, ya que los autores suelen ocultar su rastro; además, muchas veces el quid de la cuestión es encontrar al organizador del mismo que, en la mayoría de las ocasiones, no es el que comete la transgresión. Así pues, resolver estas cuestiones requiere que las fuerzas y cuerpos de seguridad de los Estados actúen en consonancia, con instrumentos adecuados para la persecución de los delitos informáticos y con personal especializado, dada la complejidad que entrañan.[34]

Dentro del proceso para perseguir efectivamente los delitos informáticos, el primer eslabón de la cadena es la Policía, que es la encargada de investigar mediante las adecuadas diligencias de investigación. Por eso, es importante que este primer obstáculo sea superado con éxito, pues de otra forma el proceso fracasará y ni siquiera

[32] Antonio Pedro Rodríguez Bernal, "Los cibercrímenes en el espacio de libertad, seguridad y justicia", *Revista de Derecho Informático*, núm. 103 (2007): 8.

[33] Velasco Núñez, *Delitos cometidos a través de Internet*, 69-70.

[34] Jorge Alexandre González Hurtado, "Delincuencia informática: daños informáticos del artículo 264 del Código Penal y propuesta de reforma" (Tesis doctoral, Universidad Complutense de Madrid, Departamento de Derecho Penal, 2013), 268.

podremos llegar al juicio oral. Así, el éxito en este primer punto solo puede ser alcanzado mediante la ciberinteligencia policial.

El Tribunal Europeo de Derechos Humanos ya ha advertido a España en más de una ocasión sobre su escasa regulación respecto a estos temas.[35] El triunfo policial se obtiene por medio de la cooperación interpolicial, que se logra cuando los problemas más habituales se plantean en los foros o congresos y, sobre la base de estos, se elaboran acuerdos de cooperación.

Para conseguir una lucha efectiva contra la cibercriminalidad, es indispensable conocer el medio mejor que los propios autores.[36] Aunque el criminal intente camuflar su identidad, resulta difícil que no queden rastros, ya sea por una razón u otra; es ahí en donde la Policía tiene que entrar en escena para aprovecharse de los puntos débiles de Internet.

Respecto a la actuación policial, encontramos grandes avances tanto en Europa como en el país. De entrada, hay que destacar la creación del Centro Europeo de la Ciberdelincuencia y de la Escuela Europea de Policía que, en conjunto, brindan un marco óptimo para la formación de la Policía y el inicio de la investigación que promueve la cooperación interpolicial. En España, también cabe subrayar el papel fundamental de la Policía Judicial, que principalmente está integrada por la Guardia Civil y el Cuerpo Nacional de Policía.

1.2.2. En el ámbito judicial

Bien es cierto que la Policía constituye el primer eslabón de la cadena y que su actuación para perseguir los delitos informáticos precisa de conocimientos técnicos y de no cometer fallos para que el proceso no fracase.

No obstante, no podemos olvidarnos del resto de la cadena que también ha de hacer su trabajo de forma efectiva y eficaz. Esto se consigue con una especialización suficiente por parte de la Fiscalía, de los jueces y los magistrados.

[35] Albert González Jiménez, "Las diligencias policiales y su valor probatorio" (Tesis doctoral, Universidad Rovira i Virgili, Departamento de Derecho Privado, Procesal y Financiero, 2014), 17.

[36] Juan Carlos Ruiloba Castilla, "La actuación policial frente a los déficits de seguridad de Internet", *Revista de Internet, Derecho y Política*, núm. 2 (2006): 56, 61.

- ***Fiscalía de Criminalidad Informática***

A pesar de la existencia en España de una Delegación de Criminalidad Informática desde 2005, es con la Instrucción 2/2011[37] que se introduce una especialización, al crear la Fiscalía de Criminalidad Informática. Esta especialización surgió como una necesidad, habida cuenta de los malos datos en la lucha contra los delitos informáticos y la proliferación de casos, dado que el uso cada vez más habitual de Internet nos ha llevado a la creación de nuevas formas de criminalidad.[38]

Para paliar esta situación e ir camino al éxito, se hizo necesario reforzar la actuación del Ministerio Fiscal y la mejor manera para ello fue la especialización, porque los delitos informáticos requieren conocimientos específicos y técnicos concretos. No obstante, no todo hecho delictivo en el que se utilicen las tecnologías de información y comunicación puede incluirse entre los asuntos que trata esta Fiscalía especial, pues esto solo nos llevaría a la desnaturalización de esta especialización y a que la unidad quedara desbordada de trabajo.[39]

No era aconsejable elaborar un catálogo cerrado, pues como es lógico, el mundo tecnológico avanza sin parangón y con el paso del tiempo se crearán otras formas de criminalidad informática o nuevos mecanismos para cometer los delitos informáticos ya tipificados en el Código Penal.

Entre sus funciones están cumplir con las pautas establecidas por la Fiscalía General del Estado, intervenir en los procedimientos más complejos de los hechos delictivos de los que debe encargarse, colaborar de forma efectiva cuando el ciberdelito afecte a territorios de diferentes Fiscalías Provinciales, elaborar un informe anual, colaborar con las unidades especializadas de las fuerzas y cuerpos de seguridad del Estado, participar en las reuniones organizadas para la unificación de criterios, etc.[40]

37 Fiscalía General del Estado, *Instrucción 2/2011*, "Sobre el Fiscal de Sala de Criminalidad Informática y las Secciones de Criminalidad Informática de las Fiscalías" (Madrid: Fiscal.es, 11 de octubre de 2011).
38 Rayón Ballesteros y Gómez Hernández, "Cibercrimen", 216.
39 Fiscalía General del Estado, *Instrucción 2/2011*.
40 Fiscalía General del Estado, *Instrucción 2/2011*.

- ***Jueces y magistrados***

Según nuestra Ley de leyes, que recoge los derechos fundamentales reconocidos a los ciudadanos del territorio español, los jueces y magistrados son quienes tienen que velar por la no vulneración de los mismos, ya sea en la fase de investigación como en la fase del juicio oral.

Como ha podido evidenciar en la práctica Jorge Bermúdez, fiscal delegado de Delitos Informáticos en España, la realidad es que muy pocos jueces o magistrados son diestros en esta materia. La mayoría de las diligencias de investigación tecnológica requieren mandato judicial, pero ¿cómo va a entender el juez o magistrado todos los extremos de lo que se le solicita, si carece de especialización en el área de la ciberdelincuencia? ¿Cómo va a ponderar que la diligencia solicitada es la adecuada?

Son algunas de las preguntas que nos vienen a la cabeza inmediatamente cuando nos dicen que los jueces y magistrados no son duchos en ciberdelitos. Es cierto que tienen un abanico de cursos a los que pueden asistir a lo largo del año, pero en el hipotético caso de que escogiesen el relativo a la ciberdelincuencia, un curso de uno o un par de días no es suficiente cuando estamos ante una disciplina tan compleja y tan técnica, que es la razón por la que haya tanta impunidad al respecto. No obstante, hay que encomiar la tarea de aquellos jueces como Velasco Núñez, que sí han profundizado en este campo por motivaciones personales, cuyas resoluciones sí pueden ser debidamente motivadas.[41]

En conclusión, los delitos informáticos exigen un plus en comparación con los delitos tradicionales, como conocimientos técnicos por parte de todos los funcionarios que participan en el proceso y cooperación internacional por el carácter transnacional de los mismos.

Podemos apreciar que en el campo policial se han hecho muchos avances y no se trata de un sector olvidado. La evolución constante y la creación de organismos europeos reflejan un buen primer punto de partida. La crítica ha de hacerse a nuestro ordenamiento jurídico. Si bien la Policía Judicial obtiene cada vez mejores resultados y no deja de invertir en la lucha contra la ciberdelincuencia, el lado flaco está en la legislación, pues esta institución debería regularse de forma más amplia

[41] Toda la información fue obtenida en entrevista personal con el fiscal Jorge A. Bermúdez, delegado de Criminalidad Informática en España.

y específica, con una estructura jerarquizada que ponga orden y no haga que nos preguntemos si una determinada Policía forma parte del cuerpo de la Policía Judicial.

Por otro lado, el aspecto más sombrío de la cualificación proviene de las esferas judiciales. Tenemos grandes progresos con la creación de la Fiscalía de Criminalidad Informática, ya que esto promueve que haya fiscales centrados en esta materia y no en el reparto habitual de los delitos tradicionales, lo que se traduciría en inexperiencia y en una labor menos profesional.

Sin duda alguna, la peor parte, que hay que resolver de inmediato, proviene de los jueces y magistrados que no poseen conocimientos técnicos suficientes para dictar sus resoluciones de forma suficientemente motivada. Paradójico, pues, que aquellos que son garantes de los derechos y las libertades de los ciudadanos y que tienen que asegurar un proceso con todas las garantías sean los que más trabajo tengan por delante.

2. Retos para una real tutela judicial efectiva: la garantía del debido proceso

En el Artículo 24.1[42] se consagra el derecho a la tutela judicial efectiva, sin que pueda producirse indefensión. Este derecho tiene su vertiente positiva y su vertiente negativa. La primera de ellas hace referencia a que toda persona tiene derecho a acudir al juez para que resuelva su problema en un juicio que respete todas las garantías y mediante una resolución motivada en Derecho. La segunda vertiente[43] hace alusión a que no puede haber indefensión.[44]

No podemos pasar por alto que vivimos en un Estado de Derecho, lo que conlleva que para la resolución de conflictos se haga uso del debido proceso para garantizar a los ciudadanos esta tutela efectiva de sus derechos e intereses legítimos. Al día de

[42] "Todas las personas tienen derecho a obtener la tutela efectiva de los jueces y tribunales en el ejercicio de sus derechos e intereses legítimos, sin que, en ningún caso, pueda producirse indefensión". España, *Constitución Española de 1978* (Madrid: *Boletín Oficial del Estado* No. 311, 29 de diciembre de 1978), art. 24.1.

[43] El Tribunal Constitucional se manifestó sobre la vertiente negativa de la tutela judicial efectiva, al afirmar en su Fundamento Jurídico Primero que se trata del "empleo de los medios lícitos necesarios para preservar o restablecer una situación jurídica perturbada o violada, consiguiendo una modificación jurídica que sea debida, tras un debate (proceso), decidido por un órgano imparcial (jurisdicción)". Tribunal Constitucional, Sala Segunda, *Sentencia 48/1984, de 4 de abril*. M. P. Luis Díez-Picazo y Ponce de León.

[44] Olaf Bernárdez Cabello e Ignacio Ramos-Paúl de la Lastra, "Retos de la tutela judicial efectiva frente a las ciberamenazas" en *Retos del Derecho ante las nuevas amenazas*, coord. María Susana de Tomás Morales (Madrid: Dykinson, 2015), 116.

hoy, resulta evidente que no es posible una organización que goce de una única soberanía planetaria para resolver las controversias en todo el mundo. La falta de voluntad comporta que el proyecto fracase, pero si en verdad la hubiera, el único camino que podríamos seguir es el del proceso debido. Como promueve Esparza Leibar, hay que apostar por el proceso debido, cuyo resultado final no es otro que la consecución de la justicia.[45]

El debido proceso es inevitablemente positivo para los ciudadanos con la finalidad de conseguir justicia, ya que se trata de un modelo que no está estancado, sigue enriqueciéndose y es el único compatible con un verdadero Estado de Derecho. A modo ejemplificativo de su buen hacer tenemos el espacio judicial europeo, en el que los países que se nieguen a modificar su ordenamiento jurídico en la dirección adecuada, no tendrán otro resultado que estar condenados:

> […] al ostracismo, a la autarquía, al aislamiento, a la pobreza y al fracaso. Incluso pudiendo ser actor en el escenario internacional, lo será incómodo, interesado y poco fiable para el resto, lo que constituirá con toda probabilidad, el inicio de un círculo vicioso.[46]

> Por tanto, toda actividad probatoria debe de llevarse a cabo garantizando el respeto a la tutela judicial efectiva del sujeto, en lo que se refiere a su admisión y práctica en el procedimiento judicial, de forma que todas las capacidades de detección, reacción, análisis, recuperación, respuesta, investigación y coordinación a que se refiere la Estrategia de Ciberseguridad han de practicarse respetando las garantías procesales de las personas para que resulten exitosas.[47]

Estas razones resultan muy poderosas para que la resolución de los delitos informáticos respete el proceso debido en todas sus facetas.

[45] Iñaki Esparza Leibar, "El proceso debido como único modelo aceptable para la resolución de conflictos en un estado de derecho y como presupuesto para la globalización" en *El Derecho Procesal español del siglo XX a golpe de tango: Liber Amicorum, en homenaje y para celebrar su LXX cumpleaños*, coord. Juan-Luis Gómez Colomer, Silvia Barona Vilar, Pía Calderón Cuadrado (Valencia: Tirant lo Blanch, 2012), 337-338.

[46] Esparza Leibar, "El proceso debido como único modelo aceptable", 337-338.

[47] Bernárdez Cabello y Ramos-Paúl de la Lastra, "Retos de la tutela judicial efectiva", 116.

2.1. Problemas que plantean las nuevas diligencias de investigación tecnológica sobre las garantías procesales del sospechoso

Al margen de la configuración constitucional existente en el Artículo 18 en relación con la ciberdelincuencia, la nueva Ley Orgánica 13/2015, de modificación de la Ley de Enjuiciamiento Criminal, ha supuesto un gran avance en un sector que apenas tenía regulación y donde la regla general era la analogía para resolver los problemas. El simple hecho de que el constituyente fuera consciente en 1978 de los peligros que podría entrañar la Informática para los derechos fundamentales, si se utilizaba mal, nos muestra la gran relevancia que tiene esta reforma.

Esta legislación española en materia de delitos informáticos se caracteriza, como apunta Rubio Alamillo, por ser ambigua y poco clara, hecho que se refleja en el uso de lenguaje "incorrecto", pues utiliza de forma indistinta conceptos que no son lo mismo. Con la nueva ley, no queda del todo claro si hemos dado dos pasos hacia delante o uno hacia atrás, ya que la tutela judicial efectiva podría verse afectada al vulnerar derechos fundamentales de los sospechosos y crearles indefensión.[48] Todavía es pronto para saber cómo se va a emplear en la práctica; tal vez, los que han de aplicar la ley aprecien estos peligros y diagnostiquen la enfermedad antes de que salga a la superficie.

Es comprensible que el Legislador no tenga conocimientos informáticos, pero sin duda debe rodearse de los profesionales apropiados para que lo asesoren. Esta cuestión podía haberse resuelto de mejor forma, vista la redacción de algunos artículos. La reforma versa sobre la manera como se han de investigar los delitos informáticos, pero un cariz muy importante introducido por esta Ley es que ahora es posible la suspensión de los derechos fundamentales de los sospechosos en algunos supuestos, algo que no se permitía antes de la reforma —salvo excepciones, como delitos cometidos en el seno de una organización criminal—.[49]

Una de las diligencias que podemos encontrar consiste en que un policía informático puede mandar archivos ilícitos a un sospechoso en el marco de una investigación ¿Cuál es el problema? Si no existe un inventario sobre los archivos ilícitos enviados por los policías informáticos auditados por profesionales en la materia y con sus respectivos códigos *hash*, esto podría dar lugar a errores de diversa índole. Si no

[48] Javier Rubio Alamillo, "La informática en la reforma de la Ley de Enjuiciamiento Criminal", *Diario La Ley*, núm. 8662 (2015): 3.

[49] Rubio Alamillo, "La informática en la reforma de la Ley", 3-4.

existe un control sobre esos archivos que la Policía envía para entrar en el círculo del sospechoso, por ejemplo, podría atribuirse al sospechoso un delito que no ha cometido si, ante una eventual requisa de su dispositivo, encuentran en el mismo dichos archivos ilícitos previamente enviados por la Policía. Una diligencia pensada, sobre todo, para la pornografía infantil y que el problema que plantea no está resuelto.

En el Artículo 588 ter a,[50] el Legislador vuelve a caer en la generalidad. Al no ser más claro, esto se traduce en que cualquier persona podrá ser investigada por el mero hecho de tener algún tipo de contacto telefónico o mediante aplicaciones informáticas con un sujeto que sea sospechoso de haber cometido un hecho delictivo. El Legislador debió precisar el tipo de información transmitida para que puedan intervenirse las comunicaciones de esa tercera persona.

Por otro lado, los prestadores de servicios de comunicaciones también tienen el deber de colaborar según el Artículo 588 ter e LECrim,[51] es decir, cuando se les pida una determinada información, han de cederla. Traducción: un ciudadano inocente podría ver afectado su derecho a la intimidad al encontrar que sus datos personales han sido cedidos a la justicia por el simple hecho de haber escrito comentarios subidos de tono en un foro o tener contacto directo y habitual con alguien que lo hace.[52]

Asimismo, de la lectura del Artículo 588 sexies a LECrim[53] podemos deducir que el Legislador no le ha dado la importancia debida a algo tan importante como la

[50] "La autorización para la interceptación de las comunicaciones telefónicas y telemáticas solo podrá ser concedida cuando la investigación tenga por objeto alguno de los delitos a que se refiere el artículo 579.1 de esta ley o delitos cometidos a través de instrumentos informáticos o de cualquier otra tecnología de la información o la comunicación o servicio de comunicación". Ministerio de Gracia y Justicia, *Real Decreto de 14 de septiembre de 1882*, art. 588 ter a. Presupuestos.

[51] Deber de colaboración: "1. Todos los prestadores de servicios de telecomunicaciones, de acceso a una red de telecomunicaciones o de servicios de la sociedad de la información, así como toda persona que de cualquier modo contribuya a facilitar las comunicaciones a través del teléfono o de cualquier otro medio o sistema de comunicación telemática, lógica o virtual, están obligados a prestar al juez, al Ministerio Fiscal y a los agentes de la Policía Judicial designados para la práctica de la medida la asistencia y colaboración precisas para facilitar el cumplimiento de los autos de intervención de las telecomunicaciones. 2. Los sujetos requeridos para prestar colaboración tendrán la obligación de guardar secreto acerca de las actividades requeridas por las autoridades. 3. Los sujetos obligados que incumplieren los anteriores deberes podrán incurrir en delito de desobediencia". Ministerio de Gracia y Justicia, *Real Decreto de 14 de septiembre de 1882*, art. 588 ter e.

[52] Rubio Alamillo, "La informática en la reforma de la Ley", 4-5.

[53] Necesidad de motivación individualizada: "1. Cuando con ocasión de la práctica de un registro domiciliario sea previsible la aprehensión de ordenadores, instrumentos de comunicación telefónica o telemática o dispositivos de almacenamiento masivo de información digital o el acceso a repositorios telemáticos de datos,

cadena de custodia y que serán la Policía Judicial y el juez en cuestión los que decidan en cada caso concreto cómo se ha de practicar tal cadena.

La custodia es esencial para que estemos ante un proceso con todas las garantías, ya que sin ella sería muy fácil modificar o destruir lo incautado y se daría lugar a pruebas contaminadas. En definitiva, no se estarían haciendo efectivas las garantías que propician el derecho a la tutela judicial efectiva.

Para que nos hagamos a la idea de lo sensible que es la cadena de custodia, veamos el siguiente ejemplo. Supongamos que hay una información o unos archivos que nos interesan en un disco duro o en una memoria USB. El simple acto de conectarlos a un ordenador sin haber llevado a cabo ningún tipo de interacción contamina la prueba. Por ello, el disco duro o la memoria USB se han de conectar a bloqueadores de escritura para que no queden directamente conectados al ordenador. La conclusión que se extrae de esto es que la cadena de custodia no es baladí y que si queremos asegurar las garantías procesales, lo idóneo es utilizar material forense especializado para clonar[54] el contenido y proporcionar un código *hash*.

Así pues, aunque en nuestro ordenamiento jurídico se garantice la cadena de custodia, en la práctica queda condicionada a la buena fe de los funcionarios que vayan a intervenir. Si algún funcionario tuviera interés en modificar algún contenido y lo hiciera, no dejaría rastro y nadie se enteraría.[55]

Otra imprecisión lingüística que el Legislador ha pasado por alto es que la Ley habla de copias de datos y no de copias de dispositivos. Para copiar datos no queda de otra que acceder al propio contenido, lo que supondría una contaminación directa de la prueba; cuando se copian datos, los archivos eliminados no se copian, razón por la cual lo adecuado es un clonado.[56]

---

la resolución del juez de instrucción habrá de extender su razonamiento a la justificación, en su caso, de las razones que legitiman el acceso de los agentes facultados a la información contenida en tales dispositivos. 2. La simple incautación de cualquiera de los dispositivos a los que se refiere el apartado anterior, practicada durante el transcurso de la diligencia de registro domiciliario, no legitima el acceso a su contenido, sin perjuicio de que dicho acceso pueda ser autorizado ulteriormente por el juez competente". Ministerio de Gracia y Justicia, *Real Decreto de 14 de septiembre de 1882*, art. 588, sexies a.

54 No confundir "clonar" con "copiar". Se trata de conceptos diferentes para la Informática Forense. Rubio Javier Alamillo, "Clonación de discos duros en el peritaje informático", http://peritoinformaticocolegiado.es/clonacion-de-discos-duros-en-el-peritaje-informatico (acceso marzo 8, 2017).

55 Rubio Alamillo, "La informática en la reforma de la Ley", 5-6.

56 Rubio Alamillo, "La informática en la reforma de la Ley", 6-7.

Existen más ejemplos de los errores que se han cometido con la nueva Ley Orgánica, pero estos son suficientes para ilustrar la encrucijada jurídica que nos proporciona. Si bien el constituyente en 1978 era consciente de los peligros que podía entrañar el mundo digital, hoy esa certeza parece haberse evaporado, cuando de forma inexplicable la Ingeniería Informática es la única que ni siquiera está regulada por el Estado.

En conclusión, no podemos estar más de acuerdo con los temores manifestados por el fiscal Bermúdez,[57] así como con lo expresado por Rubio Alamillo:

> [La] Ley de Enjuiciamiento Criminal ha sido redactada sin el correcto asesoramiento técnico, que se abre un nuevo tiempo de inseguridad jurídica en el que los derechos fundamentales de los ciudadanos podrán ser suspendidos por la simple sospecha de la comisión de delitos considerados menores, que sigue sin establecerse un reglamento que garantice el mantenimiento de la cadena de custodia de dispositivos informáticos intervenidos y, finalmente, que la Policía Judicial podrá enviar a nuestros ordenadores, si considera que somos sospechosos de cometer delitos incluso menores, todo tipo de ficheros ilícitos y troyanos que podrán espiar nuestro ordenador y comunicaciones, que no serán auditados por los únicos profesionales que conocen en profundidad la Informática y las redes y que, teniendo en cuenta que, de entrada, no serán indexados y almacenados de forma segura, podrán aparecer en nuestros sistemas informáticos en intervenciones que realice la Policía Judicial en nuestros domicilios, como ficheros conseguidos de forma ilícita.[58]

2.2. El escaso desarrollo de la informática forense en España en detrimento de la tutela judicial efectiva

Los sistemas informáticos almacenan información y, para que esta sea válida en un proceso legal, se ha creado la Informática Forense. Bernárdez Cabello la entiende como "la aplicación de técnicas científicas y analíticas especializadas a infraestructuras y dispositivos tecnológicos que permitan identificar, preservar, analizar y presentar datos que sean válidos dentro de un proceso legal".[59]

[57] Impresiones obtenidas en la entrevista personal con el fiscal Jorge A. Bermúdez, delegado de Criminalidad Informática en España.

[58] Rubio Alamillo, "La informática en la reforma de la Ley", 8.

[59] Bernárdez Cabello y Ramos-Paúl de la Lastra, "Retos de la tutela judicial efectiva", 116.

El quid de la cuestión reside en obtener la información necesaria, que esta pueda ser válida en un proceso legal y que, a la vez, no se cree indefensión. Esta última parte es la que más problemas genera, pues resulta difícil determinar dónde está la barrera a partir de la cual los derechos de las personas quedan afectados. Hay que tener en cuenta que la Informática Forense suele practicarse sobre todo en la prueba documental y en el informe pericial. Por tanto, hemos de centrarnos en ellos.

2.2.1. La prueba documental

Si acudimos a la Ley de Enjuiciamiento Civil,[60] nos encontramos con que se recoge de forma amplia el término "documento". Sin embargo, en cuanto al valor probatorio hay que matizar si se trata de un documento público o privado.[61]

De acuerdo con el Artículo 319 LEC, los documentos públicos hacen prueba plena del hecho, acto o estado de cosas que documenten —con la posibilidad de impugnación en algunos casos—, mientras los documentos privados, aunque también hacen prueba plena, dejan de tener ese valor si son impugnados por la parte perjudicada. No obstante, el valor probatorio del documento privado, no es impedimento para que el juez o el tribunal lo valore de acuerdo con la sana crítica y en conjunto con las demás pruebas.

La LEC no es la única que habla del documento en estos términos: la jurisprudencia[62] también se ha decantado por esta amplitud. En la STS 1066/2009 podemos apreciar que el Tribunal Supremo equipara el documento tradicional con el documento electrónico, a consecuencia de la falta de regulación exhaustiva en torno a la ciberdelincuencia en la que la analogía ha estado a la orden del día.

Si el documento informático es impugnado por falta de veracidad, la parte que lo ha aportado ha de demostrar su autenticidad, sin perjuicio de que luego el juez o tribunal lo valore de acuerdo con las reglas de la sana crítica.[63] En definitiva,

60 La prueba documental se regula en Jefatura del Estado, *Ley 1/2000*, "De enjuiciamiento civil" (Madrid: *Boletín Oficial del Estado* No. 7, 8 de enero de 2000), arts. 382-384.

61 Para más información sobre qué se entiende por documento público ver la definición del Código Civil en su Artículo 1216. No obstante, en el Artículo 317 LEC se enlistan los documentos públicos que tienen valor probatorio.

62 Tribunal Supremo, Sala de lo Penal, *Sentencia 1066/2009, de 4 de noviembre*, M. P. José Antonio Martín Pallín, fundamento jurídico segundo.

63 Bernárdez Cabello y Ramos-Paúl de la Lastra, "Retos de la tutela judicial efectiva", 117-118.

tener que recurrir a la analogía no es precisamente la mejor forma de asegurar las garantías procesales y promover la tutela judicial efectiva.

2.2.2. El informe pericial

El informe pericial tiene lugar cuando para valorar un hecho de especial relevancia se requieren conocimientos científicos o artísticos. Según el articulado de la LECrim, el informe pericial se ha de hacer por dos peritos designados por el juez de oficio que, además, tienen la obligación de jurar o prometer decir la verdad y de responder con la mayor objetividad posible haciendo gala de su profesionalidad.

Es necesario volver a abordar aquí el tema del valor probatorio —en este caso, del informe pericial—. Los peritos deben responder a las preguntas y a las repreguntas e incluso el informe puede llegar a ser prueba anticipada[64] en los casos en los que lo permite la ley. Aquí también el juez o el tribunal seguirá las reglas de la sana crítica, de acuerdo con el Artículo 348 LEC.[65]

El asunto es diferente en el caso de la prueba pericial informática. En esta casuística no se puede pasar por alto que existe una certificación de calidad, según la normativa ISO 27001 e ISO 71505. La ventaja que nos aporta el hecho de que nos encontremos con una certificación radica en que en esta se establece una serie de criterios que se han de tener en cuenta a la hora de elaborar el informe pericial informático.[66]

Hasta aquí todo parece idílico y mejor regulado en el sector de la criminalidad informática. Nada más lejos de la realidad, cuando lo cierto es que en nuestro ordenamiento jurídico se desconoce su existencia y ni siquiera se exige en sede judicial.[67] Dicho de otra forma, la informática forense en España dista de ser tan eficaz como debiera ser; a pesar de tener las herramientas para ello, no se sabe por qué motivo se obvian. El resultado es que puede crearse indefensión, puesto que los informes no se practican de la forma en la que debiera hacerse, a causa de que los jueces y magistrados no tienen conocimientos suficientes sobre la materia

64 Ministerio de Gracia y Justicia, *Real Decreto de 14 de septiembre de 1882*, art. 730.

65 Valoración del dictamen pericial: "El tribunal valorará los dictámenes periciales según las reglas de la sana crítica". Jefatura del Estado, *Ley 1/2000*, art. 348.

66 Bernárdez Cabello y Ramos-Paúl de la Lastra, "Retos de la tutela judicial efectiva", 118-119.

67 Bernárdez Cabello y Ramos-Paúl de la Lastra, "Retos de la tutela judicial efectiva", 119.

como para exigir unos requisitos mínimos de validez de la prueba, así como para poder juzgarla con las reglas de la sana crítica.

No podríamos estar más de acuerdo con Bernárdez Cabello cuando afirma que "se aprecia la inexistencia de un marco jurídico operativo y eficaz que permita la persecución del ciberterrorismo y ciberdelincuencia en los términos previstos por la *Estrategia*[68] *de Ciberseguridad Nacional*.[69]

2.2.3. Derecho comparado: Estados Unidos como referencia

En Estados Unidos existe una regulación en la que se recoge que los peritos tienen que ser expertos en la materia en cuestión y que los métodos o principios que se apliquen al caso concreto sean fiables. A partir de esta premisa, hay dos principales diferencias en comparación con la legislación española en materia de informática forense:

> Se requiere que el testigo sea experto por conocimiento, capacidades, experiencia, prácticas y educación. Con lo cual los criterios para poder presentar el informe pericial son más exigentes, no limitándose a los aspectos subjetivos del perito.
>
> Se ha de acreditar que el testimonio está basado en principios y métodos fiables y que esos principios y métodos se han aplicado al caso concreto. Con lo cual, se ha de dar cuenta de lo que se ha hecho y por qué.[70]

Asimismo, introducen una distinción en cuanto a si se trata de un documento original o una copia, símbolo de la importancia que se le otorga allí a la cadena de custodia. La parte que introduzca la prueba ha de demostrar que esta es real.[71]

---

68 "La Estrategia de Ciberseguridad Nacional es el documento estratégico que sirve de fundamento al Gobierno de España para desarrollar las previsiones de la Estrategia de Seguridad Nacional en materia de protección del ciberespacio con el fin de implantar de forma coherente y estructurada acciones de prevención, defensa, detección, respuesta y recuperación frente a las ciberamenazas". Gobierno de España, Presidencia del Gobierno, *Estrategia de Ciberseguridad Nacional* (Madrid: Autor, 2013), 1.

69 Bernárdez Cabello y Ramos-Paúl de la Lastra, "Retos de la tutela judicial efectiva", 117-119.

70 Bernárdez Cabello y Ramos-Paúl de la Lastra, "Retos de la tutela judicial efectiva", 120.

71 Bernárdez Cabello y Ramos-Paúl de la Lastra, "Retos de la tutela judicial efectiva", 120.

Si se tiene como guía el manual *Forensic Examination of Digital Evidence: A Guide for Law Enforcement*,[72] la Informática Forense ha de seguir una serie de pautas: la valoración, la adquisición, el examen y la documentación de la evidencia. Así es como el informe pericial puede tener un real valor probatorio. En la primera, el perito valora la evidencia de forma amplia y general para tomar la decisión sobre qué acciones son necesarias. En la segunda, puesto que la evidencia digital es muy fácil de alterar o destruir, se elabora una copia (mejor, un clonado) de la original para trabajar sobre ella. En tercer lugar, se recupera la información contenida en el soporte que la almacenaba y se procede a su interpretación, una vez esté en formato lógico. En último lugar, es muy importante que todo el proceso haya sido documentado por el perito mediante un informe.[73] Así se respetan las máximas garantías posibles de la evidencia y se evita la indefensión, como pretende el Artículo 24 CE de nuestro ordenamiento jurídico, que recoge el derecho a la tutela judicial efectiva.[74]

En definitiva:

> […] lo más relevante del caso estadounidense es que todas las autoridades, agencias, fiscales y jueces, son formados en la materia, de forma que la valoración de la prueba se hace desde unos conocimientos básicos de la informática forense que tienen por objeto garantizar que el medio de prueba ha sido analizado con respecto de todas las garantías procesales, lo cual permite por tanto la introducción de dicha prueba en el proceso, quedando respetado el derecho a la tutela judicial efectiva.[75]

Por otro lado, hay que resaltar la poca Informática Forense que hay en España, lo que va en perjuicio de la tutela judicial efectiva, pues podemos encontrarnos con casos en los que no se respeten todas las garantías. Así pues, se requieren cambios normativos como operativos.

¿Cómo formular una Informática Forense en España que siga la estela de la estadounidense? Para comenzar, como se ha venido insinuando, es necesario que se regule la figura del perito informático para asegurar que se trata de una persona

[72] National Institute of Justice, *Forensic Examination of Digital Evidence: A Guide for Law Enforcement* (Washington: Autor, 2004), 1-91.
[73] Bernárdez Cabello y Ramos-Paúl de la Lastra, "Retos de la tutela judicial efectiva", 119-121.
[74] Bernárdez Cabello y Ramos-Paúl de la Lastra, "Retos de la tutela judicial efectiva", 121.
[75] Bernárdez Cabello y Ramos-Paúl de la Lastra, "Retos de la tutela judicial efectiva", 121.

con la cualificación suficiente para emitir un juicio correcto sobre la evidencia. Se debería desarrollar reglamentariamente el Artículo 478 LECrim, que recoge el contenido del informe pericial, para que las exigencias sean más similares a las de Estados Unidos. Para ello, es necesario invertir más en I+D, porque se necesitan equipos informáticos de alta tecnología para poder hacer unas buenas copias (clonado) de las evidencias y analizar los resultados, así como para formar a los peritos en el uso de estos equipos.[76]

Quizás uno de los aspectos más importantes sería el de formar a todas las personas que sean parte del proceso en la lucha contra los delitos informáticos, para que cuando tengan entre manos un informe puedan identificar con facilidad que se han respetado todas las garantías. Tal cuestión es relevante en el caso de los jueces y tribunales, puesto que sin la debida formación no pueden valorar el informe forense de acuerdo con las reglas de la sana crítica.[77]

No podemos olvidar que para que se respete el derecho fundamental de la tutela judicial efectiva se han de respetar absolutamente todas las garantías, resultado que solo se puede conseguir mediante el proceso debido, ya que como indica Lorca Navarrete, la sustantividad del debido proceso "no es ajena al cómo institucional que la hace posible y que incide en la prestación del servicio público de la justicia".[78]

3. La cooperación internacional como única vía

El carácter transnacional de los delitos informáticos ya nos da una pista sobre cómo se puede avanzar en esta materia y luchar contra la impunidad. Díaz Gómez parece haber captado cuál es el camino y, por tanto, sus palabras serán tomadas como referencia.

Hemos avanzado desde el caso Yahoo o el caso Dow Jones vs. Joseph Gutnick,[79] pero todavía queda un largo camino para llegar a un estado de seguridad y de gran eficacia en materia de criminalidad informática. Venimos de una reciente reforma tanto en el Código Penal como en la Ley de Enjuiciamiento Criminal, ambas de

[76] Bernárdez Cabello y Ramos-Paúl de la Lastra, "Retos de la tutela judicial efectiva", 122.

[77] Bernárdez Cabello y Ramos-Paúl de la Lastra, "Retos de la tutela judicial efectiva", 121-122.

[78] Antonio María Lorca Navarrete, "El derecho procesal como sistema de garantías", *Boletín Mexicano de Derecho Comparado* XXXVI, núm. 107 (2003): 557.

[79] Son dos importantes casos de la jurisprudencia internacional que los tribunales siempre tienen como referencia. Andrés Díaz Gómez, "El delito informático, su problemática y la cooperación internacional como paradigma de su solución: El Convenio de Budapest", *Redur* 8 (2010): 175-176.

2015, que reflejan el esfuerzo del Legislador español para adecuar la situación a las esferas europeas e internacionales y dar una mejor cobertura a la persecución de los delitos informáticos.

No obstante, hay que tener cuidado: ya que el Derecho Penal está reservado para las conductas más graves, hay que ponderar si se necesita un nuevo tipo penal o si sería suficiente con que esa determinada conducta fuera desvalorada por alguna regulación administrativa o civil. En algunas legislaciones sí que se han tomado malas decisiones.

La mayor dificultad radica en el Derecho Procesal Penal Internacional. Es imperativo conjugar los esfuerzos de todos los Estados en aras de poner en marcha políticas conjuntas y generales que no solo les afecten a ellos, sino a todos los sectores de la sociedad. El camino nos indica, entonces, que la dirección correcta es elaborar convenios multilaterales para abarcar al mayor número posible de Estados.[80] Mientras haya Estados que no colaboren en esta lucha internacional, la impunidad seguirá a la orden del día, ya que los buenos criminales informáticos se informarán de aquellos lugares ideales para sus planes y se beneficiarán de esas lagunas.

La cooperación internacional pasa por fomentar el desarrollo del Derecho Penal Informático, de las normas procesales y de la cooperación de las Administraciones de justicia de los diferentes Estados. Dicha colaboración está íntimamente relacionada con la solidaridad intercultural: hay que respetar todas las sociedades existentes y dar la bienvenida a todas las ideas y propuestas posibles.

La generalidad desempeña un papel tanto positivo como negativo. Como no podía ser de otra forma, la desventaja consiste en la dificultad de poner de acuerdo a tantos Estados, cuando cada uno tiene su propia realidad y, por supuesto, sus propios intereses.[81]

La cooperación pasa por un mayor intercambio de información. Para que se materialice de forma efectiva, en la práctica este intercambio ha de superar dos fases. La primera de ellas es el intercambio nacional entre instituciones, órganos y autoridades, es decir, entre las fuerzas y cuerpos de seguridad del Estado, instituciones gubernamentales y los órganos jurisdiccionales. Una vez se consigue que

[80] Díaz Gómez, "El delito informático", 182-183.
[81] Díaz Gómez, "El delito informático", 187.

la información fluya sin impedimentos, hay que ponerse a trabajar en la segunda fase. Esta se refiere a un intercambio de información internacional, que pone en marcha normas de Derecho Procesal Penal Internacional para que esta transmisión se haga mediante las herramientas adecuadas.

La transmisión de información se ha de caracterizar por agilidad y rapidez, sin que el fin justifique los medios y que en el camino echemos por tierra los derechos y las garantías que asisten a los ciudadanos. Es esta la mayor ventaja de la cooperación internacional, dado su carácter transversal que afecta a la actividad administrativa y jurisdiccional común. Más allá, no se puede abordar una política común sin tener en cuenta a las víctimas y a los delincuentes: para las víctimas, hay que establecer medios sencillos de denuncia, posibilitar el acceso a una reparación efectiva de los daños, garantizar que se persigan adecuadamente los delitos informáticos, etc. Respecto al delincuente, no podemos olvidarnos de respetar sus derechos humanos, reconocidos y consolidados por sendos textos internacionales.[82]

Como se ha indicado, el campo donde más se ha de trabajar para obtener una mayor cooperación internacional es en el ámbito procesal. Este hecho lo confirma la doctrina que viene solicitando mayor armonización procesal en la lucha contra la criminalidad informática y que en la práctica el Derecho Penal sustantivo haya sido relegado a un segundo plano por el Derecho Procesal Penal Internacional.

Hay que entender que lo que se necesita es la armonización y no la duplicidad de tipos y de penas que generan inseguridad. En resumidas cuentas, el objetivo de la cooperación internacional es que no haya conductas que estén penadas en un sitio y en otro no, por lo que hay que evitar a toda costa la existencia de "paraísos delictivos".[83]

En línea con las pautas de Díaz Gómez, una correcta cooperación internacional debería revestir o cumplir una serie de requisitos. El punto de partida, sin duda alguna, tiene que ser un pensamiento universal para abarcar al máximo número posible de Estados. Por otro lado, esta cooperación ha de detentar límites formales y materiales. Con los formales nos referimos a que hay que respetar cada uno de los ordenamientos jurídicos, así como los tratados internacionales; los materiales

[82] A efectos de más datos sobre la transmisión de la información, consultar Díaz Gómez, "El delito informático", 188-189.

[83] Díaz Gómez, "El delito informático", 190.

hacen referencia a que hay que respetar los principios propios del Derecho Penal, ya que estamos ante delitos informáticos, sí, pero delitos, al fin y al cabo.

La cooperación debe provenir de todos los sectores de la sociedad, lo que nos brinda la posibilidad de conseguir una regulación coherente y homogénea donde no haya contradicciones y exista una lógica normativa. La respuesta que se dé atenderá todos los problemas y no dará una solución parcial. Esto está muy relacionado con el carácter transversal de los delitos informáticos, porque estas respuestas tienen que poner atención también al resto del ordenamiento jurídico. Aunque la Unión Europea haya conseguido grandes avances en materia de criminalidad informática, la cooperación debe surgir de las más altas instancias, como Naciones Unidas.[84]

Parece que, hasta el día de hoy, el mayor avance obtenido en materia de cooperación es el Convenio de Budapest o el Convenio sobre cibercriminalidad, elaborado por el Consejo de Europa.[85] La pregunta es: ¿cumple con todos los requisitos mencionados? Se trata de un instrumento internacional que, pese a ser un gran paso de cooperación en la lucha contra la ciberdelincuencia, no es tan perfecto como se hubiera deseado. Aun así, el propio Convenio refleja también el hecho de que en gran parte hay que enfocar los esfuerzos hacia el Derecho Procesal Penal Internacional, ya que los artículos de esta materia en el Convenio superan casi por el doble a los de Derecho Penal Internacional.[86]

Morón Lerma parece indicarnos que el Convenio de Budapest tiene tres objetivos primordiales: "[…] armonizar el Derecho Penal material, establecer medidas procesales o cautelares adaptadas al medio digital y poner en funcionamiento un régimen rápido y eficaz de cooperación internacional".[87] No obstante ciertos errores, no se

84 Díaz Gómez, "El delito informático", 192-194.

85 El Convenio sobre Cibercriminalidad está en vigor para España desde el 1 de octubre de 2010. Fue publicado en el *BOE* del 17 de septiembre de 2010. "Cuestiones prácticas y procesales relacionadas con la investigación de los delitos informáticos", http://190.104.117.163/2014/septiembre/prueba/contenido/ponencias/Anexos/Legislacion/Cuestiones%20practicas%20y%20procesales%20investigacion%20delitos%20informaticos.pdf (acceso marzo 8, 2017), 28.
La ratificación del mismo se produjo el 3 de junio de 2010. Iván Salvadori, "Los nuevos delitos informáticos introducidos en el Código Penal español con la Ley Orgánica 5/2010: perspectiva de Derecho comparado", *Anuario de Derecho Penal y Ciencias Penales* 64, núm. 1 (2011): 251.

86 Para más información puede observarse cómo el Convenio de Budapest dedica los artículos 2 a 13 para regular cuestiones de Derecho Penal Internacional y los artículos 14 a 35 para hacer alusión a temas de Derecho Procesal Penal Internacional. Díaz Gómez, "El delito informático", 196.

87 Esther Morón Lerma y María José Rodríguez Puerta, "Traducción y breve comentario del Convenio sobre Cibercriminalidad", *Revista de Derecho y proceso penal*, núm. 7 (2002): 169; Díaz Gómez, "El delito informático", 196.

vicia el resto del Tratado, que supone un antes y un después en la lucha contra los delitos informáticos.

No hay que olvidar que el mundo digital seguirá avanzando y desarrollándose, por lo que hay que salvar el antagonismo diplomático existente entre los Estados y tomar decisiones conjuntas y coordinadas. La cooperación internacional es la única forma de crear conciencia en los Estados, un elemento muchas veces relegado a un puesto sin importancia, para que cada vez más Estados se sumen a la lucha contra la criminalidad informática.

Conclusiones

La criminalidad informática está rodeada de una serie de términos y de conceptos que no son de fácil comprensión si no se está habituado a ellos. Por esta razón, la legislación —tanto sustantiva como procesal— ha de ir en sintonía con esta terminología. No obstante, por los ejemplos que se han puesto a lo largo de todo el trabajo, parece que el Legislador no se ha rodeado de los técnicos informáticos adecuados para que lo asesoren y eso se ha traducido en que se utilicen como sinónimos términos que no lo son. El hecho de que el Legislador no conozca el mundo digital de primera mano ha llevado a que en la nueva Ley 13/2015, que regula diligencias de investigación tecnológica, nos encontremos con redacciones que, más que solucionar un problema, lo están instaurando al dar casi carta blanca a la Policía Judicial para investigar los delitos informáticos, en detrimento de las garantías procesales.

En el marco nacional, puesto que la Policía Judicial es la encargada de investigar los delitos informáticos en la primera fase del procedimiento, se hace necesaria una regulación específica de la misma para que exista una jerarquía clara que organice las funciones de cada uno y unifique materiales y recursos humanos para evitar un despilfarro de tiempo y dinero. Esta estructura, además, nos sirve para toda la delincuencia y no se trata de algo específico para la criminalidad informática, por lo que los beneficios que puede aportar son múltiples.

El tratamiento para los delitos informáticos no puede ser el mismo que se dispensa a los delitos clásicos o tradicionales. No se puede obviar el hecho de que la delincuencia informática tiene una serie de características intrínsecas que exigen un tratamiento procesal específico.

Para comenzar, a diferencia de lo que ocurre en los delitos tradicionales, en los informáticos observamos que el autor suele cometer el hecho delictivo desde un determinado territorio y que los resultados se materializan en otro muy distinto, lo que le otorga carácter transnacional.

Este acontecimiento dificulta la persecución del mismo, pues posibilita que diferentes órganos jurisdiccionales sean potencialmente competentes; por eso, el Tribunal Supremo optó por aplicar el principio de ubicuidad, que es el que menos zonas de impunidad ofrece. Dicha nota de internacionalidad no es propia de los delitos tradicionales, ya que la acción y el resultado suelen darse en el mismo lugar. Cuestión distinta es la necesidad de cooperación para atrapar al autor del hecho delictivo en el caso de que huya; por tanto, los delitos informáticos precisan de una cooperación internacional sin parangón que implica que deban tratarse de forma específica.

La segunda razón por la que la criminalidad informática precisa un tratamiento procesal específico es por la dedicación y energía que hay que poner para resolverlos en comparación con los convencionales. La mayoría de delitos informáticos queda sin resolver, porque los autores suelen ser personas muy diestras en el mundo digital y, como es lógico, si se desea perseguir estas conductas, se requiere un personal experto, así como herramientas tecnológicas adecuadas que estén a la altura de las que utilizan los cibercriminales.

Dada la dificultad que entrañan los delitos informáticos para su investigación y que la Policía Judicial es la encargada de llevar a cabo las diligencias de investigación en la práctica, resulta lógico que esté especializada en criminalidad informática. Podemos decir orgullosos que nuestra Policía Judicial se ha puesto las pilas, que existen unidades especializadas tanto en la Guardia Civil como en la Comisaría General del Estado y que se invierte constantemente en esta materia para no quedar obsoletas y ser cada vez más eficaces. Incluso, la Policía que tiene un campo de actuación inferior al nacional, como puede ser la Ertzaintza (Policía autonómica del País Vasco), ha creado su propia unidad para los delitos informáticos y está formando a sus trabajadores.

Aunque la Fiscalía también ha hecho avances al crear una Fiscalía Especial, el punto débil lo tenemos en los órganos jurisdiccionales y en los jueces y magistrados que no son duchos en la materia. Al igual que en Estados Unidos, los jueces y magistrados deben tener conocimientos tecnológicos, sobre la base de que la mayoría de las diligencias de investigación tecnológica requieren de mandato judicial; no

es posible que el juez o magistrado motive debidamente sus resoluciones si no es consciente de lo que se le pide o tiene ante sí. Por eso, es necesaria una inminente instrucción en criminalidad informática, una formación específica que les permita conseguir capacitación para tratar esta materia por parte de todo el que intervenga de una forma u otra en el proceso.

Es inadmisible que quienes tienen que asegurar las garantías y los derechos de los ciudadanos sean el eslabón más débil, mientras la Policía Judicial hace esfuerzos para progresar y renovarse. En resumen, hay que remar todos juntos, porque si no, nunca llegaremos a la meta.

La tutela judicial efectiva ha de respetarse en todo momento, por lo que hay que garantizar que se respeten todas las garantías mediante el proceso debido. Aunque la nueva Ley 13/2015 pueda pecar de ambiciosa al pretender abarcar el máximo número de situaciones posibles, inadvertidamente en perjuicio de las mencionadas garantías, hay que alabar el gran paso que supone después de décadas de pedir no una nueva regulación en materia de delitos informáticos, sino una regulación a secas.

Tras localizar los problemas o los aspectos que pueden traer algún que otro quebradero de cabeza, se trata ahora de andar con cautela a la hora de poner en práctica las diligencias de investigación, hasta que todas estas cuestiones "dudosas" sean resueltas mediante una nueva redacción o jurisprudencia.

Es un hecho que España no está a la vanguardia en lo que se refiere a la persecución de los delitos informáticos. Hemos sido condenados en más de una ocasión por el Tribunal Europeo de Derechos Humanos por no tener una regulación al respecto y, al darnos ya por imposibles, se ha conformado con la aplicación de la analogía y un desarrollo jurisprudencial.

La actitud del Legislador español es criticable desde todos los aspectos, para empezar, porque inexplicablemente seguimos teniendo una Ley de Enjuiciamiento Criminal de 1882 a la que se le han ido haciendo reformas, cual herida a la que se le pone una tirita y porque cuando se ha puesto a legislar lo ha hecho tarde y no tan bien como se esperaba.

En definitiva, hay que hacer gala de una herramienta muy valiosa como lo es el Derecho comparado y si otros Estados están haciendo algo bien en esta materia, seguir el mismo camino que ellos para paliar la criminalidad informática.

Tras la lectura de múltiples artículos de diversos autores, se saca en claro que, si de verdad se quiere luchar contra la criminalidad informática, no es suficiente con que cada Estado promueva independientemente un desarrollo normativo interno de medios, de personal, etc., sino que se deben aunar fuerzas y pasar por la cooperación internacional. No en vano los delitos informáticos se caracterizan por su carácter transnacional, que es uno de los elementos que más dificultades crea en la práctica.

Ya que para luchar contra la criminalidad informática no nos sirve la justicia universal y tampoco la Corte Penal Internacional, no se trata de seguir buscando instituciones internacionales que resuelvan las controversias, sino de coordinar las nacionales que, al fin y al cabo, aunque con algunas peculiaridades, coinciden en los mínimos esenciales. A esto se le llama la compatibilidad y un buen ejemplo de lo expresado es el espacio judicial europeo.

Es cierto que no es fácil conseguir cooperación internacional cuando hablamos de Estados que primero miran por sus propios intereses, pero también lo es que desde hace algunos años parece que los Estados han comenzado a concienciarse respecto a que no pueden luchar solos contra la ciberdelincuencia. Aunque el progreso es lento, debido a que es difícil coordinar a tantos Estados, hay que terminar con un aliento de esperanza porque cuando se quiere, se puede.

Referencias

"Cuestiones prácticas y procesales relacionadas con la investigación de los delitos informáticos". http://190.104.117.163/2014/septiembre/prueba/contenido/ponencias/Anexos/Legislacion/Cuestiones%20practicas%20y%20procesales%20investigacion%20delitos%20informaticos.pdf (acceso marzo 8, 2017).

"Jorge Bemúdez - LECr* elviervice Pack 2 [Rooted CON 2015 - ESP]". Video de YouTube. 1:28:02. Publicado por "Rooted CON". 10 de junio de 2015. https://www.youtube.com/watch?v=-PfcUXCwjOM

Álvarez-Cienfuegos Suárez, José María. "Aspectos procesales en relación con la investigación de delitos informáticos". *Revista Catalana de Seguretat Pública*, núm. 3 (1998): 27-44.

Audiencia Nacional, Sala de lo Penal. *Sentencia 14/2001, de 10 de marzo*. M. P. Rosa María Arteaga Cerrada.

Benítez Ortuzar, Ignacio. "Informática y delito. Aspectos penales relacionados con las nuevas tecnologías" en *Reforma del Código Penal. Respuestas para una sociedad del siglo XXI*, compilado por Lorenzo Morillas Cueva, María José Cruz Blanca y Gonzalo Quintero Olivares, 111-136. Madrid: Dykinson, 2009.

Bernárdez Cabello, Olaf e Ignacio Ramos-Paúl de la Lastra. "Retos de la tutela judicial efectiva frente a las ciberamenazas" en *Retos del Derecho ante las nuevas amenazas*, coordinado por María Susana de Tomás Morales, 111-123. Madrid: Dykinson, 2015.

Chinchilla, Antonia. "Ciberdelincuencia: ojo al dato". http://diario-informacion.vlex.es/vid/ciberdelincuencia-ojo-dato-523529010 (acceso marzo 8, 2017).

Consejo de Europa. *Convenio sobre la Ciberdelincuencia*, Budapest, 23 de noviembre de 2001.

De la Cuesta Arzamendi, José Luis y Norberto J. de la Mata, coords. *Derecho Penal Informático.* Madrid: Civitas, 2010.

Díaz Gómez, Andrés. "El delito informático, su problemática y la cooperación internacional como paradigma de su solución: El Convenio de Budapest". *Redur* 8 (2010): 169-203.

El País. "Golpe policial a la 'Deep Web". http://el-pais.vlex.es/vid/golpe-policial-deep-web-543508626 (acceso marzo 8, 2017).

España. *Constitución Española de 1978*. Madrid: *Boletín Oficial del Estado* No. 311, 29 de diciembre de 1978.

Esparza Leibar, Iñaki. "El proceso debido como único modelo aceptable para la resolución de conflictos en un estado de derecho y como presupuesto para la globalización" en *El Derecho Procesal español del siglo XX a golpe de tango: Liber Amicorum, en homenaje y para celebrar su LXX cumpleaños*, coordinado por Juan-Luis Gómez Colomer, Silvia Barona Vilar, Pía Calderón Cuadrado, 319-338. Valencia: Tirant lo Blanch, 2012.

Fiscalía General del Estado. *Instrucción 2/2011*, "Sobre el Fiscal de Sala de Criminalidad Informática y las Secciones de Criminalidad Informática de las Fiscalías". Madrid: Fiscal.es, 11 de octubre de 2011.

Gobierno de España, Presidencia del Gobierno. *Estrategia de Ciberseguridad Nacional*. Madrid: Autor, 2013.

González Hurtado, Jorge Alexandre. "Delincuencia informática: daños informáticos del artículo 264 del Código Penal y propuesta de reforma". Tesis doctoral, Universidad Complutense de Madrid, Departamento de Derecho Penal, 2013.

González Jiménez, Albert. "Las diligencias policiales y su valor probatorio". Tesis doctoral, Universidad Rovira i Virgili, Departamento de Derecho Privado, Procesal y Financiero, 2014.

Hernández Díaz, Leyre. "El delito informático". *Eguzkilore*, núm. 23 (2009): 227-243.

Jefatura del Estado. *Ley 1/2000*, "De enjuiciamiento civil". Madrid: *Boletín Oficial del Estado* No. 7, 8 de enero de 2000.

Jefatura del Estado. *Ley Orgánica 13/2015*, "De modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica". Madrid: *Boletín Oficial del Estado* No. 239, 6 de octubre de 2015.

López-Barberá, Arantzazu. "Deep web' o Internet profundo". *Seguritecnia: Revista Decana Independiente de Seguridad*, núm. 407 (2014): 96-97.

Lorca Navarrete, Antonio María. "El derecho procesal como sistema de garantías". *Boletín Mexicano de Derecho Comparado* XXXVI, núm. 107 (2003): 531-557.

Ministerio de Gracia y Justicia. *Real Decreto de 14 de septiembre de 1882*, "Por el que se aprueba la Ley de Enjuiciamiento Criminal". Madrid: *Boletín Oficial del Estado* No. 260, 17 de septiembre de 1882.

Morón Lerma, Esther y María José Rodríguez Puerta. "Traducción y breve comentario del Convenio sobre Cibercriminalidad". *Revista de Derecho y proceso penal*, núm. 7 (2002): 167-200.

National Institute of Justice. *Forensic Examination of Digital Evidence: A Guide for Law Enforcement.* Washington: Autor, 2004.

Rayón Ballesteros, María Concepción y José Antonio Gómez Hernández. "Cibercrimen: particularidades en su investigación y enjuiciamiento". *Anuario Jurídico y Económico Escurialense*, núm. 47 (2014): 209-234.

Rodríguez Bernal, Antonio Pedro. "Los cibercrímenes en el espacio de libertad, seguridad y justicia". *Revista de Derecho Informático*, núm. 103 (2007): 1-42.

Rubio Alamillo, Javier. "Clonación de discos duros en el peritaje informático". http://peritoinformaticocolegiado.es/clonacion-de-discos-duros-en-el-peritaje-informatico (acceso marzo 8, 2017).

Rubio Alamillo, Javier. "La informática en la reforma de la Ley de Enjuiciamiento Criminal". *Diario La Ley*, núm. 8662 (2015): 1-9.

Ruiloba Castilla, Juan Carlos. "La actuación policial frente a los déficits de seguridad de Internet". *Revista de Internet, Derecho y Política*, núm. 2 (2006): 52-62.

Salvadori, Iván. "Los nuevos delitos informáticos introducidos en el Código Penal español con la Ley Orgánica 5/2010: perspectiva de Derecho comparado". *Anuario de Derecho Penal y Ciencias Penales* 64, núm. 1 (2011): 221-252.

San Juan, César, Laura Vozmediano y Ana Vergara. "Miedo al delito en contextos digitales: un estudio con población urbana". *Eguzkilore*, núm. 23 (2009): 175-190.

Tribunal Constitucional, Sala Segunda. *Sentencia 237/2005, de 26 de septiembre*. M. P. Guillermo Jiménez Sánchez.

Tribunal Constitucional, Sala Segunda. *Sentencia 48/1984, de 4 de abril*. M. P. Luis Díez-Picazo y Ponce de León.

Tribunal Supremo, Sala de lo Penal. *Auto de 4 de marzo de 2009*. M. P. José Ramón Soriano Soriano.

Tribunal Supremo, Sala de lo Penal. Sentencia 1066/2009, de 4 de noviembre. M. P. José Antonio Martín Pallín.

Tribunal Supremo, Sala General. *Acuerdo no jurisdiccional de 3 de febrero de 2005*.

Velasco Núñez, Eloy. *Delitos cometidos a través de Internet: cuestiones procesales.* Madrid: La Ley, 2010.