Grado en Derecho por la Universidad del País Vasco/ Euskal Herriko Unibertsitatea

Año académico 2015/2016

# LA ODISEA PROCESAL DE LA CRIMINALIDAD INFORMÁTICA

*"Los avances en la construcción naval trajeron los piratas, las armas de bolsillo trajeron los atracadores y la revolución informática ha traído al ciberdelincuente".*

Salvador Garriga

Trabajo realizado por Lorena AROCENA ALONSO

Dirigido por Iñaki ESPARZA LEIBAR

# ÍNDICE

## I. INTRODUCCIÓN

1. Justificación del tema

La sociedad avanza y evoluciona, y junto a ella, ha de hacerlo el Derecho. Ésta es la premisa con la que hemos de partir a la hora de abordar los delitos informáticos; una realidad candente fruto de las nuevas tecnologías. Es por ello que partiendo 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[1]. Lo que termina traduciéndose en tipos penales abiertos e indeterminación.

La delincuencia también se nutre de los cambios sociales, en consecuencia, las nuevas tecnologías además de brindarnos múltiples facilidades e información, 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 que se vean afectados los bienes jurídicos tradicionales pero mediante un elemento en particular; la aplicación de las nuevas tecnologías[2].

Tal es la relevancia de los delitos informáticos que es la tercera potencia delictiva llegando a afectar a más de 500 millones de personas. El desconocimiento y la inconsciencia con las que se utilizan las nuevas herramientas, da 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 número de teléfono o correo haciendo un flaco favor a nuestra persona, que a saber las consecuencias según en manos de quien caiga*"[3].

---

[1] Álvarez-Cienfuegos Suárez, J. M. (1998). Aspectos procesales en relación con la investigación de delitos informáticos. *Revista Catalana de Seguretat Pública,* (3), p. 27.

[2] Benítez Ortuzar, I. F. (2009). Informática y delito. Aspectos penales relacionados con las nuevas tecnologías. En L. Morillas Cueva, M. J. Cruz Blanca, & G. Quintero Olivares, *Reforma del Código Penal. Respuestas para una sociedad del siglo XXI* (p. 112). Dykinson.

[3] Chinchilla, A. (s.f.). *vLex España.* Recuperado el 25 de enero de 2016, de http://diario-informacion.vlex.es/vid/ciberdelincuencia-ojo-dato-523529010. Sin embargo, San Juan, C., Vozmediano, L., & Vergara, A. (2009). Miedo al delito en contexto digitales: Un estudio con población urbana. Eguzkilore: Cuadernos del Instituto Vasco de Criminología (23), p. 178, 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.

En este sentido, 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[4]. Estos rasgos indican la necesidad de una cooperación a nivel policial y judicial si se pretende conseguir que los delitos informáticos no queden impunes. Como resultado de esta colaboración internacional tenemos el Convenio sobre Ciberdelincuencia del Consejo de Europa de 23 de noviembre de 2001; un primer paso en esta área, pero no definitivo[5].

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[6]. El resultado es que los delitos informáticos se catalogan dentro del "Derecho informático", siendo éste el conjunto de normas que regulan todas las relaciones que tengan que ver con la informática[7].

El desconocimiento ha sido la causa de tantos años de impunidad y de desorientación. Pero no hay que olvidar que Internet es mucho más grande que lo que un simple usuario puede llegar a pensar, pues la parte que ve no es más que "la punta del iceberg". En este sentido, hay que hablar de la Deep Web (también conocida como Internet profundo o Hidden Web, entre otros), el lugar a donde los motores de búsqueda como Google o Yahoo no pueden llegar y donde precisamente se almacena el 80 por 100 del contenido real de Internet. Y por supuesto, es el medio que utilizan muchos ciberdelincuentes para evitar dejar rastro y que su persecución sea más dificultosa si se carecen de los medios y los conocimientos adecuados[8]. Dada la complejidad que

---

[4] Velasco Núñez, E. (2010). *Delitos cometidos a través de Internet: cuestiones procesales.* Madrid: La Ley. p 47.

[5] Benítez Ortuzar, I. F. (2009). Informática y… ob. cit. pp. 112-114.

[6] Rayón Ballesteros, M. C., & Gómez Hernández, J. A. (2014). Cibercrimen: particularidades en su investigación y enjuiciamiento. Anuario Jurídico y Económico Escurialense, (47), p.211.

[7] Hernández Díaz, L. (2009). El delito informático. Eguzkilore: Cuaderno del Instituto Vasco de Criminología (23), pp. 227-228.

[8] López-Barberá Martín, A. (2014). `Deep Web´ o Internet profundo. *SEGURITECNIA: Revista Decana Independiente de Seguridad* (407), pp. 96-97. 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. Ver El País. (25 de enero de 2016). vLex España. Obtenido de http://el-pais.vlex.es/vid/golpe-policial-deep-web-543508626.

supondría llevar a cabo también el análisis de los aspectos procesales de los delitos informáticos cometidos en la Deep Web, habré de centrarme 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 del Internet superficial, no nos deja en un buen lugar si la meta es conseguir que no haya impunidad, ni siquiera en la Deep Web.

## 2. Objetivos

El objetivo general del trabajo consiste en reseñar la importancia actual de la ciberdelincuencia en un mundo digital donde los *smartphones*, los ordenadores, la transferencia de archivos, etc. están a la orden del día. Así pues, se pretende poner de relieve la singularidad de los delitos informáticos que requieren un tratamiento procesal específico en comparación con los delitos convencionales, no sólo por las diligencias particulares de investigación tecnológica que requieren, sino también por el personal especializado que se necesita para que finalmente el proceso no fracase y puedan perseguirse de forma satisfactoria.

Como objetivos específicos se han considerado los siguientes:

- Encomiar la actualización de la Ley de Enjuiciamiento Criminal y a la vez, resaltar la peligrosidad de haber abordado un proyecto de esta complejidad sin un asesoramiento del todo `óptimo´, poniendo en peligro derechos de los ciudadanos y creando problemas que antes eran inexistentes.

- Abordar la necesidad de un personal especializado en la Administración de Justicia, teniendo en consideración que para el ejercicio de la mayoría de las nuevas diligencias de investigación tecnológicas aportadas por la nueva Ley Orgánica, se requiere resolución judicial motivada.

- Aclarar que la única vía para progresar en esta materia y conseguir resultados realmente satisfactorios pasa por una imperativa y real cooperación internacional entre los Estados.

## II. CUESTIONES PROCESALES DE LOS DELITOS INFORMÁTICOS

1. Conceptos y clasificación

En la medida en que han ido evolucionando las TICS (Tecnologías de la información y comunicación), el concepto de delito informático también ha ido desarrollándose progresivamente. En este sentido, en un principio se limitaba al ámbito patrimonial por lo que las definiciones hacían referencia a obtener un `beneficio´. Con las siguientes definiciones comenzaron a vislumbrarse algunas de las características actuales de los delitos informáticos y se comprendió, que el ordenador podía ser también el objeto del delito y no una mera herramienta.

Teniendo en consideración que las conductas que podían considerarse como delitos informáticos fueron aumentando con el paso del tiempo, en 1983 la OCDE[9] reunió un Comité de Expertos que dio la siguiente definición de delito informático: "*cualquier comportamiento, no ético o no autorizado relacionado con el procesado automático de datos y/o transmisiones de datos*"[10].

Sin embargo, otros autores como ROMEO CASABONA o GUTIÉRREZ FRANCÉS, se alejaron del término "delito" y preferían hablar de "delincuencia informática", ya que consideraban que conductas que podían clasificarse dentro del delito informático, no estaban tipificados como tal penalmente. En definitiva, no hablaban de un único delito, sino de una pluralidad con diferentes características en cada caso, donde el nexo resultaba ser la vinculación con los ordenadores y donde ni siquiera llegaba a verse afectado siempre el mismo bien jurídico[11].

En consecuencia, por los motivos expuestos, actualmente la doctrina mayoritaria prefiere recurrir a hablar de "Delincuencia informática", "Criminalidad informática" o, en plural, "Delitos informáticos". Por lo que a lo largo de todo el trabajo utilizaré estas denominaciones de forma indistinta.

Por tanto, dada la dificultad para encontrar una definición satisfactoria, podríamos quedarnos por un lado con la realizada por ACURIO DEL PINO al decir que "*delincuencia informática es todo acto o conducta ilícita e ilegal que pueda ser considerada como criminal, dirigida a alterar, socavar, destruir, o manipular, cualquier*

[9] Las siglas de Organización para la Cooperación y Desarrollo Económicos (OCDE). Aquí se puede consultar la página web oficial: http://www.oecd.org/centrodemexico/laocde/

[10] Recomendación número R(81) 12 del Consejo de Europa.

[11] Para más información ver Hernández Díaz, L. (2009). El delito... ob. cit. pp. 230-234.

*sistema informático o alguna de sus partes componentes, que tenga como finalidad causar una lesión o poner en peligro un bien jurídico cualquiera*"[12].

Por otro lado, también podemos valernos de una definición un poco diferente acuñada por VELASCO NUÑEZ al indicar que se incluyen dentro de los mismos "*tanto el delito tradicional cometido a través de ordenador o Internet (v. gr., injurias a través de correo electrónico, venta de droga, extorsión o amenazas vehiculizadas a través de Internet), como el propiamente tal, delito contra la informática –por atacar los datos o sistemas informáticos o las vías telemáticas de comunicación, especialmente a través de Internet-, ya sea bloqueando sistemas, destruyendo programas, dañando dispositivos de almacenamiento, alterando datos (fraude), destruyéndolos (sabotaje) o usándolos ilícitamente (piratería, espionaje)*"[13].

Una vez hemos definido en qué consisten los delitos informáticos, hay que remarcar que dentro de los mismos cabe distinguir diferentes tipos. Una posible clasificación simple y genérica es la que se ramifica en dos categorías. En la primera de ellas el bien jurídico que queda afectado es la confidencialidad, la integridad o disponibilidad del sistema, etc. ya que el ordenador o el sistema informático viene a ser el objetivo del ataque. En la segunda, el ordenador no es más que una mera herramienta o instrumento para cometer delitos tradicionales como el robo o la falsificación[14].

Basándonos, sin embargo, en el Código Penal español, la clasificación es tripartita y hablaríamos de ciberdelincuencia económica, ciberdelincuencia intrusiva y finalmente, ciberespionaje y ciberterrorismo. Porcentualmente los más importantes serían los primeros que implican un 70 por 100 de los delitos informáticos, en los cuales se ataca el patrimonio ajeno mediante la informática. El segundo grupo se corresponde con los ataques informáticos a la intimidad y a la privacidad, entendiéndose el artículo 18 de la Constitución Española en toda su extensión. Aunque en menor medida, este tipo de ciberdelito constituye el 25 por 100 y ejemplos del mismo serían la pornografía infantil, las injurias y calumnias informáticas, etc. En tercer y último lugar, aunque numéricamente sean los menos significativos, son los más importantes en cuanto a sus consecuencias ya que lo que se ataca son intereses supraindividuales con los que se

[12]Acurio del Pino, S. (2011). Delitos informáticos: Generalidades. Obtenido de http://www. oas. org/juridico/spanish/cyb_ecu_delitos_inform. Pdf.

[13] Velasco Núñez, E. (2010). Delitos cometidos… ob. cit. p. 41.

[14] Consultar Rodríguez Bernal, A. P. (2007). Los cibercrímenes en el espacio de libertad, seguridad y justicia. *Revista de derecho informático* (103), p.9.

pretende alterar el sistema político. Ejemplo de ellos sería el delito de revelación de secretos relativos a la defensa nacional[15].

Por otro lado, dada la confusión conceptual que pueda llegar a darse a causa de la terminología propia de la criminalidad informática y la dificultad que entraña la misma, es imperativo perfilar también otra serie de conceptos que nos guíen en esta materia.

Cuando se habla de delitos informáticos indirectamente se tiende a pensar en los hackers; aquellas personas con avanzados conocimientos técnicos en la materia. Sin embargo, esto no es del todo correcto. El origen de los mismos se remonta al año 1959; pero lejos de ser personas sin escrúpulos que buscan hacer el mal, motivados por retos intelectuales disponen de un código de conducta para todo aquel que forme parte del colectivo. Así pues, entre sus normas encontramos no hacer daño intencionadamente, no poder *hackear* por razones personales de cualquier índole o la obligación de no modificar nada más que lo estrictamente necesario para que no sean interceptados. Hay toda una filosofía de vida detrás de estas personas, pero ni de lejos puede llegar a llamárseles delincuentes cuando precisamente muchas veces alertan al administrador que ha sido *hackeado* de los fallos de seguridad que han encontrado, así como de la forma de solucionarlos[16]. Estos hackers a los que les gusta hacer el bien, son conocidos también como “hackers de sombrero blanco”.

La confusión se da con los “hackers de sombrero negro” o crackers. Este término es el utilizado realmente para aquellas personas que cometen delitos informáticos, ya que pretenden destruir o buscar algún tipo de beneficio con la actividad que llevan a cabo. Precisamente fueron los propios hackers los que en 1985 acuñaron esta denominación de cracker dado el mal uso que se estaba haciendo del término hacker[17].

Otra denominación a tener en cuenta es la de phreakers que son personas especializadas en los sistemas telefónicos. La filosofía que hay detrás de los phreakers no es estafar a las empresas de telefonía o grandes multinacionales, sino precisamente subsanar las estafas que consideran que llevan a cabo las compañías telefónicas. Por esta razón, lo que buscan es no pagar las facturas; como se puede apreciar se parecen más a los crackers que a los hackers dada la falta de la ética correspondiente a estos

[15] Para más información acudir a Velasco Núñez, E. (2010). *Delitos cometidos*… ob. cit. pp.42-44.

[16] Si se quiere profundizar más en el tema ir a De la Cuesta Arzamendi, J. L., De la Mata Barranco, N. J., Esparza Leibar, I., San Juan Guillén, C., Pérez Machío, A. I., Saiz Garitaonandia, A., . . . Hernández Díaz, L. (2010). Derecho penal informático. Aranzadi, SA, pp.103-105.

[17] *Ibídem*, pp.105-106.

últimos. Pero no hay que pasar por alto la potencial peligrosidad de los phreakers, pues pueden llegar a realizar escuchas telefónicas que sirvan de mecanismo para cometer un delito[18].

Finalmente, también podemos hablar de viruckers. Como su nombre nos invita a pensar, son aquellas personas que introducen virus en los sistemas informáticos con un fin pernicioso. Se acercan a las características de los crackers, aunque a los viruckers les gusta trabajar individualmente; lo que está claro es que pueden resultar un arma letal en el siglo XXI[19].

En nuestro ordenamiento jurídico rige el *nullum crime, nulla poena sine praevia lege*[20], lo que se traduce en una serie de garantías que han de ser respetadas y en consecuencia, toma un papel muy importante el uso concreto de los conceptos. En este sentido, hay que aclarar algunas otras cuestiones terminológicas ya que, por ejemplo, no es lo mismo un ordenador que un sistema informático, ni una red informática e Internet.

Partiendo de la definición que nos aporta la Real Academia Española sobre ordenador o computadora[21], se necesita de la combinación de un hardware y un software para hacer operativo el mismo. Dos conceptos estos últimos, que a simple vista no llegan a quedar del todo claros.

Se entiende por hardware *"las partes tangibles o físicas de un sistema informático; normalmente compuestas por sistemas eléctricos, electrónicos y mecánicos*"[22]. Por lo que los monitores, impresoras, etc. también se consideran parte

---

[18] Acudir a De la Cuesta Arzamendi, J. L., De la Mata Barranco, N. J., Esparza Leibar, I., San Juan Guillén, C., Pérez Machío, A. I., Saiz Garitaonandia, A., . . . Hernández Díaz, L. (2010). *Derecho…* ob. cit. pp.106-107.

[19] De la Cuesta Arzamendi, J. L., De la Mata Barranco, N. J., Esparza Leibar, I., San Juan Guillén, C., Pérez Machío, A. I., Saiz Garitaonandia, A., . . . Hernández Díaz, L. (2010). *Derecho…* ob. cit. pp.107-108.

[20] Ningún delito, ninguna pena sin ley previa. El autor de este principio de legalidad fue el abogado alemán Paul Johann Anselm Von Feuerbach. Para más información consultar Pérez Vaquero, C. (s.f.). El muchacho de ninguna parte. IN ALBIS, 30-31.

[21] "*Máquina electrónica que, mediante determinados programas, permite almacenar y tratar información, y resolver problemas de diversa índole*" (RAE). A efectos de consultar la definición acceder al siguiente link: http://dle.rae.es/?id=A4hIGQC

[22] González Hurtado, J. A. (2013). *Delincuencia informática: daños informáticos del artículo 264 del Código Penal y propuesta de reforma.* Tesis doctoral, Universidad Complutense de Madrid, Departamento de Derecho Penal, Madrid, p.32.

del hardware; la puntualización que cabe realizar, entonces, es que hay que diferenciar entre hardware básico –indispensable- y hardware complementario -prescindible-.

Por otro lado, software se ha de entender como "*el equipamiento lógico de un sistema informático y comprende el conjunto de los componentes lógicos necesarios para hacer posible la realización de tareas específicas para las que están diseñados los elementos físicos del sistema (hardware)*"[23]. Su conjunción con el hardware hace que el ordenador sea operativo, aunque luego existen múltiples tipos de software y cada uno atiende a finalidades diferentes.

Hemos señalado que un ordenador no es lo mismo que un sistema informático, por lo que ahora hay que dilucidar a qué nos referimos cuando hablamos de este segundo. Podemos referirnos indistintamente a sistemas de información o sistemas informáticos. Aunque existe alguna acepción estadounidense, partiremos de la definición que se da en el Convenio sobre la Ciberdelincuencia de Budapest, de 23 de junio de 2001, donde se entiende por sistema informático "*todo 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*."[24] En último lugar, cabe precisar que cuando hablamos de sistema de información no hemos de limitarnos meramente al ordenador. Es decir, el sistema de información hace referencia a toda conjunción de hardware-software, así como pueden serlo también un teléfono móvil o una videoconsola; así lo entiende, de hecho, el legislador español.

Por otro lado, no podemos equiparar las redes informáticas e Internet. Una definición acertada de redes informáticas es la que dice que "*suponen una serie de sistemas informáticos (por tanto, no sólo ordenadores) conectados entre sí por medio de dispositivos físicos que envían y reciben información a través de cualquier medio hábil para el transporte de datos, con la finalidad de compartir recursos y ofrecer*

[23] González Hurtado, J. A. (2013). *Delincuencia…* ob. cit. p. 33.

[24] Convenio del Consejo de Europa sobre la Ciberdelincuencia de Budapest, de 23 de junio de 2001. Pero la Decisión Marco 2005/222/JAI del Consejo, de 24 de febrero de 2005 relativa a los ataques contra los sistemas de información, también nos da una definición asequible y hasta más completa al indicar que un sistema informático es "*todo aparato o grupo de aparatos interconectados o relacionados entre sí, uno o varios de los cuales realizan, mediante un programa, el tratamiento automático de datos informáticos, así como los datos informáticos almacenados, tratados, recuperados o transmitidos por estos últimos para su funcionamiento, utilización, protección y mantenimiento*".

*servicios*"[25]. Sin embargo, Internet vendría a ser "*una red informática de extensión global que conecta sistemas informáticos en todas las partes del mundo*"[26].

En definitiva, lo que podemos sacar en claro es que la complejidad del mundo cibernético, aparte de dificultar la tarea de perseguir los delitos informáticos, también nos obstaculiza el fijar un perfil con una serie de características intrínsecas a los autores de los mismos dada la diversidad con la que nos encontramos, ya que podemos hallar tanto autores jóvenes como mayores, que tengan o bien motivaciones personales o bien patrimoniales.

## 2. Perspectiva histórica

### 2.1. La Constitución Española de 1978

Si acudimos a la Norma Normarum de nuestro ordenamiento jurídico encontraremos, como por otra parte es lógico, un único artículo que puede ponerse en relación con los delitos informáticos, aunque ni siquiera de forma específica. Lo destacable de este precepto es que se recoge la garantía del secreto de las comunicaciones en el 18.3[27] y la protección de datos en relación a la informática en el 18.4[28]. Teniendo presente en todo momento que la Constitución es de 1978 parece normal que sea de los primeros textos en recoger algo de esta índole, si tenemos en cuenta que es hacia esta época cuando empiezan a darse cuenta de la amenaza que puede suponer permitir el uso indiscriminado de datos informáticos.

Es más, el propio Tribunal Constitucional interpretó mediante su jurisprudencia que estamos ante un verdadero derecho independiente[29] del derecho a la intimidad y que ni siquiera requiere de desarrollo normativo[30] para que sea vinculante para los poderes públicos[31].

---

[25] Para más información consultar González Hurtado, J. A. (2013). *Delincuencia…* ob. cit. p.37.

[26] *Ibídem*, p.37.

[27] *Vid.* el artículo 18.3. "*Se garantiza el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial*". Constitución Española de 1978.

[28] Véase el artículo 18.4. "*La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos*". Constitución Española de 1978.

[29] STC 254/1993, de 20 de julio y 290/2000, de 30 de noviembre.

[30] STC 254/1993.

[31] Elvira Perales, A. (enero de 2011). Congreso de los Diputados. Recuperado el 8 de abril de 2016, de http://www.congreso.es/consti/constitucion/indice/sinopsis/sinopsis.jsp?art=18&tipo=2.

## 2.2. Una Ley de Enjuiciamiento Criminal de más de cien años

La Ley de Enjuiciamiento Criminal data de 1882 y, con sus más o menos parches de actualización, ha sido escasa para dar una respuesta satisfactoria a la persecución de los delitos informáticos durante todo este tiempo.

Esta legislación procesal del siglo XIX tuvo una primera actualización en la cual se hablaba de la posibilidad de intervenir las comunicaciones postales con autorización judicial. Evidentemente, esta insuficiente regulación resultaba pobre si con ella querían investigarse los delitos informáticos. Así pues, durante casi más de cien años es lo único que había –aunque tampoco era tan necesario como hoy en día- para perseguir la criminalidad informática, hasta que llegó la Constitución en 1978 y se garantizó en su artículo 18[32] el secreto de las comunicaciones salvo autorización judicial.

Consiguientemente, desde 1978 hasta 1988 lo único que había en el procedimiento penal para poder intervenir una comunicación telefónica y aportarla como prueba era lo recogido en nuestra Constitución. A consecuencia de ello, se sucedieron una serie de sentencias del Tribunal Europeo de Derechos Humanos[33] condenando a España por haber intervenido comunicaciones telefónicas sin tener siquiera una normativa que lo permitiese. El resultado de todo esto fue que al artículo 579 de la Ley de Enjuiciamiento Criminal –dedicado a la correspondencia postal y telegráfica-, se le

[32] *Vid.* el artículo 18.3. "*Se garantiza el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial*". Constitución Española de 1978. Ni siquiera se preveía la posibilidad de que hubiese autorización de los comunicantes para intervenir la comunicación, a diferencia de lo que sucede con el domicilio donde no es necesaria la autorización judicial si hay autorización del morador. Información obtenida de la Conferencia impartida por el Fiscal Jorge A. Bermúdez, Fiscal Delegado de Criminalidad Informática: LECr* Service Pack 2. Rooted CON 2015; un Congreso de Seguridad Informática que se celebra anualmente. Para acceder a la conferencia consultar el siguiente enlace: https://www.youtube.com/watch?v=-PfcUXCwjOM

[33] *Vid.* Sentencia Valenzuela Contreras C. España, 30.07.1998. El Tribunal Europeo de Derechos Humanos condenó a España por no tener una normativa que permitiese la intervención de las comunicaciones telefónicas aunque fuese con mandato judicial, garantizando así el principio de legalidad.

incluyó un segundo escueto párrafo[34] indicando que también se podrían intervenir las comunicaciones telefónicas con autorización judicial[35].

Durante décadas ésta ha sido la única regulación existente para intervenir comunicaciones. Todo se traducía en que ante la falta de más preceptos, se acudía al Tribunal Europeo de Derechos Humanos, por lo que el Tribunal Supremo fue estableciendo en sus sentencias un catálogo de medidas y de requisitos a seguir. Finalmente, el TEDH tuvo que darse por satisfecho y permitir que la regulación fuese jurisprudencialmente. Sin embargo, esto sólo nos sirve para las comunicaciones telefónicas, pero hoy en día existen todo tipo de comunicaciones, de transferencia de archivos, de comunicaciones internas por mensajerías instantáneas, etc.

En definitiva, desde que salieron a la luz todo este abanico de posibilidades urgía la modificación de la legislación procesal penal; reforma que parecía no llegar. Por lo que todo lo que se venía realizando eran aplicaciones analógicas y se trataba, por ejemplo, a los discos duros como cajones de documentos, porque era lo único previsto en la Ley de Enjuiciamiento Criminal, y las intervenciones de IPs[36] como intervenciones telefónicas. Finalmente, la salvación parecía llegar de mano del Anteproyecto de reforma de la Ley de Enjuiciamiento Criminal que abría muchas posibilidades de investigación, las cuales no son necesarias comentar ya que el Anteproyecto nunca llegó a buen puerto[37].

### 2.3. Un nuevo horizonte con la Ley Orgánica 13/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal

Por fin llegó la 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. Las principales novedades que trae esta Ley

---

[34] *Vid.* el artículo 579.2. "*Asimismo, el Juez podrá acordar, en resolución motivada, la intervención de las comunicaciones telefónicas del procesado, si hubiere indicios de obtener por estos medios el descubrimiento o la comprobación de algún hecho o circunstancia importante de la causa*". Real decreto de 14 de septiembre de 1882 por el que se aprueba la Ley de Enjuiciamiento Criminal.

[35] Para más información acudir a la conferencia del Fiscal Jorge A. Bermúdez: LECr* Service Pack 2. Rooted CON 2015. Véase el link en el pie de página núm. 32.

[36] La IP (Internet Protocol) se trata de un "*número identificativo singularizado e irrepetible necesario para poder acceder a Internet*". Velasco Núñez, E. (2010). Delitos cometidos… ob. cit. p.222.

[37] Conferencia del Fiscal Jorge A. Bermúdez: LECr* Service Pack 2. Rooted CON 2015. Véase el link en el pie de página núm. 32.

Orgánica son dos; por un lado actualiza el ordenamiento jurídico español a las exigencias del Derecho de la Unión Europea al fortalecer los derechos procesales y, por otro lado, se encarga de regular por primera vez de forma concreta las medidas de investigación tecnológicas.

Centrándonos en esta segunda aportación, el Título VIII de la Ley de Enjuiciamiento Criminal pasa a rubricarse "De las medidas de investigación de los derechos reconocidos en el artículo 18 de la Constitución" y a dividirse en diez capítulos. Las nuevas medidas de investigación realmente se recogen de los capítulos V al X[38], mientras que en los tres primeros se agrupan las que ya existían –aunque con ciertas especificidades- y el cuarto es simplemente una recopilación de disposiciones comunes; sin perjuicio de que también se modifican otros preceptos de otros Títulos de la Ley de Enjuiciamiento Criminal[39].

En este sentido, las medidas de investigación tecnológica que se incluyen tienen como premisa los principios de idoneidad, excepcionalidad, necesidad y proporcionalidad[40]; los cuales han de ser debidamente justificados y motivados mediante resolución judicial.

Alejándonos de las aplicaciones analógicas que nos obligaban a aplicar el artículo 579 LECrim en relación a las intervenciones de comunicaciones telefónicas para poder intervenir cualquier otro tipo de comunicación, ahora queda autorizada la intervención y el registro de las demás formas de comunicación mediante el ajustado mandato judicial.

---

[38] Ver Real decreto de 14 de septiembre de 1882 por el que se aprueba la Ley de Enjuiciamiento Criminal:
CAPÍTULO V: La interceptación de las comunicaciones telefónicas y telemáticas [arts. 588 ter a) a 588 ter m)].
CAPÍTULO VI: Captación y grabación de comunicaciones orales mediante la utilización de dispositivos electrónicos [arts. 588 quater a) a 588 quater e)].
CAPÍTULO VII: Utilización de dispositivos técnicos de captación de la imagen, de seguimiento y de localización [arts. 588 quinquies a) a 588 quinquies c)].
CAPÍTULO VIII: Registro de dispositivos de almacenamiento masivo de información [arts. 588 sexies a) a 588 sexies c)].
CAPÍTULO IX: Registros remotos sobre equipos informáticos [arts. 588 septies a) a 588 septies c)].
CAPÍTULO X: Medidas de aseguramiento (arts. 588 octies).

[39] Muerza Esparza, J. (2015). DOSSIER reforma de la Ley de Enjuiciamiento Criminal: La reforma procesal penal de 2015. Thomson Reuters, p.8.

[40] *Vid.* artículo 588 bis a. Principios rectores. Ley de Enjuiciamiento Criminal.

Asimismo, una de las grandes novedades es que se permite al agente encubierto informático intercambiar o enviar archivos ilícitos en el artículo 282 bis apartado sexto LECrim. Principalmente esto se prevé porque en la era digital donde lo habitual es el anonimato mediante el uso de *nicknames*, para poder entrar, por ejemplo, en foros de pederastas el agente encubierto ha de demostrar que forma parte del grupo enviando material elaborado por él mismo o que sea desconocido. En suma, las bases de datos de la policía resultan perfectas como cebo y el broche de oro es la frase a renglón seguido que dice "*y analizar los resultados de los algoritmos aplicados para la identificación de dichos archivos ilícitos*[41]". En palabras llanas, estos archivos enviados contienen una huella numérica *hash*[42] y mediante el programa informático adecuado, una vez detenido al sospechoso, se compara la función *hash* de los archivos encontrados en su posesión para así poder demostrar la relación[43].

La nueva Ley ha superado incluso las expectativas del Anteproyecto dado que en este último se iba a establecer un deber de colaboración de las operadoras de comunicaciones con las Administraciones Públicas; en concreto con el Poder Judicial. El problema radicaba en que no se iba a recoger ningún tipo de consecuencia penal ante la pasividad de las operadoras. En todo caso se les aplicaría una multa administrativa, lo cual a veces podría llegar a compensarles antes que aportar la información solicitada. Sin embargo, con la nueva redacción de la Ley de Enjuiciamiento Criminal se contempla este deber de colaboración en el artículo 588 ter e) y en su tercer apartado se establece que ante la pasividad de los prestadores de servicios de telecomunicaciones, estos pueden incurrir en un delito de desobediencia[44].

Así, las vías de investigación que se han abierto con esta nueva Ley son muy prometedoras tal y como se puede apreciar, aunque tampoco están exentas de problemas. Estos problemas serán abordados más adelante poniéndolos en relación con la tutela judicial efectiva.

---

[41] *Vid.* Artículo 282 bis apartado sexto, segundo párrafo de la Ley de Enjuiciamiento Criminal.

[42] Entiéndase por huella numérica hash una "*huella digital exclusiva única de cada fotografía*". Velasco Núñez, E. (2010). Delitos cometidos… ob. cit. p.201.

[43] Para más información es recomendable ver la Conferencia del Fiscal Jorge A. Bermúdez: LECr* Service Pack 2. Rooted CON 2015. Véase el link en el pie de página núm. 32. Asimismo, la información se ha obtenido también de una entrevista personal realizada con el mismo Fiscal en la cual se anotaron las cosas más relevantes e interesantes para este trabajo.

[44] *Ibídem*.

## III. JUSTIFICACIÓN DE UN TRATAMIENTO PROCESAL ESPECÍFICO

Las características propias de los delitos informáticos conllevan ciertas singularidades en su tratamiento procesal tal y como pone de relieve VELASCO NUÑEZ. 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 así evitar que desaparezcan pruebas, así como poder aplicar agravaciones genéricas[45] como agravaciones específicas[46]. No sólo esto, sino que de otra forma sería imposible apreciar el *modus operandi* del delincuente y además, teniendo en cuenta que los delitos informáticos suelen ser delitos con una pena inferior a cinco años, esta medida también evita que se pasen los plazos de prescripción que debido a la pena van a ser cortos[47].

Por otro lado, dadas las incógnitas que rodean a los delitos informáticos como, por ejemplo, la ocultación de la autoría mediante diferentes técnicas, el proceso para conseguir resultados es lento y se depende mucho de la prueba pericial técnica complementada con otras actuaciones intermedias como pantallazos, análisis de los archivos, etc. En definitiva, 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*[48]*"*.

1. Principios que orientan la persecución de los delitos informáticos

En relación a la competencia para perseguir los delitos informáticos, si acudimos al artículo 22[49] del Convenio sobre Cibercriminalidad se puede apreciar que 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

[45] Con agravaciones genéricas hemos de pensar sobre todo en la agravación por delito continuado del artículo 74 del Código Penal. Velasco Núñez, E. (2010). Delitos cometidos… ob. cit. p.49.

[46] Ejemplo de agravación específica en relación a los delitos informáticos es la recogida en el artículo 250.4 del Código Penal, ya que atendiendo a la especial gravedad de la estafa basándonos en el valor de su defraudación, ésta se considera estafa de especial gravedad. Velasco Núñez, E. (2010). Delitos cometidos… ob. cit. p.49.

[47] Velasco Núñez, E. (2010). Delitos cometidos… ob. cit. pp. 48-50.

[48] Todo ello en *Ibídem*, ob. cit. p.50.

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

territorialidad *stricto sensu*[50]. El resultado ha sido que los Estados han procurado ampliar el criterio seguido por el Convenio basándose en otros delitos, y dando así lugar a diferentes teorías o versiones sobre la competencia para enjuiciar los delitos informáticos.

### 1.1. Ubicuidad

En los delitos informáticos hay que partir de la premisa de que muchas veces quedan afectados diferentes países. Este resultado es producto de que en múltiples ocasiones el delincuente comete el hecho delictivo desde una parte del mundo y la consecuencia se da en otra parte totalmente diferente[51]. Esta situación ha planteado muchos debates sobre el foro y el juez competente, ya que la víctima en sí normalmente sólo suele saber que ha sido atacada; no sabe quién es el autor ni mucho menos desde dónde ha actuado éste.

Por si estos fueran pocos problemas, el autor en muchas ocasiones comete 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*[52]".

Cuando se abordó la cuestión de qué órgano jurisdiccional iba a ser el competente, basándose en otros delitos convencionales, una parte de la doctrina propuso la teoría de la acción. Es decir, según esta teoría el juez competente debía de ser aquel del lugar desde el cual se ha llevado a cabo el hecho delictivo. Estaríamos, por tanto, ante un concepto 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. En este sentido, 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[53].

---

[50] De la Cuesta Arzamendi, J. L., De la Mata Barranco, N. J., Esparza Leibar, I., San Juan Guillén, C., Pérez Machío, A. I., Saiz Garitaonandia, A., . . . Hernández Díaz, L. (2010). Derecho penal… ob. cit. pp. 247-248.

[51] Para más información acudir a Velasco Núñez, E. (2010). Delitos cometidos… ob. cit. p.55.

[52] Velasco Núñez, E. (2010). Delitos cometidos… ob. cit. p.56.

[53] De la Cuesta Arzamendi, J. L., De la Mata Barranco, N. J., Esparza Leibar, I., San Juan Guillén, C., Pérez Machío, A. I., Saiz Garitaonandia, A., . . . Hernández Díaz, L. (2010). Derecho penal… ob. cit. pp. 249-250.

Sin embargo, en Derecho el consenso no es tan fácil y, por tanto, otra parte de la doctrina abogaba porque el juez competente fuese aquel del lugar donde se hubieran producido los resultados, alegando que hasta entonces no se genera ningún tipo de perjuicio. En este caso el "resultado" se ha de entender como afección del bien jurídico protegido. Esto se traduce en que cualquier Estado pueda manifestar que son competentes los Juzgados de su jurisdicción por el simple hecho de fundamentar que se ha producido un "peligro abstracto" de un bien jurídico que es susceptible de protección en su ordenamiento jurídico[54].

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[55] tomó carta en ella. Así pues, el Tribunal Supremo 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 lugar de resultado[56].

En definitiva, 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 haya manifestado alguna parte del hecho criminal. Dicho de otra forma, serían competentes los Juzgados y Tribunales españoles tanto si el hecho delictivo se comete desde el territorio nacional, como si se lleva a cabo desde fuera pero tiene sus consecuencias o resultados en el territorio. Basta con que algún elemento pueda relacionarse con la circunscripción española para que el territorio nacional pueda ser competente[57]. Decisión del Tribunal Supremo de abogar por el principio de ubicuidad, la cual comparto completamente ya que es la mejor alternativa para evitar que haya delitos informáticos que queden impunes.

Esta regla no es más que una pauta inicial acorde con el artículo 15 LECrim, pues si en el transcurso de la investigación se averiguase el lugar concreto desde el que

---

[54] De la Cuesta Arzamendi, J. L., De la Mata Barranco, N. J., Esparza Leibar, I., San Juan Guillén, C., Pérez Machío, A. I., Saiz Garitaonandia, A., . . . Hernández Díaz, L. (2010). Derecho penal… ob. cit. p. 250.

[55] Ver el Acuerdo no jurisdiccional del pleno de la Sala Segunda del Tribunal Supremo de 3 de febrero de 2005. "*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*".

[56] Velasco Núñez, E. (2010). Delitos cometidos… ob. cit. p.56.

[57] De la Cuesta Arzamendi, J. L., De la Mata Barranco, N. J., Esparza Leibar, I., San Juan Guillén, C., Pérez Machío, A. I., Saiz Garitaonandia, A., . . . Hernández Díaz, L. (2010). Derecho penal… ob. cit. pp. 250-252.

se ha cometido el hecho delictivo, entonces cabe de acuerdo con el mismo artículo la inhibición a favor del competente según las reglas del artículo 14 LECrim.

Sin embargo, es necesario hacer una serie de precisiones respecto de la distribución competencial de los procesos de pornografía infantil. En este sentido, 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[58] respalda la idea de que se tramiten tantas causas como imputados, salvo que pueda demostrarse fehacientemente estar ante un supuesto de codelincuencia[59].

En definitiva, ya se opte por la acción, por el resultado o por ambas, las tres vías tienen sus ventajas y desventajas. Así pues, esto muestra la complejidad y dificultad que radica en 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.

### 1.2. 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 afectan a bienes jurídicos concretos que necesitan de una persecución reforzada a consecuencia de su propia naturaleza. Precisamente por justicia universal se entiende la ampliación de excepciones respecto de la aplicación de la territorialidad de la ley penal[60].

La única forma de que entre en juego el principio de universalidad en relación con los delitos informáticos es vinculándolos con los recogidos en el precepto citado. Por ejemplo, el sabotaje informático si se asocia con el terrorismo podría llegar a ser de persecución universal.

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 están afectando a un bien jurídico

[58] ATS 4/03/2009.

[59] En estos términos lo manifiesta Velasco Núñez, E. (2010). Delitos cometidos… ob. cit. pp.56-57.

[60] De la Cuesta Arzamendi, J. L., De la Mata Barranco, N. J., Esparza Leibar, I., San Juan Guillén, C., Pérez Machío, A. I., Saiz Garitaonandia, A., . . . Hernández Díaz, L. (2010). Derecho penal… ob. cit. p. 248.

que es de protección supranacional y en consecuencia, se les debería aplicar también la nota de universalidad[61].

Al igual que con la teoría de la ubicuidad, la pornografía infantil merece una serie de especificaciones. En este sentido, este delito informático es de persecución universal por una doble vía dentro del ordenamiento jurídico español. La primera de las vías 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 en referencia al tráfico de material pornográfico infantil independientemente de que su origen sea extranjero o desconocido. Si la procedencia del material fuese desconocida, sobre la base del artículo 65.1 e) LOPJ deberían ser competentes los Juzgados Centrales de Instrucción de la Audiencia Nacional. Sin embargo, en estas situaciones –que es la mayoría de las veces-, se prefiere la aplicación del principio de ubicuidad y que conozca la causa aquel juez que lo haya conocida primero en el tiempo[62].

### 1.3. Cosa juzgada y non bis in ídem

Reiterando el carácter transnacional de los delitos informáticos, a la hora de dilucidar la competencia también se han de tener en cuenta una serie de reglas de Derecho Procesal Penal Internacional. De este modo, hay que tener siempre muy presente, en aras del principio del juez predeterminado por la ley y del derecho a un juicio justo con todas sus garantías, 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[63] respecto a hechos delictivos que no se están enjuiciando en ningún otro Estado para evitar que se pierdan pruebas. En el caso de que finalmente los juzgados españoles no sean los competentes, se procede a la acumulación a favor del Estado que mejor foro tiene.

El proceso penal tiene dos fases: la de investigación y la del juicio oral. Así pues, lo explicado únicamente puede predicarse respecto a la fase de investigación. Sin que pueda ser de otra forma, en el juicio oral hay que favorecer el mayor número de

[61] Para más información acudir a Velasco Núñez, E. (2010). Delitos cometidos… ob. cit. p.58.

[62] Todo ello en Velasco Núñez, E. (2010). Delitos cometidos… ob. cit. pp.58-59.

[63] SAN 10/03/2001 y STC 26/09/2005.

garantías posible y eso sólo 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[64] que hacen la función de intermediarios entre los jueces para una eficaz coordinación.

Finalmente, la competencia se suele atribuir 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 una serie de elementos[65] para estimar su idoneidad.

Podría darse el caso también de que al hecho delictivo se le aplicase 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 respetando el principio de *non bis in ídem* para evitar que haya dobles enjuiciamientos[66].

2. Personal especializado

Internet, desde su creación, 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 comprender

[64] *v. gr.,* Eurojust para la Unión Europea. Para más información es aconsejable consultar su página web oficial que podemos encontrarla en el siguiente link: http://www.eurojust.europa.eu/Pages/home.aspx.

[65] En este sentido Velasco Núñez, E. (2010). Delitos cometidos… ob. cit. pp.61-62 indica que 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*".

[66] Todo ello obtenido en Velasco Núñez, E. (2010). Delitos cometidos… ob. cit. pp.59-63.

los problemas que entraña la tecnología y, para colmo, 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 quedarse obsoletos en poco tiempo[67].

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

No podemos dejar pasar por alto que para el rastreo de los delitos informáticos se necesitan ciertos conocimientos técnicos a lo largo de toda la cadena de personal implicado en el asunto; refiriéndome, por tanto, desde la policía hasta el juez. Tal es así que tanto el Cuerpo Nacional de Policía como la Guardia Civil se han visto en la necesidad de poner en marcha secciones especializadas para investigar los delitos informáticos, así como llevar a cabo una territorialización de esta especialización al igual que ha sucedido con la Fiscalía[68].

### 2.1. En el ámbito policial

Los delitos informáticos, tal y como se ha dejado claro en más de una ocasión, tienen la dificultad añadida de que resulta difícil saber de dónde proviene el hecho delictivo ya que los autores suelen ocultar su rastro, así como el hecho de que muchas veces el *quid* de la cuestión es encontrar al organizador del mismo que, en la mayoría de las ocasiones, no es el que lleva a cabo la transgresión directamente. Así pues, resolver estas cuestiones requiere que las Fuerzas y Cuerpos de Seguridad de los Estados actúen en consonancia, recurriendo a instrumentos adecuados para la persecución de los delitos informáticos y utilizando personal especializado dada la complejidad que entrañan[69].

Dentro del proceso para perseguir efectivamente los delitos informáticos, el primer eslabón de la cadena resulta ser la policía, que es la encargada de investigar mediante las adecuadas diligencias de investigación. Por eso, es importante que este

[67] Esta cuestión es abordada por Rodríguez Bernal, A. P. (2007). Los cibercrímenes… ob. cit. p.8.

[68] Para más información acudir a Velasco Núñez, E. (2010). Delitos cometidos… ob. cit. pp.69-70.

[69] González Hurtado, J. A. (2013). *Delincuencia*… ob. cit. p.268.

primer obstáculo sea superado con éxito, pues de otra forma el proceso fracasará y ni siquiera podremos entrar en el juicio oral.

El éxito en este primer punto únicamente puede ser alcanzado mediante la ciberinteligencia policial, ya que el Tribunal Europeo de Derechos Humanos ya ha advertido a España en más de una ocasión sobre su escasa regulación respecto a estos temas[70]. En este sentido, el triunfo policial se obtiene a través de la cooperación interpolicial, puesto que los problemas más habituales se plantean en los foros, congresos, etc. que se celebran y sobre la base de estos se elaboran acuerdos de cooperación. Es indispensable para conseguir una lucha efectiva contra la cibercriminalidad conocer el medio mejor que los propios autores[71]. Así pues, aunque el criminal intente camuflar su identidad, resulta difícil que no queden rastros ya sea por una razón u otra y, es ahí donde la policía tiene que entrar en escena para aprovecharse de los puntos flacos de Internet.

Respecto a la actuación policial nos encontramos con grandes avances tanto a nivel europeo, como a nivel nacional. De entrada, hay que destacar la creación del Centro Europeo de la Ciberdelincuencia, así como la Escuela Europea de Policía que conjuntamente nos brindan un marco óptimo para la formación de la policía y el inicio de la investigación promoviendo la cooperación interpolicial. A nivel nacional, refiriéndome a España en concreto, también cabe subrayar el papel fundamental que juega la policía judicial que principalmente está integrada por la Guardia Civil y el Cuerpo Nacional de Policía.

#### 2.1.1. Marco europeo

La lucha contra la ciberdelincuencia no es una cuestión que pueda abordar de forma independiente cada Estado. La colaboración en esta materia pasa a jugar un papel relevante, por no decir esencial. Por tanto, para esta lucha deben existir también los medios adecuados tanto a nivel europeo como a nivel internacional, aunque aquí sólo nos centraremos en la Unión Europea por ser un marco ejemplar de colaboración entre Estados, a pesar de que todavía haya que esforzarse y aplicarse mucho más. En este sentido y tal y como se ha indicado, hay que destacar una serie de organismos que están contribuyendo al buen hacer del personal policial; personal cuya labor no hay que

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

[71] Ruiloba Castilla, J. C. (2006). La actuación policial frente a los déficits de seguridad de Internet. *Revista de Internet, Derecho y Política*, (2), pp.56 y 61.

dejar en el olvido teniendo en consideración que si éstos hacen su trabajo mal el resto será inservible, pues aunque se encuentre al autor del hecho delictivo, para desvirtuar la presunción de inocencia se requieren pruebas de cargo.

#### 2.1.1.1. Centro Europeo de la Ciberdelincuencia

En este ámbito de la delincuencia informática se pueden apreciar disparidades entre los diferentes Estados, ya que mientras algunos van avanzados en materia de prevención y aplicación de la ley, a otros todavía les queda un largo camino por recorrer por no haberse adaptado todavía efectivamente a las nuevas tecnologías[72]. Así pues, partiendo del copioso número de delitos informáticos que tienen lugar actualmente en la Unión Europea, se puso en marcha el Centro Europeo contra la Ciberdelincuencia (EC3) en la sede holandesa de Europol. La finalidad de este organismo es facilitar la coordinación de la policía nacional de los Estados Miembros. Primordialmente, sus tareas van enfocadas a perseguir las bandas de delincuencia organizada mediante medios tecnológicos de última generación[73].

De acuerdo con un comunicado de prensa de la propia Comisión Europea[74], el EC3 es un gran paso en la capacidad de la Unión Europea para luchar contra la criminalidad informática. Los delincuentes informáticos se adaptan rápidamente a la tecnología según ésta va avanzando y, es por ello que era necesario un organismo que colaborase en su lucha, así como en su prevención. La gran ventaja del EC3 es que en éste se fusiona toda la información; asimismo hay que destacar su capacidad para movilizar los recursos de los que disponen los Estados[75].

En definitiva, todo ello muestra que el camino en la lucha contra la ciberdelincuencia pasa por el intercambio de información y coordinación de esfuerzos policiales. En este sentido, el EC3 ocupa el lugar de centro neurálgico de esta cooperación.

---

[72] Malmström, C. (s.f.). Una respuesta europea a la ciberdelincuencia. *Tribuna Libre*. Recuperado el 29 de abril de 2016, de http://opinion-murcia.vlex.es/vid/respuesta-europea-ciberdelincuencia-362484182

[73] Garriga, S. (26 de junio de 2013). Los nuevos piratas. La Nueva España. Recuperado el 29 de Abril de 2016, de http://nueva-espana.vlex.es/vid/nuevos-piratas-445178618.

[74] En el siguiente link podemos encontrar el comunicado de prensa emitido por la Comisión Europea en relación a la inauguración del Centro Europeo de Ciberdelincuencia: http://europa.eu/rapid/press-release_IP-13-13_es.htm

[75] *Ibídem.*

#### 2.1.1.2. Escuela Europea de Policía

La página oficial de la Unión Europea nos ofrece información sobre la Escuela Europea de Policía (CEPOL) que se describe como la congregación de "*los funcionarios policiales de rango superior con el objetivo de fomentar la cooperación transfronteriza en la lucha contra la delincuencia y el mantenimiento de la seguridad y el orden público*"[76].

Creada en 2005 por Decisión del Consejo 2005/681/JAI de 20 de septiembre de 2005, se configura como una agencia de la Unión Europea y como tal, es financiada por ésta. Entre sus objetivos están el prevenir y luchar contra los actos delictivos pero aportando la formación necesaria para su persecución mediante conferencias, cursos, seminarios, etc. que ofrece a lo largo de todo el año, difundir las prácticas de mejor calidad, así como elaborar programas armonizados[77].

### 2.1.2. Marco nacional

De entrada, con el primer problema que nos podemos encontrar en el ordenamiento jurídico español es que la redacción de la ley, en concreto de la Ley de Enjuiciamiento Criminal, está enfocada como si fuera el Juez quien realmente llevase a cabo las diligencias, cuando quien las efectúa en la práctica es la policía. El segundo problema que presenciamos es que desde los comienzos de nuestra ley procesal no queda cristalino quiénes debemos entender que conforman la policía judicial[78].

Hay que partir del artículo 126[79] de la Constitución donde se recoge que la policía judicial depende de los Jueces, de los Tribunales y del Ministerio Fiscal. En

---

[76] Sección de la Escuela Europea de Policía en la página web oficial de la Unión Europea en el siguiente enlace: http://europa.eu/about-eu/agencies/regulatory_agencies_bodies/pol_agencies/cepol/index_es.htm

[77] La información ha sido obtenida de la Decisión 2005/681/JAI del Consejo de 20 de septiembre de 2005 por la que se crea la Escuela Europea de Policía (CEPOL) y por la que se deroga la Decisión 2000/820/JAI. Esta decisión la podemos encontrar en el siguiente link: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=URISERV%3Al14006a.

[78] A pesar de que tal y como indica González Jiménez, A. (2014). Las diligencias policiales… ob. cit. p.20. desde la promulgación de la Ley de Enjuiciamiento Criminal de 1882 hayan entrado en vigor otros textos, algunos de ellos siendo la punta de iceberg dada su relevancia, como la Constitución Española de 1978, o por otro lado, la LOFSE 2/1986, de 13 de marzo y el RD 769/1987, de 19 de junio, sobre regulación de la policía judicial, sigue quedando difuso quiénes constituyen actualmente la policía judicial.

[79] Véase el artículo 126 de la Constitución Española de 1978 "*La policía judicial depende de los Jueces, de los Tribunales y del Ministerio Fiscal en sus funciones de averiguación del delito y descubrimiento y aseguramiento del delincuente, en los términos que la ley establezca*".

consecuencia, según GONZÁLEZ JIMÉNEZ las diligencias de investigación policial giran en torno a "*garantías, rigor, contradicción, documentación y seguimiento de las autoridades oportunas*"[80].

Así pues, el primer cuerpo policial con cierta solidez lo encontramos en 1844 incluso antes de la entrada en vigor de la LECrim, con la Guardia Civil. Sin embargo, hasta que no llegó la Real Orden de 19 de septiembre de 1896 no se creó el Cuerpo de Policía Judicial, aunque sólo con operatividad en Madrid y Barcelona.

La Policía Judicial ha pasado de tener unas escasas competencias a ser la parte más importante dentro de la investigación criminal. El problema estriba en que hace falta una Ley que la regule, indique quiénes realmente forman la policía judicial[81] y le atribuya unas funciones específicas, ya que a esto hay que sumar que aunque sea personal al servicio de la Administración de Justicia, de acuerdo con el artículo 104.2 CE también depende del Gobierno. Todo esto crea un gran desconcierto sobre su real naturaleza y el lugar que ocupa en el entramado institucional. En definitiva, pese a la importancia que tiene dentro del procedimiento, puesto que se suele encargar de la fase más importante de la investigación –muchas veces el Juez y el Ministerio Fiscal incluso con un papel de meros testigos sin llegar a intervenir-, nos encontramos con que la LECrim no la regula ampliamente[82] y que, por tanto, eso se traduce en lagunas e incertidumbre.

Si acudimos a la regulación de los artículos 282 a 289 de la LECrim, aunque encontremos quiénes forman parte de la policía judicial y con qué funciones, la lista es larga y se trata de un panorama "correcto" para 1882 pero que no es adecuado para la actualidad. No se entiende, por tanto, que teniendo la policía judicial un papel tan relevante dentro de la persecución de los delitos, sin embargo, no tenga una ordenación más exhaustiva y acorde con los tiempos que corren.

---

[80] González Jiménez, A. (2014). Las diligencias policiales… ob. cit. pp. 20-21.

[81] *Ibídem*. p. 28 "*De los arts. 547 a 550 de la LOPJ se desprende la coexistencia de dos tipos de policía judicial. De un lado, la genérica, como función de auxilio en la averiguación de los delitos y en el descubrimiento y aseguramiento de los delincuentes, que vincula a todos los miembros de las fuerzas y cuerpos de seguridad, tanto si dependen del gobierno central como de las comunidades autónomas o de los entes locales, que no deja de ser una concreción de la misma obligación que a todos impone el art. 118 CE. Y por otra parte, la específica, derivada del art. 548 LOPJ, y de la cual da la razón la exposición de motivos del RD 769/1987 que se plasma en las llamadas unidades de policía judicial. (…) Sin embargo, acaba resultado que la totalidad de fuerzas y cuerpos de seguridad del Estado, con carácter genérico, forman parte de la policía judicial*".

[82] Todo ello en González Jiménez, A. (2014). Las diligencias policiales… ob. cit. pp. 22-27.

En definitiva, y en orden cronológico, se han ido creando la Guardia Civil y el Cuerpo Nacional de Policía que son los que constituyen, a día de hoy, el pilar de la policía judicial[83]. Y estos han creado unidades especializadas en materia de criminalidad informática para enfocar mejor estos asuntos y tener un mayor índice de éxito. No obstante, también es importante únicamente denotar que incluso en la Ertzaintza encontramos una Sección Central de Delitos en Tecnologías de la Información[84], (SCDTI); síntoma de que la policía se ha puesto a trabajar a todos los niveles.

2.1.2.1. La Guardia Civil

Desde el año 2000 la Guardia Civil comenzó a trabajar en la lucha contra la ciberdelincuencia, convirtiéndose en una de sus prioridades dada la proliferación que se había dado de delitos informáticos. Existen diferentes estudios y planes que comenzaron a elaborarse en aquel entonces, pero que no vieron la luz hasta el 2002 cuando se pusieron en práctica. Fue entonces cuando ingresó en la Guardia Civil el primer personal altamente cualificado para el Subgrupo de Ciberterrorismo[85]. Si bien en 1996 se creó el Grupo de Delitos Informáticos, posteriormente cuando se incrementaron los delitos informáticos fue cuando se le cambió el nombre por Departamento de Delitos de Alta Tecnología con una ampliación de competencias y, finalmente, por la actual nomenclatura de Grupo de Delitos Telemáticos. A la vez se crearon Equipos de Investigación Tecnológica (EDITEs) en todas las provincias españolas[86].

Desde aquella realización práctica en el 2002, la inversión y la motivación para seguir avanzando en esta área no han dejado de crecer. En otras palabras, la Guardia Civil apuesta contra la ciberdelincuencia. Así pues, fruto de este avance en 2007 se

[83] Sin olvidar, por supuesto, la policía local que ha asumido la competencia de policía judicial, como ocurre en el País Vasco, Cataluña y Navarra. La razón de esto es consecuencia de la Instrucción 1/2008 de la Fiscalía General del Estado es que la policía local está adquiriendo una capacitación técnica y profesional que no puede pasarse por alto en la lucha contra la ciberdelincuencia. Así manifiesta todo ello González Jiménez, A. (2014). Las diligencias policiales… ob. cit. pp. 47-50.

[84] Para más información acudir a la página oficial de la Ertzaintza que puede consultarse en el siguiente enlace: https://www.ertzaintza.net/wps/portal/ertzaintza/!ut/p/c4/04_SB8K8xLLM9MSSzPy8xBz9CP0os3gXDydTo2AzN0tLE9dAdxNzC39zAwjQL8h2VAQA8kxKRw!!/

[85] Hernández García, L. F. (2014). Ciberseguridad; Respuesta global a las amenazas cibernéticas del s.XXI. Las ciberamenazas, un nuevo reto para la jefatura de información de la Guardia Civil. Cuadernos de la Guardia Civil: Revista de seguridad pública (49), p.32.

[86] *Vid.* Página oficial de la Guardia Civil. Puede consultarse en el siguiente enlace: https://www.gdt.guardiacivil.es/webgdt/la_unidad.php

conformó el Grupo de Ciberterrorismo. Pero lo realmente importante llegó en 2011 con la creación del Área Técnica de la Jefatura de Información, con el objetivo de aunar y coordinar capacidades y esfuerzos. Tampoco podemos olvidar la Unidad de Ciberseguridad en 2012 que está compuesto por personal altamente cualificado y multidisciplinar, provisto de las últimas herramientas tecnológicas, así como de una importante dotación presupuestaria gracias a los sacrificios hechos por otras unidades de la Jefatura para poder atender a esta financiación[87]. Síntoma todo ello de que la Guardia Civil está trabajando en este campo y que, además, está obteniendo resultados[88].

Hay que reseñar la operatividad que demuestra este Grupo, ya que es constante su presencia en seminarios y conferencias internacionales. El resultado positivo de todo ello ha sido que esto les ha facilitado poder crear una red de contactos policiales que, dado el carácter trasnacional de los delitos informáticos, es esencial si se quiere realmente resolver el delito informático y atrapar a su autor o autores[89].

En resumidas cuentas, la Guardia Civil cuenta con un personal especializado en materia de delitos informáticos, siendo precursora a nivel nacional en este sentido, lo que la lleva a tener amplia experiencia en la materia.

#### 2.1.2.2. Cuerpo Nacional de Policía

El Cuerpo Nacional de Policía, aunque forma parte de la policía judicial, hay que precisar que se trata de una policía judicial específica que tiene su base normativa en el artículo 548[90] de la LOPJ, donde se prevé la creación de unidades de policía judicial y entre ellas tenemos la Unidad de Investigación Tecnológica.

Dicho de otra forma, nos encontramos con una policía judicial específica compuesta, por supuesto, por policías especializados, como no podría ser de otra forma teniendo en cuenta las peculiaridades de los delitos informáticos. Tal es el grado de

---

[87] Hernández García, L. F. (2014). Ciberseguridad; Respuesta global… ob. cit. pp. 32-33.

[88] Para datos en concreto que demuestran la efectividad de la Guardia Civil en la práctica ver Hernández García, L. F. (2014). Ciberseguridad; Respuesta global… ob. cit. pp. 33-34.

[89] *Vid.* Página oficial de la Guardia Civil. Puede consultarse en el siguiente enlace: https://www.gdt.guardiacivil.es/webgdt/la_unidad.php

[90] Ver artículo 548. **"**1. *Se establecerán unidades de Policía Judicial que dependerán funcionalmente de las autoridades judiciales y del Ministerio Fiscal en el desempeño de todas las actuaciones que aquéllas les encomienden*. 2. *Por ley se fijará la organización de estas unidades y los medios de selección y régimen jurídico de sus miembros*". Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial.

especialización técnica y profesional en muchos casos, que incluso se reconoce el estatus de policía científica[91].

Así pues, como se ha indicado, en el contexto español nos encontrarnos con que dentro del Cuerpo Nacional de Policía, la Secretaría General se bifurca en cinco Unidades entre las que se encuentra la Unidad de Investigación Tecnológica. En ésta se ha creado la Brigada Central de Investigación Tecnológica[92] para responder a las amenazas de los delitos informáticos y la Brigada Central de Seguridad Informática.

La primera de ellas tiene entre sus funciones llevar a cabo investigaciones complejas, la formación de investigadores del Cuerpo Nacional de Policía y otros cuerpos de Policía extranjeros, su propio reciclaje adquiriendo nuevos conocimientos mediante foros internacionales de cooperación policial, la colaboración con diferentes instituciones, etc. Sin olvidar, por supuesto, su obligación de velar por la seguridad de los ciudadanos; razón por la que se ha puesto en marcha un sistema de alertas tecnológicas para mantener informado al ciudadano en todo momento.

Mientras que ésta acota su campo de actuación a la intimidad, protección de los menores, la propiedad intelectual e industrial y los fraudes en las telecomunicaciones, la Brigada Central de Seguridad Informática investiga los delitos que afectan a la seguridad lógica y los fraudes, con funciones similares a la anterior[93].

### 1.1. En el ámbito judicial

Bien es cierto que la policía constituye el primer eslabón de la cadena y que, por tanto, 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 pasando por una especialización suficiente por parte, también, de la Fiscalía y de los propios Jueces y Magistrados.

---

[91] González Jiménez, A. (2014). Las diligencias policiales… ob. cit. p. 46.

[92] La Brigada Central de Investigación Tecnológica queda "*Encuadrada en la Unidad de Investigación Tecnológica (UIT) que es el órgano de la Dirección General de la Policía y de la Guardia Civil encargado de la investigación y persecución de las actividades delictivas, de ámbito nacional e internacional, en materia de delincuencia económica y fiscal, así como la coordinación operativa y apoyo técnico a las respectivas Unidades Territoriales*". Véase en la página web oficial del Cuerpo Nacional de Policía: http://www.policia.es/org_central/judicial/udef/bit_quienes_somos.html

[93] *Vid.* página oficial del Cuerpo Nacional de Policía en el siguiente enlace: http://www.policia.es/org_central/judicial/udef/bit_quienes_somos.html

### 1.1.1. Fiscalía de Criminalidad Informática

A pesar de la existencia de una Delegación de Criminalidad Informática desde 2005, no es hasta la Instrucción 2/2011[94] cuando se introduce una especialización creando 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. Sin olvidar, que el uso cada vez más habitual de Internet nos ha llevado a la creación de nuevas formas de criminalidad[95].

Para paliar esta situación e ir camino al éxito se hacía necesario reforzar la actuación del Ministerio Fiscal y la mejor manera para ello era la especialización, teniendo en cuenta que los delitos informáticos requieren de unos conocimientos específicos y técnicos concretos. Sin embargo, 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 únicamente nos llevaría a la desnaturalización de esta especialización y a que quedase desbordada de trabajo[96].

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

Así pues, la Fiscalía de Criminalidad Informática puede perseguir tres categorías de delitos:

- Delitos en los que el objeto de la actividad delictiva son los propios sistemas informáticos o las TICs[97].
- Delitos en los que la actividad criminal se sirve para su ejecución de las ventajas que ofrecen las TICs[98].

---

[94] Ver Instrucción 2/2011, de 11 de octubre de 2011, sobre el Fiscal de Sala de Criminalidad Informática y las Secciones de Criminalidad Informática de las Fiscalías.

[95] Todo ello en Rayón Ballesteros, M. C., & Gómez Hernández, J. A. (2014). Cibercrimen: particularidades... ob. cit. p.216.

[96] Instrucción 2/2011, de 11 de octubre de 2011, sobre el Fiscal de Sala de Criminalidad Informática y las Secciones de Criminalidad Informática de las Fiscalías.

[97] v. gr. artículo 264 y siguientes del Código Penal que recoge el delito de sabotaje informático. Instrucción 2/2011, de 11 de octubre de 2011.

[98] v. gr. artículo 189 y siguientes del Código Penal que sancionan los delitos de corrupción y pornografía en relación a menores o personas discapacitadas. Instrucción 2/2011, de 11 de octubre de 2011.

- Delitos en los que la actividad criminal, además de servirse para su ejecución de las ventajas que ofrecen las TICs, entraña especial complejidad en su investigación que demanda conocimientos específicos en la materia[99].

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 se tiene que encargar, 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[100].

#### 1.1.2. Jueces y Magistrados

Partiendo de nuestra Ley de Leyes, donde se recogen los Derechos Fundamentales reconocidos a los ciudadanos del territorio español, los Jueces y Magistrados son los que tienen que velar por la no vulneración de los mismos, ya sea en la fase de investigación como en la fase del Juicio Oral.

Sin embargo, tal y como ha podido evidenciar en la práctica el Fiscal Jorge Bermúdez, Fiscal Delegado de Delitos Informáticos, la realidad es que muy pocos Jueces o Magistrados son diestros en esta materia. Tal y como se ha remarcado en algún momento del trabajo, la mayoría de las diligencias de investigación tecnológica requieren de 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 y no otra?

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 elenco 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

---

[99] v. gr. artículo 169 y siguientes del Código Penal que en relación a los "*delitos de amenazas y coacciones (…) cometidos a través de las TICs siempre que dicha circunstancia fuera determinante en la actividad delictiva y generara especial complejidad en la investigación criminal*". Instrucción 2/2011, de 11 de octubre de 2011.

[100] Todo ello en Instrucción 2/2011, de 11 de octubre de 2011, sobre el Fiscal de Sala de Criminalidad Informática y las Secciones de Criminalidad Informática de las Fiscalías.

técnica, que es la razón por la que haya tanta impunidad en relación a los mismos. No obstante, hay que encomiar la tarea de aquellos jueces, como el Juez Velasco Núñez, que sí han profundizado en este campo por motivaciones personales, tal vez, y cuyas resoluciones sí que pueden ser debidamente motivadas[101].

En conclusión, los delitos informáticos requieren de un plus en comparación con los delitos tradicionales –esto no implica que otros delitos no convencionales no requieran también de un plus-; conocimientos técnicos por parte de todos los funcionarios que participan a lo largo del proceso, así como cooperación tanto a nivel europeo como internacional por el carácter trasnacional de los mismos. Podemos apreciar que en el campo policial se han hecho muchos avances; que no se trata de un sector olvidado. La evolución constante y la creación de organismos a nivel europeo reflejan un buen primer punto de partida. La crítica, no obstante, ha de hacerse a nuestro ordenamiento jurídico. Si bien la policía judicial cada vez obtiene mejores resultados y no deja de invertir en la lucha contra la ciberdelincuencia, el punto flaco lo tenemos en la legislación, ya que se debería regular de forma más amplia y específica la policía judicial, fomentando una estructura jerarquizada que ponga orden y no haga que nos volvamos a tener que preguntar 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. A nivel de la Fiscalía 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 el reparto habitual de los delitos tradicionales que se traduciría en inexperiencia y en una labor menos profesional. Pero, sin duda alguna, la peor parte, y que hay que resolver de manera inmediata, proviene de los Jueces y Magistrados que no poseen unos conocimientos técnicos aptos para poder dictar sus resoluciones de forma suficientemente motivada. Paradójico, pues, que aquellos que son garantes de los derechos y libertades de los ciudadanos y que tienen que asegurar un proceso con todas las garantías, sean los que más trabajo tengan por delante.

[101] Toda la información obtenida en entrevista personal realizada al Fiscal Jorge A. Bermúdez, Fiscal Delegado de Criminalidad Informática.

## IV. RETOS PARA UNA REAL TUTELA JUDICIAL EFECTIVA

En el artículo 24.1 CE[102] 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 mediante un juicio que respete todas las garantías y mediante una resolución motivada en Derecho. Por otro lado, la segunda vertiente[103] hace alusión a que no puede haber indefensión[104].

No podemos pasar por alto que vivimos en un estado de derecho que conlleva intrínsecamente que para la resolución de conflictos, hagamos uso del debido proceso para garantizar a los ciudadanos esta tutela efectiva de sus derechos e intereses legítimos. A día de hoy resulta evidente que no es posible una organización mundial que goce de una única soberanía planetaria para resolver las controversias a nivel mundial. 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. Así pues, tal y como promueve ESPARZA LEIBAR hay que apostar por el proceso debido, cuyo resultado final no es otro que la consecución de la justicia[105].

En este sentido, el debido proceso resulta inevitablemente positivo para los ciudadanos, con la finalidad de conseguir justicia, ya que se trata de un modelo que no está estancado y sigue enriqueciéndose, así como que 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 viertan una negativa a modificar su ordenamiento jurídico en la dirección que resulta la adecuada, no tendrán otro resultado

---

[102] Artículo 24.1. "*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"*. Constitución Española de 1978.

[103] El Tribunal Constitucional se manifestó sobre la vertiente negativa de la tutela judicial efectiva en la STC 48/1984, de 4 de abril, 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)*".

[104] Bernárdez Cabello, O., & Ramos-Paúl de la Lastra, I. (2015). Retos de la tutela judicial efectiva frente a las ciberamenazas. Retos del derecho ante las nuevas amenazas, p.116.

[105] Esparza Leibar, I. (2012). El proceso debido como único modelo aceptable para la resolución de conflictos en un estado de derecho y como presupuesto para la globalización. El derecho procesal español del siglo XX a golpe de tango: Liber Amicorum, en homenaje y para celebrar su LXX cumpleaños, pp. 337-338.

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*"[106].

"*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*"[107]. Resultan, éstas, razones muy poderosas para que la resolución de los delitos informáticos respete, en todas y cada una de sus facetas, el proceso debido.

1. Problemas que plantean las nuevas diligencias de investigación tecnológica en relación a las garantías procesales del sospechoso

Sin repetir la configuración constitucional existente en el artículo dieciocho en relación a la ciberdelincuencia, la nueva Ley Orgánica 13/2015, de 5 de octubre, 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. Tal es así que todos los delitos clásicos pueden cometerse también en el mundo virtual; incluso tiene sus propios delitos este mundo virtual.

Sin embargo, esta legislación española en materia de delitos informáticos se caracteriza, tal y como apunta RUBIO ALAMILLO, por ser ambigua y poco clara; hecho que se refleja en el propio lenguaje "incorrecto" que se utiliza en la ley al utilizar de forma indistinta conceptos que no son lo mismo. Por lo que 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 con las actuaciones previstas Derechos Fundamentales de los sospechosos y crearles indefensión[108]. Pero todavía es pronto para saber cómo se va a llegar a aplicar en la práctica; tal vez, los que han de

[106] Esparza Leibar, I. (2012). El proceso debido… ob. cit. pp. 337-338.

[107] Bernárdez Cabello, O., & Ramos-Paúl de la Lastra, I. (2015). Retos de la tutela judicial… ob. cit.p.116.

[108] Rubio Alamillo, J. (2015). La informática en la reforma de la Ley de Enjuiciamiento Criminal. Diario La Ley (8662), p.3.

aplicar la ley aprecien estos peligros y diagnostiquen la enfermedad antes de que salga a la superficie.

Es comprensible, pues, que el legislador no tenga conocimientos informáticos, pero sin duda debe rodearse de los profesionales adecuados para que le asesoren. Cuestión ésta que podía haberse resuelto de mejor forma vista la redacción de algunos artículos. La reforma versa sobre la forma en la que se han de investigar los delitos informáticos, pero un cariz muy importante introducido por esta Ley es que ahora se permite 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[109].

Una de las diligencias de investigación que podemos encontrar es la de que un policía informático puede mandar archivos ilícitos[110] a un sospechoso; archivos que posteriormente podrán ser encontrados en nuestro ordenador. ¿Dónde está el problema? En que si no existe un inventario sobre los archivos ilícitos enviados por los policías informáticos, debidamente auditados por profesionales en la materia y con su respectivo código *hash*[111], esos archivos estarán en nuestros dispositivos y se nos podría acusar de haber cometido un delito[112]. Bien es cierto que como se ha indicado en otro momento, esta posibilidad está enfocada sobre todo para los delitos de pornografía infantil. No obstante, el problema sigue persistiendo.

En el artículo 588 ter a[113], el legislador vuelve a caer en la generalidad ya que, 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 a través de comunicación telefónica o mediante aplicaciones informáticas, con un sujeto que sea sospechoso de haber cometido un hecho delictivo. El legislador debía haber precisado qué tipo de información

---

[109] Rubio Alamillo, J. (2015). La informática… ob. cit. pp.3-4.

[110] Esta redacción podemos encontrarla en la Ley de Enjuiciamiento Criminal. Artículo 282.2 bis, apartado sexto, segundo párrafo. "*El agente encubierto informático, con autorización específica para ello, podrá intercambiar o enviar por sí mismo archivos ilícitos por razón de su contenido y analizar los resultados de los algoritmos aplicados para la identificación de dichos archivos ilícitos*".

[111] Ver pie de página núm. 42 donde podremos encontrar qué significa el código *hash*.

[112] Para más información acudir a Rubio Alamillo, J. (2015). La informática… ob. cit. p.4.

[113] Ley de Enjuiciamiento Criminal. Artículo 588 ter a. Presupuestos. "L*a 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*".

es necesario que se transmita 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[114]. Es decir, cuando se les pida una determinada información, han de cederla. Traducción, un ciudadano totalmente inocente podría ver su derecho a la intimidad afectado 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 pone comentarios subidos de tono en un foro[115].

Asimismo, de la lectura del artículo 588 sexies a LECrim[116], podemos apreciar que el legislador no le ha dado la importancia debida a algo tan importante como la cadena de custodia y que, por tanto, será la policía judicial y el juez en cuestión los que decidan en cada caso concreto cómo se ha de practicar la cadena de custodia. Custodia que es esencial para que estemos ante un proceso con todas las garantías, ya que sin ella sería muy fácil modificar, destruir, etc. lo incautado, dando lugar a pruebas contaminadas con la de problemas que dan en la práctica. En definitiva, no se estarían haciendo efectivas las garantías que dan lugar al derecho a la tutela judicial efectiva.

---

[114] Ley de Enjuiciamiento Criminal. Artículo 588 ter e. 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*".

[115] Rubio Alamillo, J. (2015). La informática… ob. cit. pp.4-5.

[116] Esta redacción podemos encontrarla en la Ley de Enjuiciamiento Criminal. Artículo 588 sexies a. 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, 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".

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 hecho de conectarlos a un ordenador sin haber llevado a cabo ningún tipo de interacción, contamina la prueba. Es por ello que el disco duro o la memoria USB se han de conectar a bloqueadores de escritura para que no queden directamente conectados al ordenador. Por tanto, la conclusión que se extrae de esto es que la cadena de custodia no es baladí y que si realmente queremos asegurar las garantías procesales, lo idóneo es utilizar material forense especializado para *clonar*[117] el contenido y proporcionar un código *hash*[118].

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. Lo que se traduce en que algún funcionario pudiese tener interés en modificar algún contenido y lo hiciese sin dejar ningún tipo de rastro y sin que nadie llegue a enterarse[119].

Otra imprecisión lingüística que el legislador probablemente haya pasado por alto es que la Ley habla de copias de datos y no de copias de dispositivos. Es decir, para copiar datos no queda de otra que acceder al propio contenido, lo que supondría una contaminación directa de la prueba. Y por otro lado, cuando se copian datos los archivos eliminados no se copian, razón por la cual lo adecuado es un clonado[120].

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. Asimismo, si bien el constituyente en 1978 era consciente de los peligros que podía entrañar el mundo digital, esa certeza parece haberse evaporado a día de hoy cuando de forma inexplicable la Ingeniería Informática es la única Ingeniería que ni siquiera está regulada por el Estado.

---

[117] No confundir “clonar” con “copiar”. Se trata de conceptos diferentes para la Informática Forense y para más información consultar Rubio Alamillo, J. (1 de junio de 2014). Clonación de discos duros en el peritaje informático. Recuperado el 29 de abril de 2016, de http://peritoinformaticocolegiado.es/clonacion-de-discos-duros-en-el-peritaje-informatico/

[118] La definición del código *hash* se puede encontrar en el pie de página núm.42.

[119] Rubio Alamillo, J. (2015). La informática… ob. cit. pp.5-6.

[120] Para más información consultar Rubio Alamillo, J. (2015). La informática… ob. cit. pp.6-7.

En conclusión, visto lo visto, no puedo estar más de acuerdo con los temores que me manifestó el Fiscal BERMÚDEZ[121], así como con lo expresado por RUBIO ALAMILLO al declarar que 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*"[122].

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 ésta sea válida en un proceso legal se ha creado la informática forense. Así pues, 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*"[123].

El *quid* de la cuestión reside, por tanto, en obtener la información necesaria, que ésta pueda ser válida en un proceso legal y que a la vez, no se cree indefensión. Sin embargo, 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, por ser estos los habituales, hemos de centrarnos en ellos.

[121] Impresiones obtenidas en la entrevista personal realizada al Fiscal Jorge A. Bermúdez, Fiscal Delegado de Criminalidad Informática.

[122] Rubio Alamillo, J. (2015). La informática… ob. cit. p.8.

[123] Bernárdez Cabello, O., & Ramos-Paúl de la Lastra, I. (2015). Retos… ob. cit. p.116.

### 2.1. La prueba documental

Si acudimos a la Ley de Enjuiciamiento Civil[124] 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[125]. Mientras que de acuerdo con el 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-, los documentos privados aunque también hacen prueba plena, dejan de tener ese valor si son impugnados por la parte perjudicada. No obstante, aunque el documento privado tenga valor probatorio, ello no es impedimento para que el Juez o Tribunal luego lo valore de acuerdo a la sana crítica y en conjunto con las demás pruebas.

Pero la LEC no es la única que habla del documento en estos términos; la jurisprudencia[126] también se ha decantado por esta amplitud. En la STS 1066/2009 de 4 de noviembre podemos apreciar que el Tribunal Supremo equipara el documento tradicional al documento electrónico. Consecuencia, ello, de la falta de regulación exhaustiva en torno a la ciberdelincuencia en la que como hemos podido apreciar la analogía ha estado a la orden del día. Así pues, si el documento informático es impugnado por falta de veracidad, la parte que lo ha aportado ha de demostrar su autenticidad, sin perjuicio, siempre, de que luego el Juez o Tribunal lo vaya a valorar de acuerdo a las reglas de la sana crítica[127]. En definitiva, 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. El informe pericial

El informe pericial tiene lugar cuando para valorar un hecho de especial relevancia se requieren conocimientos científicos o artísticos. De acuerdo con el articulado de la LECrim, el informe pericial se ha de hacer por dos peritos designados

[124] La prueba documental se regula en los artículos 382 a 384 de la Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil.

[125] 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 enumera qué documentos públicos en concreto son los que van a tener valor probatorio.

[126] Ver STS 1066/2009 de 4 de noviembre, fundamento jurídico segundo.

[127] Todo ello obtenido de Bernárdez Cabello, O., & Ramos-Paúl de la Lastra, I. (2015). Retos… ob. cit. pp.117-118.

por el juez de oficio, además de que tienen la obligación de jurar o prometer decir la verdad, así como de responder con la mayor objetividad posible haciendo gala de su profesionalidad.

Resulta necesario volver a abordar aquí el tema del valor probatorio, en este caso del informe pericial. Así pues, los peritos deben responder a las preguntas, a las repreguntas e incluso el informe puede llegar a ser prueba anticipada[128] en los casos que lo permite la ley. Sin embargo, aquí también de acuerdo con el artículo 348 LEC[129], el Juez o Tribunal seguirá las reglas de la sana crítica.

Esto en términos generales, pero el asunto es ciertamente diferente en el caso de la prueba pericial informática. En esta casuística no se puede pasar por alto que existe una certificación de calidad de acuerdo con 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 ésta se establecen una serie de criterios que se han de tener en cuenta a la hora de realizar el informe pericial informático[130].

Hasta aquí todo parece idílico y que esto en concreto está 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 que ni siquiera se exige en sede judicial[131]. Dicho de otra forma, la informática forense en España dista de ser lo eficaz que debiese ser; a pesar de tener las herramientas para ello, no se sabe por qué motivo se obvian. El resultado de esto es que puede crearse indefensión puesto que los informes no se practican de la forma en la que debieran hacerse, a causa de que los jueces y magistrados no tienen unos conocimientos suficientes sobre la materia como para exigir unos requisitos mínimos de validez de la prueba, así como para poder juzgarla de acuerdo con las reglas de la sana crítica.

No podría estar más de acuerdo con BERNÁRDEZ CABELLO cuando afirma que "*se aprecia la inexistencia de un marco jurídico operativo y eficaz que permita la*

[128] Vid. Artículo 730 del Real decreto de 14 de septiembre de 1882 por el que se aprueba la Ley de Enjuiciamiento Criminal.

[129] Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil. Artículo 348. Valoración del dictamen pericial. El tribunal valorará los dictámenes periciales según las reglas de la sana crítica.

[130] Todo ello obtenido de Bernárdez Cabello, O., & Ramos-Paúl de la Lastra, I. (2015). Retos… ob. cit. pp.118-119.

[131] *Ibídem*. p. 119.

*persecución del ciberterrorismo y ciberdelincuencia en los términos previstos por la Estrategia[132] de Ciberseguridad Nacional*[133]".

3. Derecho comparado: Estados Unidos como referencia

En Estados Unidos existe una regulación donde 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. Partiendo 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*"[134].

Asimismo, introducen una distinción en relación 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. Añadir también que la parte que introduzca la prueba ha de demostrar que ésta es real[135].

Teniendo como guía el Manual "Forensic Examination of Digital Evidence: A Guide for Law Enforcement", la informática forense ha de seguir una serie de pautas: la valoración de la evidencia, la adquisición de la misma, su examen y su documentación. Así es como puede tener un real valor probatorio el informe pericial. En la primera, el perito valorando la evidencia de forma amplia y general toma la decisión sobre qué acciones son necesarias. En la segunda, teniendo en cuenta que la evidencia digital es muy fácil que sea alterada, destruida, etc., se realiza una copia (mejor un clonado) de la

[132] "*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*". Para más información consultar Gobierno de España: Departamento de Seguridad Nacional, Presidencia del Gobierno. (2013). Estrategia de Ciberseguridad Nacional.

[133] Todo ello en Bernárdez Cabello, O., & Ramos-Paúl de la Lastra, I. (2015). Retos… ob. cit. pp.117-119.

[134] Bernárdez Cabello, O., & Ramos-Paúl de la Lastra, I. (2015). Retos… ob. cit. p.120.

[135] *Ibídem*, p. 120.

original para pasar a trabajar sobre esa copia. En tercer lugar, se recupera la información contenida en el soporte que la almacenaba y así, se procede a su interpretación una vez está en formato lógico. Y en cuarto y último lugar, es muy importante que todo el proceso haya sido documentado por el perito mediante un informe[136]. Así, se respetan las máximas garantías posibles de la evidencia y se evita la indefensión tal y como pretende el artículo 24 CE de nuestro ordenamiento jurídico, que recoge el derecho a la tutela judicial efectiva[137].

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*"[138].

Por otro lado, hay que resaltar la poca informática forense que hay en España. Por tanto, esto va en perjuicio de la tutela judicial efectiva pues podemos encontrarnos con casos en los que no se respetan todas las garantías. Así pues, se requieren cambios tanto a nivel normativo, como operativos.

¿Cómo formular una Informática Forense en España que siga la estela de la de Estados Unidos? Para comenzar, tal y como se ha venido insinuando, es necesario que se regule la figura del perito informático para asegurar que realmente se trata de una persona con la cualificación suficiente para dar un juicio correcto sobre la evidencia. Para continuar, se debería desarrollar reglamentariamente el artículo 478 LECrim, que es donde se recoge el contenido del informe pericial, para que las exigencias sean más similares a las de Estados Unidos. Pero para ello es necesario invertir más en I+D, ya que se necesitan equipos informáticos de alta tecnología para poder realizar unas buenas copias (mejor el clonado) de las evidencias, para analizar los resultados, así como para formar a los peritos en el uso de estos equipos[139].

---

[136] Todo ello en Bernárdez Cabello, O., & Ramos-Paúl de la Lastra, I. (2015). Retos… ob. cit. pp.119-121.

[137] Para más información acudir a Bernárdez Cabello, O., & Ramos-Paúl de la Lastra, I. (2015). Retos… ob. cit. p.121.

[138] Bernárdez Cabello, O., & Ramos-Paúl de la Lastra, I. (2015). Retos… ob. cit. p.121.

[139] Para más información consultar Bernárdez Cabello, O., & Ramos-Paúl de la Lastra, I. (2015). Retos… ob. cit. p. 122.

Para terminar, y probablemente uno de los aspectos más importantes tal y como se quiere evidenciar con este trabajo, 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 forense informático puedan identificar fácilmente que se han respetado todas las garantías. Cuestión especialmente relevante en el caso de los jueces y tribunales, ya que sin la debida formación no pueden valorar el informe forense de acuerdo con las reglas de la sana crítica[140].

Y 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 únicamente se puede conseguir mediante el proceso debido, ya que tal y 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[141].

## V. LA COOPERACIÓN INTERNACIONAL COMO ÚNICA VÍA

El carácter trasnacional de los delitos informáticos ya nos da una pista sobre cómo se puede avanzar en esta materia y así luchar contra la impunidad. En este sentido 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[142], pero todavía queda un largo camino para llegar a un estadio de seguridad y de un gran número de 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 2015, que reflejan el esfuerzo realizado por el legislador español para adecuar la situación a las esferas europeas e internacionales y dar una mejor cobertura a la persecución de los delitos informáticos.

[140] Todo ello en Bernárdez Cabello, O., & Ramos-Paúl de la Lastra, I. (2015). Retos… ob. cit. pp. 121-122.

[141] Lorca Navarrete, A. M. (2003). El derecho procesal como sistema de garantías. *Boletín Mexicano de derecho comparado* (107), p.557.

[142] Son dos importantes casos de la jurisprudencia internacional que los Tribunales siempre tienen como referencia. Para profundizar en los mismos consultar Díaz Gómez, A. (2010). El delito informático, su problemática y la cooperación internacional como paradigma de su solución: El Convenio de Budapest. Revista electrónica del Departamento de Derecho de la Universidad de La Rioja, REDUR (8), pp. 175-176.

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

Sin embargo, tal y como se pondrá de relieve, 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 sólo les afecten a ellos, sino también 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 de Estados posible[143]. Pero mientras siga habiendo Estados que no colaboren en esta lucha internacional, la impunidad seguirá estando 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.

Por tanto, la cooperación internacional pasa por fomentar el desarrollo en el Derecho Penal Informático, en las normas procesales, así como en la cooperación de las Administraciones de Justicia de los diferentes Estados. Colaboración que 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. Generalidad que juega 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[144].

La cooperación ha de pasar estrictamente por un mayor intercambio de información. En este sentido, este intercambio para que se materialice de forma efectiva en la práctica ha de superar dos fases. La primera de ellas es el intercambio a nivel nacional entre las diferentes instituciones, órganos y autoridades; es decir, entre las Fuerzas y Cuerpos de Seguridad del Estado, instituciones gubernamentales y los órganos jurisdiccionales. Una vez esto se ha resuelto y se consigue que la información fluya de un lado a otro sin impedimentos, es cuando hay que ponerse a trabajar en la segunda de las fases. Esta segunda se refiere a un intercambio de información a nivel internacional, poniendo en marcha normas de Derecho Procesal Penal Internacional que posibiliten esta transmisión mediante las herramientas adecuadas.

---

[143] Para más información consultar Díaz Gómez, A. (2010). El delito informático… ob. cit. pp. 182-183.

[144] Acudir a Díaz Gómez, A. (2010). El delito informático… p. 187.

Esta transmisión de información se ha de caracterizar por agilidad y rapidez, pero sin que el fin justifique los medios y en el camino echemos por tierra los derechos y garantías que asisten a los ciudadanos. Es ésta, pues, probablemente, la mayor de las ventajas de la cooperación internacional teniendo en cuenta su carácter transversal al afectar también a la actividad administrativa y jurisdiccional común. Pero no sólo esto, ya que no se puede abordar una política común sin tener en cuenta a las víctimas y a los delincuentes. Por tanto, para las víctimas hay que establecer medios sencillos de denuncia, que puedan conseguir una reparación efectiva de los daños, que persigan adecuadamente los delitos informáticos, etc. Respecto al delincuente, por el contrario, no podemos olvidarnos de respetar sus derechos tales como los Derechos Humanos que están reconocidos y consolidados por sendos textos internacionales[145].

Así pues, como se ha indicado, el campo donde más se ha de trabajar para obtener una mayor cooperación internacional es en el ámbito procesal. Hecho que lo confirma la doctrina que viene ya tiempo solicitando mayor armonización procesal en la lucha contra la criminalidad informática, así como que en la práctica el Derecho Penal sustantivo haya sido relegado a un segundo plano siendo el foco de atención 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"[146].

Siguiendo las pautas de DÍAZ GÓMEZ, una correcta cooperación internacional debería revestir o cumplir una serie de requisitos. Para empezar, el punto de partida, sin duda alguna, tiene que ser un pensamiento universal para abarcar al máximo número de Estados posibles. Por otro lado, esta cooperación ha de detentar una serie de límites formales y materiales. Con los formales nos referimos a que hay que respetar todos y cada uno de los ordenamientos jurídicos, así como los Tratados Internacionales; los materiales 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.

Asimismo, la cooperación ha de 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, exista una lógica normativa, etc. La respuesta que se

[145] A efectos de más datos sobre la transmisión de la información consultar Díaz Gómez, A. (2010). El delito informático… pp.188-189.

[146] Para más información acudir a Díaz Gómez, A. (2010). El delito informático…ob. cit. p. 190.

dé ha de responder a todos los problemas y no dar una solución parcial. Y 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. Finalmente y como no podía ser de otra forma, aunque la Unión Europea haya conseguido grandes avances en materia de criminalidad informática, la cooperación ha de provenir de las más altas instancias como es Naciones Unidas[147].

Y 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[148]. La pregunta es, ¿cumple con todos los requisitos mencionados? Se trata de un instrumento internacional que, aunque haya sido un gran paso de cooperación en la lucha contra la ciberdelincuencia, no es todo lo perfecto que hubiera gustado que fuese. Aun así, el propio Convenio nos refleja también el hecho de que los esfuerzos en gran parte hay que enfocarlos 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[149].

Así pues, el propio 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*"[150]. No obstante, tiene ciertos errores, pero que no vician el resto del Tratado que supone un antes y un después en la lucha contra los delitos informáticos.

---

[147] Todo ello en Díaz Gómez, A. (2010). El delito informático…ob. cit. pp. 192-194.

[148] El Convenio sobre Cibercriminalidad está en vigor para España desde el día 01/10/2010, habiendo sido publicado en el BOE de 17/09/2010. Cuestiones prácticas y procesales relacionadas con la investigación de los delitos informáticos. (s.f.), p.28. La ratificación del mismo se produjo el 3 de junio de 2010 tal y como indica Salvadori, I. (2011). 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 (1), p.251.

[149] 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, A. (2010). El delito informático… p. 196.

[150] Morón Lerma, E., & Rodríguez Puerta, M. (2002). Traducción y breve comentario del Convenio sobre Cibercriminalidad. Revista de derecho y proceso penal (7), p.169. Visto en Díaz Gómez, A. (2010). El delito informático… p. 196.

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 de forma conjunta y coordinada. La cooperación internacional es la única forma de crear conciencia en el resto de Estados, un elemento éste último muchas veces relegado a un puesto sin importancia, y así progresivamente cada vez más Estados se sumarán a la lucha contra la criminalidad informática.

## VI. CONCLUSIONES

### PRIMERA

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 innumerables y constantes ejemplos que se han puesto a lo largo de todo el trabajo, parece apreciarse que el legislador no se ha rodeado de los técnicos informáticos adecuados para que le asesorasen y eso se ha traducido, por ejemplo, en que se utilicen como sinónimos expresiones que no son lo mismo. Asimismo, el hecho de que el legislador no conozca el mundo digital de primera mano ha conllevado también que en la nueva Ley 13/2015, donde se regulan las 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.

### SEGUNDA

En el marco nacional, siendo la policía judicial 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, así como unificar materiales y recursos humanos para evitar un despilfarro de tiempo y dinero. Esta estructura, además, nos sirve para toda la delincuencia en general y no se trata de algo específico para la criminalidad informática, por lo que son múltiples los beneficios que puede aportar.

### TERCERA

El tratamiento que se ha de conferir a los delitos informáticos no puede ser, ni mucho menos, 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 – sin obviar que también hemos asistido al nacimiento de nuevos delitos en otras materias que requieren asimismo de un tratamiento específico, como puede ser la corrupción-. Para comenzar, a diferencia de lo que ocurre en los tradicionales, en los delitos informáticos observamos que el autor en la mayoría de las ocasiones realiza el hecho delictivo desde un determinado territorio y que los resultados se materializan en otro muy distinto, llegando a tener un carácter trasnacional. Este acontecimiento dificulta *per se* la persecución del mismo pues conlleva que diferentes órganos jurisdiccionales sean potencialmente competentes; razón por la que se haya decantado el Tribunal Supremo por aplicar el principio de ubicuidad que es el que menos zonas de impunidad ofrece. Sin embargo, esta nota de internacionalidad no es propia de los delitos tradicionales, ya que la acción y el resultado suele darse en el mismo lugar; otra cuestión diferente 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 haya que tratarlos de forma específica.

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

**CUARTA**

Partiendo de la dificultad que entrañan para su investigación los delitos informáticos, siendo la policía judicial la que se encarga de llevar a cabo las diligencias de investigación en la práctica, resulta lógico que estén especializados en criminalidad informática. Podemos decir orgullosos que nuestra policía judicial se ha puesto las pilas y que existen unidades especializadas tanto en la Guardia Civil como en la Comisaría General del Estado, así como que invierten constantemente en esta materia para no quedarse obsoletos y ser cada vez más eficaces. Sin olvidar que incluso la policía que tiene un campo de actuación inferior al nacional, como puede ser la Ertzaintza, ha creado su propia unidad para los delitos informáticos y está formando a sus trabajadores.

Sin embargo, aunque la Fiscalía también haya hecho sus avances creando una Fiscalía Especial, en este sentido el punto débil lo tenemos en los órganos jurisdiccionales; 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 llega a ser consciente de lo que realmente se le pide o tiene ante sí. Por lo que es necesario una inminente instrucción en criminalidad informática; una formación específica que nos permita conseguir capacitación para tratar esta materia por parte de todo el que intervenga de una forma u otra en el proceso. Pero como indico, es inadmisible que precisamente los que tienen que asegurar las garantías y los derechos de los ciudadanos sean el eslabón más débil, mientras que la policía judicial hace esfuerzos para progresar y renovarse. En resumen, hay que remar todos juntos porque si no nunca llegaremos a la meta.

**QUINTA**

La tutela judicial efectiva ha de respetarse en todo momento, por lo que hay que garantizar que se respeten todas y cada una de las garantías mediante el proceso debido. La nueva Ley 13/2015 aunque pueda pecar, a veces, de ambiciosa pretendiendo abarcar el máximo de situaciones posibles, inadvertidamente en perjuicio de las mencionadas garantías, hay que alabar el gran paso que supone después de décadas pidiendo no una nueva regulación en materia de delitos informáticos, sino una regulación a secas. Por tanto, habiendo localizado dónde están 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 jurisprudencialmente.

**SEXTA**

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 dándonos ya por imposibles, se ha conformado con la aplicación de la analogía y un desarrollo jurisprudencial. La actitud del legislador español desde luego 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 para terminar, porque cuando se ha puesto

a legislar lo ha hecho tarde y no todo lo bien que 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 demostrando que realmente tenemos como propósito paliar la criminalidad informática.

**SÉPTIMA**

Tras la lectura de múltiples artículos de diferentes autores realmente saco en claro que si de verdad se quiere luchar contra la criminalidad informática, no es suficiente con que cada Estado promueva independientemente a nivel interno un desarrollo normativo, de medios, de personal, etc., sino que necesariamente se han de aunar fuerzas y pasar por la cooperación internacional. No en vano los delitos informáticos se caracterizan por su carácter trasnacional –a pesar de que la delincuencia del siglo XXI en general sea propiamente así, la ciberdelincuencia especialmente-, que precisamente es uno de los elementos que más dificultades crea en la práctica.

Así pues, sobre la base de que para luchar contra la criminalidad informática no nos sirve la justicia universal, ni 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, en los mínimos esenciales coinciden. 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 es cierto que ya desde hace algunos años parece que los Estados han comenzado a concienciarse respecto a que a nivel particular no son suficiente para luchar contra la ciberdelincuencia. Y aunque el progreso es lento porque es difícil coordinar a tantos Estados, me gustaría terminar con un aliento de esperanza porque cuando se quiere, se puede.

**BIBLIOGRAFÍA**

- Autores:


Acurio del Pino, S. (2011). Delitos informáticos: Generalidades. Obtenido de http://www. oas. org/juridico/spanish/cyb_ecu_delitos_inform. pdf.

Álvarez-Cienfuegos Suárez, J. M. (1998). Aspectos procesales en relación con la investigación de delitos informáticos. *Revista Catalana de Seguretat Pública* (3), pp.27-46.

Amich Elías, C. (2015). Los marcos legales aplicables a las amenazas y riesgos cibernéticos. *Retos del derecho ante las nuevas amenazas*, pp.93-109.

Benítez Ortuzar, I. F. (2009). Informática y delito. Aspectos penales relacionados con las nuevas tecnologías. En L. Morillas Cueva, M. J. Cruz Blanca, & G. Quintero Olivares, *Reforma del Código Penal. Respuestas para una sociedad del siglo XXI* (pp. 111-136). Dykinson.

Bernárdez Cabello, O., & Ramos-Paúl de la Lastra, I. (2015). Retos de la tutela judicial efectiva frente a las ciberamenazas. *Retos del derecho ante las nuevas amenazas*, pp. 111-123.

Chinchilla, A. (s.f.). *vLex España.* Recuperado el 25 de enero de 2016, de http://diario-informacion.vlex.es/vid/ciberdelincuencia-ojo-dato-523529010

Corcoy Bidasolo, M. (2007). Problemática de la persecución penal de los denominados delitos informáticos: particular referencia a la participación criminal y al ámbito espacio temmporal de comisión de los hechos. *Eguzkilore: Cuaderno del Instituto Vasco de Criminología* (21), pp.7-32.

Cuestiones prácticas y procesales relacionadas con la investigación de los delitos informáticos. (s.f.).

De la Cuesta Arzamendi, J. L., De la Mata Barranco, N. J., Esparza Leibar, I., San Juan Guillén, C., Pérez Machío, A. I., Saiz Garitaonandia, A., . . . Hernández Díaz, L. (2010). *Derecho penal informático.* Aranzadi, SA.

Díaz Gómez, A. (2010). El delito informático, su problemática y la cooperación internacional como paradigma de su solución: El Convenio de Budapest. *Revista electrónica del Departamento de Derecho de la Universidad de La Rioja, REDUR* (8), pp.169-203.

Elvira Perales, A. (enero de 2011). *Congreso de los Diputados*. Recuperado el 8 de abril de 2016, de http://www.congreso.es/consti/constitucion/indice/sinopsis/sinopsis.jsp?art=18&tipo=2

Esparza Leibar, I. (2012). El proceso debido como único modelo aceptable para la resolución de conflictos en un estado de derecho y como presupuesto para la globalización. *El derecho procesal español del siglo XX a golpe de tango: Liber Amicorum, en homenaje y para celebrar su LXX cumpleaños*, pp. 319-338.

Faraldo Cabana, P. (2007). Los conceptos de manipulación informática y artificio semejante en el delito de estafa informática. *Eguzkilore: Cuaderno del Instituto Vasco de Criminología* (21), pp.33-57.

Gobierno de España: Departamento de Seguridad Nacional, Presidencia del Gobierno. (2013). Estrategia de Ciberseguridad Nacional.

González Hurtado, J. A. (2013). *Delincuencia informática: daños informáticos del artículo 264 del Código Penal y propuesta de reforma.* Tesis doctoral, Universidad Complutense de Madrid, Departamento de Derecho Penal, Madrid.

González Jiménez, A. (2014). *Las diligencias policiales y su valor probatorio.* Tesis doctoral, Universidad Rovira i Virgili, Departamento de Derecho Privado, Procesal y Financiero, Tarragona.

Hernández Díaz, L. (2009). El delito informático. *Eguzkilore: Cuaderno del Instituto Vasco de Criminología* (23), pp.227-243.

Hernández García, L. F. (2014). Ciberseguridad; Respuesta global a las amenazas cibernéticas del s.XXI. Las ciberamenazas, un nuevo reto para la jefatura de información de la Guardia Civil. *Cuadernos de la Guardia Civil: Revista de seguridad pública* (49), pp.6-36.

López-Barberá Martín, A. (2014). `Deep Web´ o Internet profundo. *SEGURITECNIA: Revista Decana Independiente de Seguridad* (407), pp.96-97.

Lorca Navarrente, A. M. (2003). El derecho procesal como sistema de garantías. *Boletín Mexicano de derecho comparado* (107), pp.532-557.

Morón Lerma, E. (2007). Quiebras de la privacidad en escenarios digitales: espionaje industrial. *Eguzkilore: Cuaderno del Instituto Vasco de Criminología* (21), pp.117-144.

Morón Lerma, E., & Rodríguez Puerta, M. (2002). Traducción y breve comentario del Convenio sobre Cibercriminalidad. *Revista de derecho y proceso penal* (7).

Muerza Esparza, J. (2015). *DOSSIER reforma de la Ley de Enjuiciamiento Criminal: La reforma procesal penal de 2015.* Thomson Reuters.

National Institute of Justice. (2004). *Forensic Examination of Digital Evidence: A Guide for Law Enforcement.* U.S. Department of Justice.

Pérez Vaquero, C. (s.f.). El muchacho de ninguna parte. *IN ALBIS*, pp.30-31.

Planchadell Gargallo, A. (2007). Especialidades procesales en la persecución de los delitos contra la propiedad intelectual e industrial. *Eguzkilore: Cuaderno del Instituto Vasco de Criminología* (21), pp.145-161.

Puente Aba, L. (2007). Delitos contra la intimidad y nuevas tecnologías. *Eguzkilore: Cuaderno del Instituto Vasco de Criminología* (21), pp.163-183.

Rayón Ballesteros, M. C., & Gómez Hernández, J. A. (2014). Cibercrimen: particularidades en su investigación y enjuiciamiento/ Cybercrime: particularities in investigation and prosecution. *Anuario Jurídico y Económico Escurialense* (47), pp.209-234.

Rodríguez Bernal, A. P. (2007). Los cibercrímenes en el espacio de libertad, seguridad y justicia. *Revista de derecho informático* (103).

Rubio Alamillo, J. (2015). La informática en la reforma de la Ley de Enjuiciamiento Criminal. *Diario La Ley* (8662).

Ruiloba Castilla, J. C. (2006). La actuación policial frente a los déficits de seguridad de Internet. *Revista de Internet, Derecho y Política* (2), pp.52-62.

Salvadori, I. (2011). 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* (1), pp.221-252.

San Juan , C., Vozmediano, L., & Vergara, A. (2009). Miedo al delito en contextos digitales: Un estudio con población urbana. *Eguzkilore: Cuadernos del Instituto Vasco de Criminología* (23), pp.175-190.

Stern Briones, E. (2007). El sentido de la privacidad, la intimidad y la seguridad en el mundo digital: ámbitos y límites. *Eguzkilore: Cuaderno del Instituto Vasco de Criminología* (21), pp.185-199.

Velasco Núñez, E. (2006). Aspectos procesales de la investigación y de la defensa en los delitos informáticos. *La Ley: Revista jurídica española de doctrina, jurisprudencia y bibliografía* (3), pp.1857-1864.

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

- Legislación

- Organización Internacional. Convenio sobre la Ciberdelincuencia, hecho en Budapest el 23 de noviembre de 2001. Consejo de Europa, [consultado 29 abril 2016]. Disponible en: https://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/ETS_185_spanish.PDF

- Unión Europea. Decisión Marco 2005/222/JAI del Consejo, de 24 de febrero de 2005 relativa a los ataques contra los sistemas de información. *Diario Oficial de la Unión Europea*, 16 de marzo de 2005 [consultado 29 abril 2016]. Disponible en: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2005:069:0067:0071:ES:PDF

- Unión Europea. Decisión nº 2005/681/JAI del Consejo, de 20 de septiembre de 2005, por la que se crea la Escuela Europea de Policía (CEPOL) y por la que se deroga la Decisión 2000/820/JAI. Diario Oficial de la Unión Europea, 1 de octubre de 2005 [consultado 29 abril 2016]. Disponible en: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex%3A32005D0681

- España. Constitución Española de 1978. *Boletín Oficial del Estado,* 29 de diciembre de 1978, núm. 311, pp. 29313-29424, [consultado 29 abril 2016]. Disponible en: https://www.boe.es/diario_boe/txt.php?id=BOE-A-1978-31229.

- España. Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial. *Boletín Oficial del Estado*, 2 de julio de 1985, núm. 157, pp. 20632-20678, [consultado 29 abril 2016]. Disponible en: https://www.boe.es/buscar/act.php?id=BOE-A-1985-12666.

- Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal. *Boletín Oficial del Estado*, 24 de noviembre de 1995, núm. 281, pp. 33987-34058, [consultado 29 abril 2016]. Disponible en: https://www.boe.es/buscar/act.php?id=BOE-A-1995-25444

- España. Ley Orgánica 13/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica. *Boletín Oficial del Estado*, 6 de

octubre de 2015, núm. 239, pp. 90192-90219, [consultado 29 abril 2016]. Disponible en: https://www.boe.es/diario_boe/txt.php?id=BOE-A-2015-10725

- Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil. *Boletín Oficial del Estado*, 8 de enero de 2000, núm. 7, pp. 575-728, [consultado 29 abril 2016]. Disponible en: https://www.boe.es/buscar/act.php?id=BOE-A-2000-323

- España. Real Decreto de 14 de septiembre de 1882 por el que se aprueba la Ley de Enjuiciamiento Criminal. *Boletín Oficial del Estado,* 17 de septiembre de 1882, núm. 260, pp. 803-806, [consultado 29 abril 2016]. Disponible en: https://www.boe.es/buscar/act.php?id=BOE-A-1882-6036

- España. Real Decreto de 24 de julio de 1889 por el que se publica el Código Civil. *Boletín Oficial del Estado*, 25 de julio de 1889, núm. 206, pp. 249-259, [consultado 29 abril 2016]. Disponible en: https://www.boe.es/buscar/act.php?id=BOE-A-1889-4763.

- España. Instrucción 1/2008 de la Fiscalía General del Estado, sobre la dirección por el Ministerio Fiscal de las actuaciones de la Policía Judicial. Boletín Oficial del Estado, *Fiscal.es,* [consultado 29 abril 2016]. Disponible en: https://www.fiscal.es/fiscal/PA_WebApp_SGNTJ_NFIS/descarga/memoria2009_Instruccion1_2008.pdf?idFile=3dd781e4-7ed3-4fce-a893-f8482bb78af3

- España. Instrucción 2/2011, de 11 de octubre de 2011, sobre el Fiscal de Sala de Criminalidad Informática y las Secciones de Criminalidad Informática de las Fiscalías. *Fiscal.es,* [consultado 29 abril 2016]. Disponible en: https://www.fiscal.es/fiscal/PA_WebApp_SGNTJ_NFIS/descarga/memoria2012_vol1_instru_02.pdf?idFile=6311c525-d23a-45d7-9e50-458f6f8c3406

- España. Real Orden de 19 de septiembre de 1896, que crea el Cuerpo de Policía Judicial para Madrid y Barcelona destinado a la persecución de delitos cometidos por medio de explosivos.

- Jurisprudencia

- Tribunal Europeo de Derechos Humanos. Caso Valenzuela Contreras contra España. Sentencia de 30 de julio de 1998.

- España. Tribunal Constitucional (Sala Segunda) [versión electrónica – buscador de jurisprudencia Constitucional], Sentencia 48/1984, de 4 de abril. [consultado 29 abril 2016].

- España. Tribunal Constitucional (Sala Primera) [versión electrónica – buscador de jurisprudencia Constitucional], Sentencia 254/1993, de 20 de julio. [consultado 29 abril 2016]

- España. Tribunal Constitucional (Pleno) [versión electrónica – buscador de jurisprudencia Constitucional], Sentencia 290/2000, de 30 de noviembre. [consultado 29 abril 2016]

- España. Tribunal Constitucional (Sala Segunda) [versión electrónica – buscador de jurisprudencia Constitucional], Sentencia 237/2005, de 26 de septiembre. [consultado 29 abril 2016].

- España. Tribunal Supremo (Sala de lo Penal) [versión electrónica – buscador de jurisprudencia CENDOJ], Sentencia 1066/2009, de 4 de noviembre. [consultado 29 abril 2016].

- España. Tribunal Supremo (Sala de lo Penal) [versión electrónica – buscador de jurisprudencia CENDOJ], Auto de 4 de marzo de 2009. [consultado 29 abril 2016].

- España. Tribunal Supremo (Sala General) [versión electrónica – buscador de jurisprudencia CENDOJ], Acuerdo no jurisdiccional de 3 de febrero de 2005. [consultado 29 abril 2016].

- España. Audiencia Nacional (Sala de lo Penal) [versión electrónica – buscador de jurisprudencia CENDOJ], Sentencia 14/2001, de 10 de marzo. [consultado 29 abril 2016].

- Páginas web y otros

Comisión Europea. (s.f.). Recuperado el 29 de abril de 2016, de http://europa.eu/rapid/press-release_IP-13-13_es.htm

Conferecia impartida por el Fiscal Jorge A. Bermúdez, Fiscal Delegado de Criminalidad Informática: LECr* Service Pack 2. Rooted CON 2015; un Congreso de Seguridad Informática que se celebra anualmente. Ver enlace: https://www.youtube.com/watch?v=-PfcUXCwjOM

Cuerpo Nacional de Policía. (s.f.). Recuperado el 29 de abril de 2016, de http://www.policia.es/org_central/judicial/udef/bit_quienes_somos.html

El País. (25 de enero de 2016). *vLex España.* Obtenido de http://el-pais.vlex.es/vid/golpe-policial-deep-web-543508626

Entrevista personal realizada al Fiscal Jorge A. Bermúdez, Fiscal Delegado de Criminalidad Informática.

Ertzaintza. (s.f.). Recuperado el 6 de mayo de 2016, de https://www.ertzaintza.net/wps/portal/ertzaintza/!ut/p/c4/04_SB8K8xLLM9MSSzPy8xBz9CP0os3gXDydTo2AzN0tLE9dAdxNzC39zAwjQL8h2VAQA8kxKRw!!/

Garriga, S. (26 de Junio de 2013). Los nuevos piratas. *La Nueva España*. Recuperado el 29 de Abril de 2016, de http://nueva-espana.vlex.es/vid/nuevos-piratas-445178618

Guardia Civil. (s.f.). Recuperado el 29 de abril de 2016, de https://www.gdt.guardiacivil.es/webgdt/la_unidad.php

Malmström, C. (s.f.). Una respuesta europea a la ciberdelincuencia. *Tribuna Libre*. Recuperado el 29 de Abril de 2016, de http://opinion-murcia.vlex.es/vid/respuesta-europea-ciberdelincuencia-362484182

Organización para la Cooperación y Desarrollo Económicos (OCDE). (s.f.). Recuperado el 29 de abril de 2016, de http://www.oecd.org/centrodemexico/laocde/

Rubio Alamillo, J. (1 de junio de 2014). *Clonación de discos duros en el peritaje informático.* Recuperado el 29 de abril de 2016, de http://peritoinformaticocolegiado.es/clonacion-de-discos-duros-en-el-peritaje-informatico

Unión Europea: Sección de la Escuela Europea de Policía. (s.f.). Recuperado el 29 de abril de 2016, de http://europa.eu/about-eu/agencies/regulatory_agencies_bodies/pol_agencies/cepol/index_es.htm