Anuario Jurídico y Económico Escurialense, **XLVII (2014) 209-234 / ISSN: 1133-3677**

Cibercrimen: particularidades en su investigación y enjuiciamiento

Cybercrime: particularities in investigation and prosecution

Dra. María Concepción RAYÓN BALLESTEROS
Universidad Complutense de Madrid

José Antonio GÓMEZ HERNÁNDEZ
Abogado y Socio Director de Azertia Abogados

Resumen: Recorrido general sobre el cibercrimen, desde la perspectiva de la investigación y persecución junto con sus principales especialidades.

Abstract: This article is a basic overview of the cybercrime from the perspective of the investigation and prosecution and with its major specialities.

Palabras clave: Nuevas Tecnologías de la información y las comunicaciones (TIC), ciberdelincuencia, cibercrimen, delincuencia organizada, investigación, enjuiciamiento.

Keywords: information and communication technologies (ICT), cyberdelinquency, cybercrime, organized delinquency, investigation, prosecution.

Sumario:

Recibido: diciembre 2013.
Aceptado: enero 2014.

I. LA CIBERDELINCUENCIA Y LA DIFICULTAD DE SU PERSECUCIÓN

El desarrollo de Internet y de las nuevas tecnologías asociadas a la red relacionadas con la información y las comunicaciones hacen del ciberespacio un nuevo lugar para la perpetración de distintos ataques a bienes jurídicos tan importantes como la intimidad, el honor, la propiedad, la libertad sexual y hasta la integridad física y la vida. Aunque la mayoría de las conductas no son, en esencia, algo nuevo en sí mismas la extraordinaria particularidad del medio con el que se cometen, o sobre el que actúan, confiere a estas conductas una especial configuración que obliga a romper los esquemas clásicos para su investigación y enjuiciamiento.

Afortunadamente el Derecho Penal y el Derecho Procesal Penal han evolucionado para enfrentarse a ese nuevo cauce de ejecución delictiva que se desarrolla en un ámbito virtual y tecnológico, diferente al modelo tradicional de criminalidad física, individual e interpersonal, ya que cuestiona los axiomas vigentes.

Precisamente por esto consideramos de interés realizar en este artículo una especial referencia, desde el punto de vista procesal, a las más importantes particularidades que ofrece la investigación y enjuiciamiento de estas conductas delictivas comprendidas bajo el término cibercrimen.

Se entiende por "ciberdelito"[1] o "cibercrimen" cualquier infracción punible, ya sea delito o falta, en el que se involucra un equipo informático o Internet y en el que el ordenador, teléfono, televisión, reproductor de audio o vídeo o dispositivo electrónico, en general, puede ser usado para la comisión del delito o puede ser objeto del mismo delito.

[1] Sobre la diferencia entre el delito informático (que se vale de elementos informáticos para la perpetración) y el ciberdelito (que se refiere a una posterior generación delictiva vinculada a las TIC en el que interviene la comunicación telemática abierta, cerrada o de uso restringido) puede verse ROMEO CASABONA, Carlos. "De los delitos informáticos al cibercrimen. Una aproximación conceptual y político-criminal" en *El cibercrimen nuevos retos jurídico-penales, nuevas respuestas político-criminales*. Editorial Comares. Granada 2006, pp. 1-42.

Es evidente que para hacer frente a esta forma de delincuencia se precisa realizar un enfoque supranacional, con unidades policiales de investigación especializadas y dotadas de los medios técnicos necesarios para la efectividad de su trabajo e, igualmente, se hace preciso un enjuiciamiento rápido y especializado de este tipo de conductas.

En este sentido el Convenio sobre Ciberdelincuencia, firmado en Budapest el 23 de noviembre de 2001, supone la respuesta a la necesidad de tener medios eficaces de cooperación para la lucha contra la cibercriminalidad. Se refiere al desarrollo y la utilización, cada vez mayor, de las Tecnologías de la Información y la Comunicación, así como la necesidad de aplicar una política penal común, encaminada a proteger a la sociedad frente a la este nuevo tipo de delincuencia, adoptando y armonizando una legislación adecuada en todos los países y manteniendo una política de cooperación internacional.

El Convenio contempla expresamente los delitos informáticos y define los tipos penales que han de considerarse para cada uno ellos: delitos contra la confidencialidad, la integridad, y la disponibilidad de los datos y sistemas informáticos, delitos relacionados con el contenido, delitos relacionados con infracciones de la propiedad intelectual y derechos afines[2]. Para completar la materia en 2003 se promulgó la firma del Protocolo Adicional al Convenio de Ciberdelincuencia del Consejo de Europa criminalizando los actos de racismo y xenofobia relacionados con las nuevas tecnologías.

Por lo que respecta a nuestro país en concreto hay que destacar que en el Código Penal no se contempla expresamente el concepto de ciberdelito ni delito informático en ningún capítulo en concreto, sino que se definen las distintas conductas delictivas en las que interviene de alguna manera una actividad relacionada con las nuevas tecnologías de la información y las comunicaciones. Así se identifican como delitos informáticos aquellos en los que el nexo común alrededor del cual se producen es un ordenador o un dispositivo electrónico con conexión a Internet, bien porque el objeto sobre el que recae la conducta es el propio sistema, el programa informático o el equipo, bien porque ese sistema es utilizado como medio a través del cual se realiza la conducta delictiva o bien porque el bien jurídico protegido es la integridad de la información, la confidencialidad de la misma o los datos y los sistemas o programas informáticos[3].

---

[2] El Convenio se refiere especialmente a los delitos de acceso ilegal, interceptación ilegal, violación de la integridad de datos y sistemas, violación de dispositivos, falsificación informática, fraude informático, pornografía infantil y violaciones del derecho de autor.

[3] Dentro de las figuras delictivas más habituales en las que participan las nuevas tecnologías encontramos los relacionados con falsedades documentales, revelación de secretos, publicidad

La L.O. 15/2010, de 22 de junio de 2010, por la que se modifica la L.O. 10/1995, de 23 de noviembre, del Código Penal[4] introdujo algunos cambios en la materia de manera que en la actualidad podemos hablar de los siguientes tipos de ciberdelitos: las amenazas, los delitos de exhibicionismo y provocación sexual, los delitos relativos a la prostitución y corrupción de menores, los delitos contra la intimidad, los delitos contra el honor, las estafas, las defraudaciones de fluido eléctrico y las defraudaciones en telecomunicaciones siempre y cuando se utilice un mecanismo para la realización de la misma, o alterando maliciosamente las indicaciones o empleando medios clandestinos, los daños, los delitos relativos a la propiedad intelectual, los delitos relativos a la propiedad industrial, los delitos relativos al mercado y a los consumidores. Hay supuestos que no se encuentran específicamente tipificados en el Código Penal sino que hay que acudir a la legislación complementaria que regula la sociedad de la información[5] donde cada vez se encuentran mejor tipificadas estas infracciones: en materia de protección de datos personales, en cuestiones de la sociedad de la información y envío de correos electrónicos, etc.

Sin embargo hay que destacar que la fenomenología delictiva vinculada a las nuevas tecnologías de la información y las comunicaciones es cada vez más variada y abundante y que cualquier regulación queda pronto anticuada, porque sus formas de perpetración van cambiando con el tiempo adaptándose a las nuevas posibilidades que ofrece el estado de la técnica. Ciertamente la realidad delictiva siempre va por delante de la regulación legal y la correspondiente sanción punitiva de las conductas reprobables pero, en estos casos en los que intervienen las nuevas tecnologías, muchísimo más dada la rapidez del desarrollo tecnológico[6], la facilidad del intercambio de la información, la comunicación

engañosa, vulneración de derechos de autor, daños informáticos, estafas electrónicas, conductas relacionadas con la intimidad y la libertad de expresión y vulneraciones relacionadas con la protección de datos y los correos electrónicos. Existen otras conductas que, si bien no se encuentran incluidas dentro del Código Penal, merecen un reproche social al suponer un mal uso de la red de redes, es el caso de los usos comerciales no éticos como el *spamming*, los actos parasitarios que interrumpen las comunicaciones y las obscenidades en comunicaciones tanto públicas como privadas. Algunas de estas conductas requerirán en el futuro una regulación interna e internacional para ser eficaces.

[4] La citada reforma del Código Penal introduce mediante el artículo 183 bis la figura internacionalmente denominada "*child grooming*", debido al creciente empleo de Internet y tecnologías de información para los abusos sexuales con menores e incorpora los delitos informáticos como conducta típica. Además se han clasificado las conductas punibles en dos grupos: relativas a los daños y respecto al descubrimiento y revelación de secretos.

[5] Ley de Servicios para la Sociedad de la Información y de comercio electrónico, Ley Orgánica de Protección de Datos , Ley sobre conservación de datos de comunicaciones electrónicas, Ley de impulso a la Sociedad de la Información, Ley General de Telecomunicaciones, Ley de Propiedad Intelectual, Ley de Firma Electrónica.

[6] Pueden cometerse por cualquier vía o canal, ya sea el correo, chats, P2P, las redes sociales, blogs o sms.

inmediata entre lugares lejanos, la fugacidad de las acciones y la facilidad para conseguir su anonimato, la dificultad para identificar las huellas digitales, la fácil alteración de los rastros de la comisión de unos hechos, dificultad en la detección y la persecución de las conductas dañosas, el carácter transnacional de estas conductas delictivas junto con su insuficiente regulación legal y la escasa conciencia de los usuarios sobre la necesidad de mantener unas mínimas medidas preventivas de seguridad.

Efectivamente, todos estos factores facilitan la impunidad de estas conductas. Y a ello hay que añadir aspectos jurídicos tales como la problemática derivada de la determinación espacial de la ley penal, el tribunal competente o la dificultad de practicar las pruebas tradicionalmente utilizadas para identificar el rastro de la conducta delictiva.

Como hemos indicado más arriba en este breve artículo plantearemos las cuestiones más importantes relacionadas con la investigación y el enjuiciamiento de estas conductas para la efectiva persecución de las mismas. Y para empezar conviene destacar que, desde nuestro punto de vista, merecen especial consideración las particularidades que presentan estos delitos en la forma de realizar algunas de las averiguaciones relacionadas con el hecho punible y su autor y en la concreción sobre la prueba que debe desarrollarse en el juicio para conseguir convencer al juzgador sobre la certeza de los hechos y la responsabilidad del autor y, por eso, prestaremos especial atención a estas cuestiones.

Desde nuestro punto de vista hay que insistir que, igual que aprendemos a circular en un vehículo de motor o a montar en bicicleta o en barco, también todos, mayores y pequeños, tenemos que enseñar/aprender a navegar por Internet, con las debidas precauciones, para tratar con personas a las que no conocemos, para no proporcionar datos que nos coloquen en una situación vulnerable que pueda perjudicarnos[7]. En resumen, queda pendiente por realizar una importante labor de concienciación a todos los internautas sobre la necesidad de navegar seguros en la red y en la conveniencia de protegerse frente a posibles riesgos y ataques que son muchos y muy variados en su tipología y sus efectos.

Hay que llamar la atención sobre el hecho de que la sociedad de la información se caracteriza por la ausencia de fronteras y la inmaterialidad de la comunicación con lo que los límites temporales y espaciales no existen dificultando la detección, investigación y persecución de estas conductas.

[7] Los delitos en los que intervienen las TIC presentan una serie de especialidades que se concentran en su dificultad de persecución, en problemas de colaboración procesal al denunciarse exclusivamente el 1 por 100 de los casos, y en cuestiones relacionadas con la dificultad probatoria de este tipo de delincuencia.

Y en este sentido, a efectos procesales, hay que matizar que la conducta delictiva puede tener su origen en uno o varios países y los resultados producirse en otro u otros, incluso puede resultar difícil determinar dónde se ha cometido la acción o por parte de quién. Obviamente ésto afecta a la **competencia jurisdiccional, a la ley penal aplicable y al procedimiento** que se tramitará para su investigación y enjuiciamiento, ya que la regla general tradicional se refiere al lugar de comisión del delito o *locus comissi delicti* (principio de territorialidad) contenido en la Ley Orgánica del Poder Judicial.

- En los delitos en que la acción y el resultado se produce dentro de un mismo Estado resulta aplicable la ley de ese Estado, cualquiera que sea la nacionalidad del autor. Aún en estos casos la complejidad es considerable pues para determinar el juzgado competente no está claro cual es el criterio aplicable: el domicilio del querellado, el lugar en el que se ejecutó el delito, el de ubicación del servidor, aquel en el que se descubrieron las pruebas materiales, el lugar en que se iniciaron las actuaciones procesales, el lugar en el que se produjeron los daños, etc. En estos casos habrá que referirse en principio al lugar en que se perpetró la acción.

- Mayores problemas surgen con los delitos perpetrados a distancia, muy frecuentes en Internet, y en los que la acción y el resultado se producen en diferentes países[8]. La doctrina y la jurisprudencia se han manifestado más favorables a apreciar la teoría de la ubicuidad que tiene en cuenta como lugar de comisión del delito tanto el lugar en el que se ha producido la acción como el resultado dañoso.

- Los problemas se plantean también cuando la actividad se perpetra en otro Estado pero tiene sus consecuencias en España, ya que existe un celo tradicional en la mayoría de los países para autorizar a que otro Estado juzgue a un ciudadano propio. Además, en muchas ocasiones, la conducta delictiva se puede haber llevado a cabo en un país con una legislación incompleta o permisiva con respecto a conductas nocivas cometidas a través de las TIC, o que no poseen medios de detección y persecución ilimitados o que no han ratificado ningún tratado de extradición, lo cual dificulta aún mucho más la investigación y enjuiciamiento de estas conductas.

[8] En este caso podría aplicarse la teoría de la actividad (que entiende cometido el delito en el lugar en que se lleva a cabo la conducta delictiva), la del resultado (que mantiene que el delito se comete en el lugar en el que tiene lugar el resultado externo) o la teoría de la ubicuidad (para la cual el delito se entiende cometido en el lugar en que se lleva a cabo la actividad o se manifiesta el resultado).

- En los casos en que la acción se produce en un Estado y el resultado en otro los datos de los países que atraviesa la comunicación (delito en tránsito) han de considerarse irrelevantes, como también es irrelevante el lugar en que radica el proveedor de acceso a la red o el prestador de servicios. En este caso el principio de territorialidad no aporta soluciones satisfactorias. Por eso se acude a la exigencia de un punto de conexión con el país en el que se ha producido el resultado y se aplica el principio de oportunidad, que implica que el delito no se haya juzgado en otro país.

II. INVESTIGACIÓN

Generalmente la investigación suele iniciarse con una **denuncia** realizada por los particulares afectados por la conducta delictiva o por solicitud al juzgado para que libre mandamiento dirigido a los proveedores de acceso a Internet para que informen sobre los datos que posean para identificar a los usuarios de las direcciones IP y las líneas desde las que se efectúan las conexiones así como sus titulares. Seguidamente el **tribunal** iniciará el procedimiento que corresponda y puede incluso llegar a autorizar la diligencia de entrada y registro en el domicilio o sede del titular de la línea, levantando acta el secretario judicial. Con esta diligencia de investigación se accede al ordenador y a los ficheros para obtener copia de los mismos.

Debido a que la perpetración de delitos tecnológicos se está incrementando exponencialmente se han creado unidades especiales de investigación en el Cuerpo de Policía Nacional, de Guardia Civil y en algunas Policías Autonómicas, e incluso se ha creado en 2011 una Fiscalía especializada en delitos informáticos[9].

Según el art. 299 de la LECrim, la fase de investigación criminal es el conjunto de actuaciones encaminadas a preparar el juicio y a hacer constar la perpetración

[9] Instrucción 2/2011 del Fiscal General del Estado, por la que se crea la denominada Fiscalía de Criminalidad Informática. Los delitos que investiga se estructuran en tres categorías:

(i) Delitos en los que el objeto de la actividad delictiva son los propios sistemas informáticos o las TIC (sabotaje informático, acceso sin autorización a datos, programas o sistemas informáticos, revelación de secretos, etc.),

(ii) Delitos en los que la actividad criminal se sirve para su ejecución de las ventajas que ofrecen las TIC (estafas informáticas, delitos contra la propiedad intelectual, corrupción de menores y personas discapacitadas, pornografía infantil, etc.), y

(iii) Delitos en los que la actividad criminal, además de servirse para su ejecución de las ventajas que ofrecen las TIC, entraña especial complejidad en su investigación que demanda conocimientos específicos en la materia (falsificación documental, injurias y calumnias contra funcionarios públicos, amenazas y coacciones, delitos contra la integridad moral, apología o incitación a la discriminación, el odio y la violencia, justificación de los delitos de genocidio, etc.).

de los delitos con todas las circunstancias que puedan influir en su calificación y la culpabilidad de los delincuentes y, junto con las medidas cautelares, asegurar sus personas y las responsabilidades pecuniarias de los mismos.

Resulta obvio que en el mundo tan técnico y avanzado de las nuevas comunicaciones se hace necesario recurrir a expertos que asesoren en el modo de desarrollar la investigación por lo que los costes y el tiempo se incrementan. En este sentido se hace necesaria la especialización de los agentes para dar respuesta a las soluciones que la sociedad demanda contra la delincuencia informática. Igualmente se hace necesario que las Fuerzas y Cuerpos de Seguridad del Estado dominen herramientas y conocimientos para poder detectar y hacer seguimiento de las conductas delictivas para identificar a su autor. En todo caso resulta importante destacar que los infractores suelen conocer muy bien el medio empleado para la comisión delictiva por lo que se convierten en especialistas para borrar las huellas o rastros que quedan en la red hasta conseguir con frecuencia su completa impunidad.

Además en este tipo de conductas destaca su habitual carácter transfronterizo y su extraterritorialidad lo que posibilita que se cometan en un lugar y se produzcan los resultados en otro lugar distinto o que se cometan simultáneamente en diferentes lugares, a veces muy distantes entre si, lo que dificulta también la investigación y la actuación de las autoridades policiales y judiciales.

2.1. *La importancia de los datos de tráfico*

El anonimato que ofrece Internet y la posibilidad de ejecución de conductas dañosas a distancia dificultan la detección de los posibles delitos. Tampoco es fácil delimitar quien es el autor de dichas conductas. Por eso para investigar una comunicación delictiva realizada a través de las TIC lo que hay que determinar los **datos de tráfico**[10] y los rastros de navegación, ya que aportan información fundamental sobre el origen de una comunicación y las idas y venidas de la misma entre los distintos dispositivos a través de la red.

[10] Internet está constituido por un gran número de ordenadores conectados entre sí formando pequeñas redes que, a su vez, se enlazan en la red de redes. El primer paso que realiza un usuario para entrar en Internet es comunicar su equipo con un Proveedor de Acceso a Internet (ISP) a través de un operador de telecomunicaciones. El proveedor asigna un identificador o número diferente IP (*Internet Protocol*) para identificar a cada usuario. Los números IP son únicos, están compuestos por cuatro grupos de números naturales que puede adquirir el valor de 0 hasta 225 separados entre si por puntos, estos dígitos combinados permiten unos 4.000 millones de combinaciones diferentes. Para que dos ordenadores distintos con sistemas operativos diferentes se intercambien información entre sí se han diseñado unos protocolos de comunicación encapsulando la información en capas o paquetes, según los servicios, que se denominan "datos del tráfico".

Los datos de tráfico no siempre se localizan fácilmente. Generalmente se almacenan por los sistemas y aplicaciones informáticas y su conservación y el tiempo de ésta es configurable por el usuario que maneja el sistema. Para conseguir dichos datos tendremos que conocer el número IP[11] en el momento de conectarse a Internet, el momento concreto de acceso para la comisión del hecho dañoso, así como identificar el ordenador, su ubicación, el abonado de la línea telefónica o el contrato de acceso.

Como regla general, realizando la investigación sobre los datos de tráfico, se podrá llegar a ubicar el equipo y a identificar al abonado[12], que no al usuario, pues puede ser otra persona diferente, por lo cual se hace necesario realizar la clásica vigilancia policial apoyada en los procedimientos comunes como vigilancia ordinaria, intervenciones telefónicas, rastreo de IP, etc.

En este sentido hay que destacar que los proveedores de servicio de Internet prestan una información determinante para la investigación, ya que los técnicos policiales necesitan básicamente los siguientes datos:

- La dirección IP asignada al sospechoso por el proveedor y los datos contractuales (nombre y dirección) junto con la hora, fecha y duración de la comunicación, la concreta transacción o intercambio realizado.
- La localización geográfica desde la que se conecta el sospechoso con el proveedor.
- Las cuentas corrientes asociadas al pago de los servicios.
- El número de teléfono de origen y destino de las comunicaciones realizadas por el sospechoso.
- La concreta transacción o intercambio ilícito.
- La copia de los ficheros de que disponga el sospechoso en su espacio web,
- Las llamadas perdidas con determinación de su hora, duración y frecuencia.
- El tipo de servicio telefónico empleado por el sospechoso.
- El identificador del equipo en los teléfonos móviles.
- Los datos de fecha y momento de activación de la tarjeta prepago de móviles, etc.

[11] TCP/IP -*Transmisión Control Protocol*o *Internet Protocol*- que constituyen la familia de protocolos que hacen posible la interconexión y tráfico de red en Internet. Cada ordenador tiene asignada una dirección IP en el momento de conectarse a Internet por lo que su seguimiento no es complejo *a priori*. Sin embargo los actuales protocolos IP no garantizan siempre la determinación de la dirección del emisor ya que la misma puede ser manipulada.

[12] El contenido de las comunicaciones postales, telegráficas y telefónicas está protegido constitucionalmente por lo que nunca podrá conocerse el exacto contenido de las comunicaciones realizadas a través de las TIC.

A partir de los datos obtenidos puede llegarse a determinar el lugar de comisión de los hechos, la máquina de origen, los autores de la conducta y el tipo de conducta punible que se ha perpetrado.

Muchos autores han puesto de manifiesto que el hecho de mejorar la seguridad implica la pérdida de privacidad e intimidad lo cual supone un elemento importante a tener en cuenta. Por eso hay que destacar que los datos de tráfico están considerados por la Ley Orgánica de Protección de datos como datos reservados de carácter personal lo cual obliga a su tratamiento adecuado, conforme a la legislación específica.

2.2. *Medidas de investigación más eficaces*

Podemos destacar que las medidas de investigación más eficaces para perseguir las conductas relacionadas con las TIC son:

- La coordinación de entradas y registros en diferentes partidos judiciales[13] a través de la vía del auxilio judicial.
- La infiltración de agente encubierto en la red de la organización criminal.
- La interceptación de las comunicaciones para descubrir sus componentes.
- El método de actuación, y el destino final de los ingresos ilícitamente obtenidos.
- La utilización de aparatos de escucha y filmación de actividades.
- Las informaciones provenientes de delatores y confidentes.
- La incautación de equipos.
- La recuperación de *logs*, mensajes o *backups*.
- El volcado de datos de dispositivos en los que se almacena la información.
- Y en general la recogida y conservación de los efectos relacionados con el ilícito.

[13] Para que se acuerden estas medidas de investigación, que restringen derechos fundamentales reconocidos en la Constitución, el Tribunal Constitucional exige la observancia del principio de proporcionalidad de manera que es necesario constatar tres condiciones:

- Si tal medida es susceptible de conseguir el objetivo propuesto (juicio de idoneidad),
- Si además es necesaria en el sentido de que no exista otra medida más moderada para la consecución de tal propósito con la misma eficacia (juicio de necesidad)
- Si la misma es ponderada y equilibrada por derivarse de ella más beneficios y ventajas para el interés general que perjuicios sobre otros bienes o valores en conflicto (juicio de proporcionalidad en sentido estricto).

La proporcionalidad de la medida debe ser valorada por el juez de guardia al que se solicita en función del hecho delictivo presuntamente cometido que debe ser grave, lo cual dificulta en muchas ocasiones la investigación de determinados delitos. La duración del registro domiciliario también es un problema a tener en cuenta, pues el proceso de volcado y de análisis inmediato se suele prolongar más en el tiempo.

Hoy en día, como consecuencia del avance de las nuevas tecnologías, existen también eficaces herramientas de ciber-rastreo o monitorización consistentes en el uso de programas informáticos de *software* para la detección de rastros delictivos en la red[14] y ofrecen buenos resultados.

Todas estas medidas de investigación tienen que realizarse de acuerdo con los mandatos y garantías legales establecidos para cada caso en la legislación contenida en la Ley de Enjuiciamiento Criminal. Su incumplimiento generará la falta de validez de las investigaciones y de las consiguientes pruebas relacionadas en el acto del juicio, por lo que resulta fundamental cumplir escrupulosamente todas las disposiciones legales previstas[15].

Desde nuestro punto de vista, y a efectos de nuestro estudio, sería conveniente destacar la necesidad de adaptación legal de las medidas de investigación a las nuevas formas de delincuencia tecnológica, puesto que la rapidez con que se produce el resultado dañoso, el efecto multiplicador del mismo a través de la red y el anonimato electrónico hacen necesario un mayor control y una mayor contundencia para la efectiva persecución de este tipo de delincuencia.

2.3. *Fases generales de la investigación*

En general el desarrollo de la investigación en el ámbito de la delincuencia tecnológica suele sistematizarse en tres fases a las que nos referiremos brevemente por separado, por perseguir objetivos diferentes y consecutivos:

- **Fase previa,** para comprender qué ha pasado, en qué ha consistido el delito y cómo se ha podido perpetrar;
- **Fase de investigación propiamente dicha,** para esclarecer quién es el posible responsable y si ha perpetrado efectivamente alguna acción punible;
- **Fase incriminatoria,** en la que se obtienen y aseguran las pruebas del delito para la posterior fase de enjuiciamiento.

[14] Sobre este tema hay publicado un artículo muy interesante de VELASCO NÚÑEZ, E., "Novedades técnicas de investigación penal vinculadas a las nuevas tecnologías", en *Revista de Jurisprudencia*, número 4, año 4 (2011) 1 a 8.

[15] Conviene destacar que las actuaciones técnicas que deben practicarse para la investigación de este tipo de delitos requieren personal técnico adecuado con objeto de evitar que los elementos obtenidos sean invalidados en posibles procesos judiciales. Sin embargo no existe una reglamentación o normativa que determine las labores propias del análisis forense digital. Generalmente se siguen una serie de prácticas reconocidas internacionalmente para documentar y razonar los análisis. Se encuentra muy extendida la base o guión CDP4F *Codes of Practices for Digital Forensics*, aunque existen otros documentos empresariales o de organismos policiales.

La **fase previa** se inicia con el conocimiento del delito por parte de las autoridades y organismos encargados de la investigación criminal, generalmente a través de la denuncia presentada por las víctimas, afectados o perjudicados por el delito[16].

Comprobar que se ha perpetrado el delito y cómo se ha perpetrado es una de las fases más complejas de toda la investigación por lo que se suele solicitar la ayuda de los servidores de la red que pueden localizar los rastros del delito de forma muy rápida según lo que hemos destacado anteriormente. Además los servidores suelen guardar un registro de sucesos de lo que ocurre (*logs*)[17], que contienen información de gran utilidad durante las investigaciones, como por ejemplo los equipos que han tenido asignada una determinada IP y en qué períodos, las fechas y archivos pedidos, la contestación, la página desde la que se pide el archivo, la información sobre la versión del navegador, el terminal del usuario, los equipos que han navegado, a qué páginas y cuando, las comunicaciones relacionadas con un incidente, los accesos a los servidores, los intentos de acceso, las acciones sospechosas, etc.

A este respecto tenemos que destacar que los ordenadores personales no suelen guardar *logs* por lo que, en la mayoría de las ocasiones, hay que realizar *back-up´s* para detectar las evidencias del delito. Más adelante especificaremos la forma de realizar este proceso para que cuente con todas las garantías exigidas legalmente y pueda llegar a suponer una prueba incriminatoria en el juicio, si llegara a ser necesario.

La **fase de investigación propiamente dicha** consiste en llevar a cabo toda una serie de operaciones técnicas para intentar determinar como se ha cometido el delito, y para comprender su forma de perpetración, así como su posible vinculación con otras posibles conductas delictivas. De esta forma se pueden llegar a identificar sus conexiones y a precisar los datos de tráfico afectados para identificar al abonado titular de la conexión[18].

Una vez realizadas las oportunas pesquisas policiales se llega a identificar un equipo y un abonado pero no al usuario concreto que presuntamente cometió un

[16] Y también tenemos que destacar que, una vez perpetrados los hechos presuntamente delictivos, muchas veces no se denuncian por desconocimiento de los padres de su realización o, conocidos por los progenitores no se denuncian para intentar preservar la estabilidad emocional y el anonimato de sus hijos.

[17] El *log* es una de las principales herramientas para conocer los detalles de las operaciones realizadas en el sistema y por tanto para la investigación de un eventual delito. Esto suscita importantes riesgos para la intimidad de los ciudadanos al contravenir el derecho al secreto en las comunicaciones.

[18] En algunos casos la vanidad del delincuente, le suele llevar a firmar sus actuaciones, lo que suele resultar de gran ayuda para llevar a cabo la investigación criminal.

acto ilícito, que podrá ser el propio abonado o un familiar o un usuario accidental o un usuario remoto, etc. Por tanto todos estos aspectos a los que nos hemos referido no serán prueba objetiva en un juicio, sino un indicio de uso de un equipo informático.

A este respecto la complejidad aumenta con la existencia de troyanos o caballos de Troya que se alojan en el interior de un "programa inocente" y se ocultan en el ordenador permitiendo el control remoto del equipo afectado como un "zombie" llegando a crearse redes de ordenadores infectados (*botnets*) que sirven de plataforma para la comisión de gran cantidad de hechos delictivos[19].

La **fase incriminatoria** comprende la intervención y aprehensión de los ordenadores -*hardware* y *software* concreto- generalmente mediante la entrada y registro domiciliario en el lugar en que se encuentren, así como la ulterior y determinante redacción de los informes periciales.

Para **intervenir y aprehender los ordenadores o dispositivos** con que se ha cometido el delito, así como los indicios relacionados con su comisión, se debe realizar una entrada y registro con un mandamiento judicial:

- Por un lado se interviene el material y dispositivos informáticos susceptibles de contener indicios de criminalidad: concretamente se intervienen todos los dispositivos informáticos y tecnológicos, así como los documentos físicos necesarios para el funcionamiento de los dispositivos intervenidos (manuales, instrucciones, anotaciones de contraseñas, pliegos de datos etc.). Se hace necesario intervenir todo el equipo completo (disco duro, monitor, teclado, ratón, *router*, memorias externas, *pen drive*, tarjetas de almacenamiento, etc.). Es muy importante intentar mantener la integridad de todo el equipo intervenido para lo cual se realizará su precintado así como su plena identificación en el acta de entrada y registro confeccionada por el secretario judicial. En muchas ocasiones estas operaciones no se realizan de la forma adecuada lo que

[19] En estos casos un conjunto de equipos informáticos cuyo número puede oscilar entre cientos y miles que pueden ser controlados maliciosamente por control remoto ejecutando las órdenes que recibe. La organización funciona en forma de estructura piramidal en ocasiones muy compleja para complicar la detección de los máximos responsables: en la cúspide se encuentra el *script writer* que es el auténtico *hacker* creando un código malicioso. Seguidamente se encuentran los *herders* que pueden controlar varios *botnets* y que reciben una cantidad económica por sus servicios. Finalmente se encuentran los ordenadores que ejecutan las órdenes en el momento indicado y que se denominan *bots* o zombies. En estas organizaciones se suelen localizar también otra serie de integrantes que se encargan de cobrar el producto de sus ataques y repartirlo entre cada uno de los participantes. El servidor a través del cual se controlan todas las operaciones suele estar localizado en un país en el que la legislación es muy permisiva con este tipo de hechos por lo que su actividad no podrá ser suspendida aun cuando sea detectada.

genera problemas, en fases posteriores de enjuiciamiento, para conseguir probar adecuadamente los hechos en el seno del procedimiento correspondiente.

- Por otro lado se interviene indicios que puedan vincular al usuario y al equipo con la comisión del hecho delictivo investigado, así como de los instrumentos y efectos relacionados.

Otra medida de investigación que puede llevarse a cabo es la de **inspección ocular** por parte del juez, para reconocer el lugar en el que se encuentran los indicios materiales del delito o los lugares por los cuales haya podido circular la comunicación delictiva. Aunque en general este tipo de investigaciones no suelen ofrecer buenos resultados en estos casos pueden ser de interés para lograr formar la convicción del juzgador sobre unos hechos supuestamente delictivos.

En todo caso conviene **aislar el lugar del crimen y el ordenador o dispositivo electrónico** desde el que se ha producido la comunicación, para poder buscar los indicios que permitan entender lo que ha sucedido y desarrollar la investigación criminal.

Por eso resultan fundamentales las primeras horas de **intervención de los equipos** y las **primeras declaraciones obtenidas del entorno del sospechoso** para conseguir los indicios necesarios y justificar la detención. En este caso se realizan **interrogatorios** dirigidos a esclarecer la comisión del hecho delictivo.

Posteriormente se procede al análisis de los efectos intervenidos para lo cual se realiza una copia previa de la información denominada "**volcado**", siempre salvaguardando el original. Esta operación se realiza para conocer, en el momento de la intervención judicial, el contenido real del ordenador intervenido. Se efectúa una copia del soporte original, tanto del *hardware* como del *software* o de cualquiera de ellos. De esta forma no se correrá peligro de que el contenido se pierda, deteriore o altere por cualquier causa, pues resulta determinante entregar al juez el auténtico cuerpo del delito al que se refiere el art. 334 de la LECrim y por ello debe preservarse intacto con mucho cuidado.

En todo caso resulta determinante **garantizar la cadena de custodia** del "volcado" realizado por lo cual debe realizarse en presencia de fedatario público -el secretario judicial- que franqueará los precintos impuestos durante la intervención. Por eso algunos cuerpos investigadores de los delitos telemáticos realizan este "volcado instantáneo" durante el propio acto de registro domiciliario, para que el secretario de fe de su intervención y de la copia realizada.

Realizado ese "volcado" debe **mantenerse el precintado de los equipos intervenidos** para garantizar la cadena de custodia de la prueba. Se realizará

el análisis pericial y se almacenarán los discos duros de forma que se garantice su integridad, para lo cual hay que guardar una serie de precauciones mínimas evitando golpes que dañarían la posterior lectura de los dispositivos. A efectos prácticos se pueden mantener los mismos en poder del secretario judicial, aunque siempre a disposición judicial.

El **análisis pericial de los investigadores** se realiza sobre el "volcado" con una doble finalidad:

- Localizar e identificar las evidencias electrónicas para constituir la prueba indiciaria,
- Localizar e identificar las evidencias que permitan vincular el equipo, el usuario, el abonado y los datos.

Para realizar este análisis no existen unas herramientas preestablecidas judicialmente, sino que cada Cuerpo de Seguridad del Estado utiliza las suyas propias de manera que se genera cierta inseguridad jurídica tanto para los propios procesados como para los investigadores[20].

Este análisis al que nos referimos resulta determinante y puede tardar semanas e incluso meses en ser culminado definitivamente, ya que depende del grado de complejidad que haya alcanzado la comisión del hecho delictivo, de los conocimientos informáticos y las técnicas de ocultación de las actividades delictivas, del tipo de dispositivo empleado, etc.

A este respecto hay que destacar que el análisis que se realiza no siempre es concluyente, de manera que los indicios que se obtienen por separado no significan nada pero, en su conjunto e interpretados de manera interrelacionada, pueden constituir la prueba para un juicio como luego veremos. **Con el conjunto de indicios obtenidos en todos los análisis efectuados se elabora un informe técnico de naturaleza policial** para que, de forma comprensible para el juez, se pueda explicar la comisión del hecho delictivo por una persona concreta. En ese informe se deberá realizar también una descripción, lo más detallada posible, de las operaciones practicadas para llegar a las conclusiones finales que se contengan en el mismo.

III. ENJUICIAMIENTO Y PRUEBA

El entorno de la ciberdelincuencia está produciendo un cambio radical en las estrategias de los abogados que deben presentar en los procesos pruebas

[20] En este sentido quizá sería conveniente que, de *lege ferenda,* se intentara fijar una serie de protocolos o herramientas de actuación para todos los casos.

informáticas o electrónicas, porque su gestión y sus criterios de admisibilidad cambian considerablemente si tenemos en cuenta el régimen jurídico tradicional de la prueba en cualquier tipo de proceso. En estos casos se hace necesario presentar documentos electrónicos y es preciso salvaguardar y adquirir las pruebas de una forma adecuada, de esta forma su eficacia no podrá quedar desvirtuada en el proceso, tal y como hemos referido anteriormente.

La prueba en formato electrónico se convierte así en la única solución para evidenciar la comisión delictiva y requerirá, tanto un exhaustivo análisis para demostrar ante la autoridad judicial la autoría de unos hechos así como su adecuada presentación en el seno del proceso con valor probatorio como tal. Y por eso vamos a referirnos seguidamente a la citada prueba electrónica.

3.1. *Prueba electrónica*

Como regla general en los delitos en que intervienen las nuevas tecnologías de la información y las comunicaciones la prueba pericial consistirá en realizar un análisis de los dispositivos aprehendidos, para examinar a fondo su contenido y llegar a acreditar la perpetración de los respectivos hechos.

Se puede definir la prueba electrónica[21] como cualquier información obtenida a partir de un dispositivo electrónico, o medio digital, que sirve para adquirir convencimiento de la certeza de un hecho. A pesar de su importancia la prueba electrónica sigue siendo un instrumento bastante desconocido en el ámbito judicial por parte de jueces, magistrados, fiscales y en general por los profesionales del Derecho. Por si fuera poco la regulación de la materia es imprecisa, con contradicciones y lagunas, de manera que genera disparidad de criterios con la consecuencia de que unos jueces admitan este tipo de prueba electrónica mientras que otros no la admitan.

La volatilidad característica de la prueba electrónica hace necesario que sea sustituida por unos protocolos seguros de actuación que garanticen su inalterabilidad o no manipulación por ningún movimiento, a veces tan fortuito como encender o apagar un ordenador, o intencionado por parte de los implicados en la comisión de un delito para ocultar su autoría.

[21] La prueba electrónica se convierte en el elemento fundamental de cualquier procedimiento en el que se hayan empleado medios electrónicos para la comisión delictiva. Y en el seno del mismo deberá reconstruirse la cadena de acontecimientos llevados a cabo ilícitamente, lo cual suele resultar muy complejo.

Desde nuestro punto de vista se hace necesaria también la formación adecuada de todos los profesionales del derecho en materia de prueba electrónica para garantizar su admisibilidad en el proceso al comprender y apreciar sus vulnerabilidades, pero también sus ventajas y garantías. De esta forma la prueba electrónica llegará a considerarse un medio de prueba más, junto a los tradicionalmente reconocidos en nuestra legislación.

3.2. *Perito informático*

El perito informático en el proceso penal va a intervenir de forma determinante. No es fácil precisar el concepto de perito informático[22]. Podemos considerar como tal a la persona que, sin ser parte en el proceso, emite declaraciones sobre hechos que tienen carácter procesal en el momento de su captación, para cuyo conocimiento o apreciación son necesarios o convenientes conocimientos informáticos.

Será en la fase de juicio donde realizará la ratificación de su informe, a los efectos de que tenga valor probatorio y sea tenido en cuenta por el juez para dictar la sentencia.

Hay que destacar que las pruebas en este tipo de delitos suelen ser realizadas por organismos oficiales dependientes de las Fuerzas y Cuerpos de Seguridad del Estado (Departamento de delitos telemáticos de la Guardia Civil o Brigada de Investigación Tecnológica de la Policía Nacional) por lo que gozan de la presunción de neutralidad e imparcialidad. Este tipo de informes cuentan con todas las garantías técnicas siempre y cuando se confeccionen por ingenieros o informáticos distintos de los que han hecho la intervención del material o equipo informático.

3.3. *El informe pericial*

El informe pericial debe practicarse con todas las formalidades y siguiendo el procedimiento a que se refieren los art. 723 a 725 de la LECrim. Debido a

[22] La Asociación de Técnicos de informática (la más importante de este tipo en nuestro país) establece un gran margen de cualificación de los peritos en este ámbito. Sin embargo en recientes normas publicadas en nuestro país se entiende por informático el ingeniero-informático aunque, en general, cualquier persona con conocimiento técnicos informáticos podría comparecer en el proceso para aportar su experiencia. El problema tiene su origen en la reciente aparición de la profesión y en la proliferación de las nuevas Tecnologías de la Información y las Comunicaciones. Además damos el nombre de informático a personas relacionadas con la informática pero que desempeñan funciones muy distintas: programador, vendedor, analista, etc.

la falta de regulación de numerosas cuestiones hay que acudir a la regulación de los artículos 456 y ss. del mismo cuerpo legal que se refiere a la pericial realizada en fase de instrucción o investigación.

Para que el informe pericial sea considerado como prueba de cargo, a efectos de destruir el principio de presunción de inocencia, es necesario que se practique en el juicio oral, bien directamente o bien por ratificación de su autor en dicho acto[23]. La Sala Segunda del TS es consciente que esta interpretación estricta de la prueba pericial llevaría a un continuo trasiego de peritos por los juzgados y tribunales, lo que resultaría especialmente problemático si se hiciera necesaria la comparecencia en juicio de los autores de los informes realizados por gabinetes policiales, colapsándose entonces el trabajo de dichos servicios. Por ello la jurisprudencia ha buscado la forma de otorgar a estos informes policiales, efectuados por organismos oficiales, eficacia probatoria sin necesidad de la citada comparecencia judicial a través de las siguientes soluciones:

1.- Sólo puede prescindirse de la ratificación cuando los informes sean emitidos por gabinetes u organismos de policía con ámbito estatal[24].
2.- Esos informes constituyen prueba documental, por lo que deben recibir el tratamiento contenido en el art. 726 de la LECrim.
3.- Otras resoluciones aluden a la doctrina de la "aceptación tácita". Según esta doctrina, los informes periciales podrían desvirtuar la presunción de inocencia sin necesidad de la comparencia a la que nos venimos refiriendo, cuando las partes acepten tácitamente el contenido de los citados informes, no contradiciéndolos en el juicio.

Las dos primeras posiciones pueden considerarse hoy abandonadas, teniendo en la actualidad plena vigencia la doctrina de la aceptación tácita, que parte de la Sentencia 24/1991 de 11 de febrero a partir de la cual el Tribunal Supremo sostiene que, cuando se trata de informes periciales o cuasi periciales sobre circunstancias de hecho fundamentales en la causa penal concreta que se tramite, practicados durante el sumario o diligencias previas, máxime cuando

[23] En este sentido la jurisprudencia ha sido muy constante y reiterativa. Destacamos en particular la STS de 13 de abril de 1991 que indica: "La doctrina jurisprudencial dominante en las sentencias del Tribunal Constitucional establece que no se puede tomar en consideración ni valorar como prueba los dictámenes periciales que no se hayan ratificado o practicado como tales pruebas en el juicio oral, pues sólo de esa manera se pueden salvar los principios constitucionales de inmediación y contradicción, entre otras podemos citar la STCo 22/88 de 18 de febrero". Vid. SSTS 26 de abril de 1990, 16 de octubre de 1990, 8 de febrero de 1991 y 14 de junio de 1991, 14 de diciembre de 1995.

[24] Las primeras sentencias del Tribunal Supremo sobre estas cuestiones son de 21 de abril de 1988, 25 de septiembre de 1988 y 12 de julio de 1989.

son realizados por organismos oficiales o por funcionarios públicos especializados al respecto, y ninguna de las partes propone prueba sobre ese extremo, lo que motiva que en el acto del juicio oral nada se practique sobre tal particular, ha de entenderse que hay una aceptación tácita por todas las partes sobre la mencionada pericial y ello permite que el juzgado o tribunal en la instancia pueda considerar como probado el hecho al que se refieren esas diligencias realizadas durante la fase de instrucción"[25].

La prueba pericial intentará poner de manifiesto la existencia de archivos con material delictivo para lo cual debe acreditarse el movimiento de entrada y salida de esta información del ordenador intervenido, así como la existencia de intercambios de ese tipo de material delictivo, por lo que resulta muy útil determinar la existencia en el sistema intervenido de carpetas de intercambiadores de ficheros (*download*) que sirvan para recibir y enviar correos electrónicos, la creación de páginas web con ese fin, detectar intercambios de este tipo de materiales, etc.

En cuanto al contenido mínimo del informe pericial realizado por la policía judicial para poder constituir prueba en fase de juicio, podríamos destacar el siguiente:

- Descripción de los elementos sometidos a análisis.
- Operaciones realizadas.
- Conclusiones razonadas obtenidas de las operaciones realizadas.

En caso de ratificarse este informe a presencia judicial será conveniente que el perito utilice un lenguaje claro y conciso tratando de responder a las preguntas: qué ha pasado, quién lo ha hecho, cómo ha sucedido, cuándo ha pasado y por qué ha pasado.

[25] Por tanto, podemos decir respecto a la prueba pericial, que la jurisprudencia ha delineado unos criterios fundamentales al respecto:

1.- Las pericias practicadas necesariamente con anterioridad a la celebración del juicio, e incluso con antelación al inicio del proceso constituyen pruebas preconstituidas que despliegan toda su validez, si no son impugnadas por ninguna de las partes y son aportadas al acervo de diligencias.

2.- Sobre los informes periciales emitidos por organismos oficiales, practicados en trámite de instrucción, si ninguna de las partes propone especialmente prueba sobre el particular, o expresamente las impugnare, debe entenderse que existe aceptación tácita por todas las partes, lo cual hace posible que la diligencia de que se trate produzca efectos de verdadera prueba de cargo, igual que si de una prueba documental se tratase.

3.- Las pruebas periciales practicadas en el sumario necesitan ser sometidas a la oportuna contradicción cuando las partes lo soliciten, pues de no efectuarse tacha alguna sobre los citados elementos, el tribunal dispondrá de ellas y puede formar su convicción legítimamente sin que sea imprescindible la ratificación de los peritos cuando no se solicita ni se cuestiona el resultado, neutralidad y competencia de los autores de la pericia, renunciándose a solicitar las explicaciones o aclaraciones que fueren pertinentes.

3.4. *La importancia de la prueba indiciaria*

Para obtener la prueba para un juicio hay que acudir en muchos casos relativos a la delincuencia informática a lo que se denomina "prueba indiciaria" que permite vincular el usuario y el hecho delictivo para realizar la incriminación concreta: según la jurisprudencia se requerirán una pluralidad de indicios, acreditados y coherentes entre sí, que mantengan un vínculo preciso y directo entre el indicio y el hecho determinante de la responsabilidad criminal conforme a las reglas de la lógica y la experiencia.

Con la prueba indiciaria es necesario que el órgano judicial precise cuales son los indicios y cómo se deduce de ellos la autoría del acusado, de tal modo que cualquier otro tribunal que intervenga con posterioridad pueda comprobar y comprender el juicio formulado a partir de tales indicios, siendo preciso, pues, que el órgano judicial explique no sólo las conclusiones obtenidas, sino también los elementos de prueba que conducen a dichas conclusiones y el *iter* mental que le ha llevado a entender probados los hechos, a fin de que pueda enjuiciarse la racionalidad y coherencia del proceso mental seguido y constatarse que el Juez ha formado su convicción sobre una prueba de cargo capaz de desvirtuar la presunción de inocencia.

3.5. *Otros tipos de pruebas en casos especiales*

Para acreditar la autoría concreta de unos hechos por parte de un infractor, especialmente en los delitos a través de las TIC en casos de ordenadores de uso compartido que serían los más complicados, serán las siguientes:

- Pericial mediante la determinación de las señas IP del usuario.
- Documental y el conocimiento de la clave del usuario y contraseña de cada uno que no puede ser conocida por terceras personas.
- Testifical como por ejemplo el uso en exclusiva de un ordenador por una persona, su uso de *nicks* o apodos, etc.
- Confesión del propio inculpado.
- Por indicios siempre que se razone de forma adecuada analizando quien percibe las cantidades provenientes del hecho delictivo, quien tiene suficientes conocimientos informáticos para perpetrar los hechos, la falsedad de las declaraciones realizadas por el imputado, etc.

IV. CONCLUSIONES SOBRE LAS PRINCIPALES DIFICULTADES PARA PERSEGUIR LOS DELITOS EN QUE INTERVIENEN LAS NUEVAS TECNOLOGÍAS

En las nuevas formas delictivas en que intervienen las tecnologías de la información y las comunicaciones existen una serie de factores que complican su investigación y enjuiciamiento. A continuación realizamos un breve planteamiento de lo que, a nuestro juicio, podría considerarse una conclusión sobre lo expuesto en este breve trabajo respecto a las principales dificultades para perseguir los delitos en que intervienen las nuevas tecnologías:

- **La tecnología facilita la perpetración de nuevas conductas dañosas y la ocultación de los rastros de las mismas.** Los continuos avances de las tecnologías de la información y comunicaciones dificultan, cada día más, la investigación y el enjuiciamiento de estos delitos. La realidad siempre va por delante de la regulación legal y la correspondiente sanción punitiva de las conductas reprobables. En consecuencia existen grandes **dificultades del legislador y del poder judicial para conocer y comprender el mundo digital** pues, su propia dinámica, sobrepasa todos los límites existentes hasta ahora. El resultado es la inadecuación y el vacío legal relacionado con algunos aspectos de la red que afectan a todo el ámbito jurídico y en particular al penológico.

- La **tipificación de las conductas resulta complicada**, pues muchas veces los hechos son tan novedosos que no están contemplados en las normas penales. El Derecho Penal se enfrenta a una criminalidad progresivamente más poderosa y peligrosa que demanda una mayor complejidad técnica y jurídica. Se hace imprescindible una política legislativa flexible, dinámica y moderna que afronte este tipo de delincuencia tan cambiante. Sería deseable que las nuevas legislaciones modernas puedan hacer frente a las múltiples manifestaciones de la ciberdelincuencia mediante la configuración de **tipos penales abiertos, dejando al margen casuísticas descriptivas, complejas y farragosas**. Quizá lo más adecuado sería realizar una reelaboración de las categorías fundamentales del derecho y del procedimiento penal, sobre los cuales se sustenta la responsabilidad criminal, para establecer tipos penales abiertos que pudieran contener los requisitos para la persecución de conductas dañosas y perjudiciales para la sociedad cualquiera que sea el estado de desarrollo de la tecnología.

- En general existe un gran **desconocimiento en el mundo judicial de la mayoría de aspectos relacionados con las nuevas tecnologías de la información y las comunicaciones** por lo que se hace precisa la formación

básica en esta materia de todos los intervinientes en el proceso para comprender el alcance de las medidas que se solicitan, de las infracciones cometidas, de la forma de perpetración de los hechos y de los mecanismos utilizados, etc. Además, al objeto de conseguir eficacia en la lucha contra este tipo de delincuencia, debería establecerse una **mayor agilidad y disposición de los Tribunales** encargados de instruir las causas, tratando de adecuarse a la realidad de los delitos informáticos.

- Igualmente debería procurarse la dotación de **recursos suficientes para la investigación de este tipo de conductas, tanto humanos (policiales e institucionales) con la correspondiente cualificación profesional, como técnicos (*software* y herramientas informáticas)**. Existe una **falta de medios tanto personales como materiales** para la persecución de estas conductas delictivas: personales con adecuada cualificación técnica y de medios materiales eficaces a la altura de los utilizados por los autores de conductas delictivas.

- En la investigación de este tipo de delitos resulta frecuente que **el autor se enmascare** bajo identidades falsas a través de la utilización de apodos, *nicks* o suplantaciones de personalidad; además suele intentar permanecer en el anonimato utilizando el *proxy*, anonimizadores existentes en la red, etc. Es más, aprovechándose de la transnacionalidad de Internet, el autor puede utilizar servidores interpuestos en el territorio de distintos países de manera que sea muy difícil determinar la identificación concreta del usuario. En ocasiones, cuando ya está localizado geográficamente el autor, cuando se va a proceder a su interceptación, ya no se encuentra en ese lugar y se ha trasladado o ha operado desde ubicaciones de usuarios públicos de imposible singularización. Con la conexión *wifi* se permite que, desde puntos muy próximos en los que se alcance la recepción de la onda, cualquier usuario se pueda conectar a Internet ocultando su identidad. Esta posibilidad ha generado un movimiento llamado "*wardriving* o *warchalking*" consistente en moverse por las calles con antenas potentes para localizar puntos de localización de *wifi* y allí hacer una pintada de posibilidad de acceso a la red de forma gratuita y anónima. Todo esto debe tenerse en cuenta en la investigación criminal al imposibilitar la identificación de usuario y generando la impunidad del delito[26].

[26] Por ejemplo en las empresas se ponen a disposición de los empleados equipos informáticos que permiten libremente su acceso sin ningún tipo de identificación de usuario. En las universidades, bibliotecas y centros de formación se ponen, a disposición de los alumnos, aulas dotadas de equipos informáticos que pueden ser utilizados por los usuarios sin realizar ningún tipo de identificación previa, se han dado casos de hackers que operan desde este tipo de equipos. En los cibercafés y centros de negocio también se posibilita el acceso a determinados equipos sin ningún tipo de control del usuario.

- En general en estos tipos delictivos suele existir una **falta de inmediación entre autor y víctima**. La actuación a través del ciberespacio en las fases decisivas de la dinámica delictiva, sin la presencia del autor en el lugar de los hechos e incluso difuminando su rastro electrónico, y en muchos casos sin inmediación con la víctima, dificultan la investigación y el enjuiciamiento. Se produce un efecto de despersonalización de la conducta delictiva.

- Existe dificultad de detección, pues en muchos casos las conductas dañosas alcanzan a numerosos objetivos en la escena mundial de forma instantánea, masiva, inadvertida y altamente dañina. La extraordinaria **potencialidad multiplicadora** de las acciones ilícitas y sus efectos lesivos facilita la difusión de este tipo de conductas lo cual requiere ser atajado de la forma conveniente.

- Existe una **anomia generalizada del ciberespacio** lo que supone, no sólo que el usuario infractor de normas cree actuar en un espacio ajeno al Derecho, sino que además no existe un cuerpo jurídico consolidado y eficaz que resuelva y supere los problemas de regulación de la actividad humana en el ciberespacio. Y aunque se puede conseguir determinar el terminal y servidor mediante los cuales se perpetró una conducta criminal, es mucho más difícil identificar al individuo concreto que perpetró la citada conducta.

- **La estructura no jerarquizada y descentralizada de la red es, de por sí, incompatible con un sistema de control institucional de la información de manera que cada vez se hace más difícil supervisar el gran volumen de información con contenido ilícito que circula por la misma**. El problema se acrecienta con el aumento exponencial del número de usuarios y las frecuencias de acceso por parte de los mismos lo que dificulta aún más la investigación y persecución criminal.

- La nota de la **extraterritorialidad es frecuente en este tipo de acciones delictivas, lo que conlleva problemas de jurisdicción, de operatividad policial y judicial, de determinación de la ley y del procedimiento aplicable**. Además en este tipo de delitos resulta habitual la **comisión a distancia**, tanto físicamente como en el tiempo, lo que genera la dificultad de asociar un hecho y un autor y resulta determinante en los análisis de investigación y posteriormente en la prueba en el juicio.

- Además las nuevas manifestaciones de este tipo de criminalidad exigen su **tratamiento desde una perspectiva internacional** ya que la acción de los

Estados con la aplicación de la propia ley nacional, es incompatible con una red global y transnacional. Se requiere la realización de un **esfuerzo de armonización normativa, tanto a nivel sustantivo como a nivel procesal, con la suscripción de tratados internacionales que intensifiquen la colaboración internacional para hacer frente a la ciberdelincuencia**. En este sentido sería favorable conseguir:

a) Que las legislaciones de los estados fuesen más homogéneas entre sí.

b) Que se estableciese una ayuda policial y judicial más estrecha.

c) Que se fijase, en conclusión, una mayor solidaridad y colaboración entre los Estados. Resulta claro que la realidad criminal más importante a nivel internacional se desarrolla en un lugar indeterminado llamado ciberespacio con unas coordenadas temporales y espaciales difíciles de aprehender.

- Por tanto podemos destacar, a modo de recapitulación final, que ante la delincuencia tecnológica que se despliega rápidamente y con gran impunidad por la aldea global sin fronteras se hace necesario **combatir el cibercrimen al margen de las fronteras convencionales de los Estados eludiendo las coordenadas de la soberanía estatal**. La solución para afrontar este tipo de delincuencia pasaría por **incrementar la cota de solidaridad y cooperación internacional para combatirla a nivel mundial con la suscripción de tratados internacionales multilaterales eficaces**.