Ciberseguridad *vs* ciberdelincuencia: obstáculos procesales en la persecución de la ciberdelincuencia organizada. Propuestas para una más eficaz represión de los ciberdelitos

Cybersecurity vs Cybercrime: Procedural Obstacles in the Prosecution of Organized Cybercrime. Proposals for a More Effective Repression of Cybercrime

María Luisa García Torres[1]
Universidad Alfonso X el Sabio.
mgarctor@uax.es | https://orcid.org/0000-0002-7638-9791

DOI: https://doi.org/10.14201/cp.31962
Recibido: 03-05-24 | Aceptado: 10-05-24

Resumen

La ciberseguridad y la ciberdelincuencia son dos caras de la misma moneda. Mientras que la ciberseguridad se refiere a las medidas diseñadas para proteger los sistemas informáticos, redes y datos contra los ataques cibernéticos, la ciberdelincuencia es aquella actividad criminal que se lleva a cabo mediante el uso de computadoras, redes y tecnologías de la información.

Los ciberdelincuentes son cada vez más, más fuertes y mejor organizados: se aprovechan de la transformación digital del mundo, y de la sociedad, del aumento de las transacciones por *Internet*, del anonimato en la navegación, del efecto multiplicador de sus acciones en la red, del desconocimiento de los ciudadanos sobre las medidas mínimas de ciberseguridad que deben adoptar en su vida diaria y de la proliferación de datos que se producen en el mundo cada día. Además, la persecución de la

1. Dra. en Derecho Procesal. Abogada del Ilustre Colegio de la Abogacía de Madrid. Directora del área jurídica de la Facultad Business & Tech, Universidad Alfonso X el Sabio.

ciberdelincuencia presenta numerosos obstáculos procesales: carácter extraterritorial de los delitos, escasez de recursos humanos y materiales, desconocimiento tecnológico de los jueces, dificultad para obtener las pruebas y la volatilidad de las evidencias son los más evidentes.

A pesar de los esfuerzos legislativos de la Unión Europea para garantizar el acceso a las pruebas electrónicas y para facilitar la investigación de estos crímenes, los resultados en la represión de la ciberdelincuencia han sido escasos hasta el momento. La cooperación internacional en materia penal se torna crucial en esta lucha.

El presente no es sencillo y el futuro una incógnita y es que la Inteligencia Artificial plantea nuevos y complejos retos para la ciberseguridad.

Palabras clave

Ciberseguridad; Ciberdelincuencia; Delincuencia organizada; Ciberdelincuencia organizada; Prueba electrónica; *Compliance*; *Behavioral compliance*.

Abstract

Cybersecurity and cybercrime are two sides of the same coin. While cybersecurity refers to measures designed to protect computer systems, networks, and data against cyber attacks, cybercrime is criminal activity carried out using computers, networks, and information technologies.

Cybercriminals are becoming increasingly powerful and they are better organized: they take advantage of the digital transformation of the world and society, the increase in online transactions, the anonymity of browsing, the multiplier effect of their actions on the network, the lack of awareness among citizens of the minimum cybersecurity measures they should adopt in their daily lives, and the proliferation of data produced in the world every day to commit crimes. Additionally, prosecuting cybercrime presents numerous procedural obstacles: the extraterritorial nature of crimes, scarcity of human and material resources, technological unfamiliarity among judges, difficulty in obtaining evidence, and the volatility of evidence.

Despite the legislative efforts of the European Union to ensure access to electronic evidence and facilitate the investigation of these crimes, results in the repression of cybercrime have

been scarce so far. International cooperation in criminal matters becomes crucial in this fight.

Keywords
Cybersecurity; Cybercrime; Organized crime; Organized cybercrime; Electronic evidence; Compliance; Behavioral compliance.

1 Algunas notas introductorias para entender el surgimiento de un nuevo término: «ciberdelincuencia organizada»

En primer lugar, debemos diferenciar ciberseguridad y ciberdelincuencia, pues, aunque son conceptos relacionados, resultan opuestos en su naturaleza y objeto:

La ciberseguridad se refiere a las medidas, prácticas y tecnologías diseñadas para proteger los sistemas informáticos, redes y datos contra accesos no autorizados, ataques cibernéticos, robo de información, daños o cualquier tipo de amenaza que pueda comprometer la seguridad de la información y la operación de los sistemas. La ciberseguridad se centra, por ende, en prevenir, detectar y responder a posibles riesgos y amenazas cibernéticas.

Sin embargo, la ciberdelincuencia es aquella actividad delictiva que se lleva a cabo mediante el uso de computadoras, redes y tecnologías de la información. La ciberdelincuencia implica el uso ilegal de la tecnología para cometer actos delictivos y causar daño a individuos, organizaciones o sistemas.

Así, la ciberseguridad busca proteger los sistemas y datos contra amenazas cibernéticas. La ciberdelincuencia representa las acciones criminales que se apoyan en las vulnerabilidades en esos sistemas y datos, todo ello con fines ilícitos. La ciberseguridad es proactiva y defensiva, mientras que la ciberdelincuencia es destructiva y criminal.

El fenómeno de la globalización ha tenido más beneficios que perjuicios para el mundo. Efectivamente, sus efectos han sido favorables para la economía, la tecnología, la sociedad y para la

cultura. Pero no podemos soslayar algunos efectos perniciosos, como el que tiene que ver con la delincuencia. La globalización, unida al imparable crecimiento de la tecnología y transformación que está produciendo en el mundo, han originado que los patrones de delincuencia hayan cambiado. De hecho, hoy hablamos de la delincuencia transnacional y de ciberdelincuencia, términos antes desconocidos.

¿Cómo podemos definir la delincuencia transnacional? ¿Son términos sinónimos los conceptos de delito internacional y de delito transnacional? No resulta tan sencillo dar una respuesta a estos interrogantes.

Podríamos intentar definir los delitos internacionales acudiendo al Estatuto de la Corte Penal Internacional, firmado, en Roma, el 17 de julio de 1998. Tanto de su Preámbulo, como de su arts. 1 y 5, podríamos inferir que un delito internacional es aquél que, siendo grave, tiene trascendencia para la comunidad internacional en su conjunto. Así serían delitos internacionales, según el art. 5 de la Norma citada, los siguientes crímenes: genocidio, lesa humanidad, crímenes de guerra y el de agresión. Se trataría, en definitiva, de graves violaciones de las normas imperativas de Derecho Internacional Público.

Sin embargo, no resulta tan claro el concepto, si atendemos a la clasificación de los crímenes internacionales que algunos autores realizan (Messuti, 2013). Los delitos internacionales se pueden agrupar en cuatro categorías diferentes: a) delitos de Derecho Internacional, por ejemplo, crímenes de guerra; b) delitos contra el Derecho Internacional, como son los delitos de piratería; c) delitos que interesan al Derecho Internacional, caracterizados por elementos jurídicos, sociológicos y antropológicos dispersos entre territorios, nacionalidades o razas diferentes, como es el caso de la trata de personas y; d) delitos según el Derecho Internacional, los cuales se fundamentan en el carácter universal del bien jurídico protegido, entre los que se encuentran el delito de abordaje marítimo o aéreo o la misma piratería. Los delitos transnacionales, según esta clasificación, podrían incluirse dentro de la tercera categoría (Zúñiga Rodríguez, 2016). Podemos observar que el delito de piratería resulta difícilmente subsumible en las categorías anteriores, lo que

evidencia la dificultad de deslindar las diferentes clases de delitos internacionales.

Sin perdernos en disquisiciones doctrinales y desde la perspectiva de Derecho positivo, en España, el principio de Justicia universal permite atribuir jurisdicción a los tribunales españoles mezclando dos grupos de delitos: los que deben perseguirse por existir un interés común, por tratarse de hechos de carácter trasnacional, que requieren el acuerdo de varios Estados para que sea posible y; aquéllos, en cuya protección están interesados todos los Estados de la Comunidad internacional, por fundamentarse en las normas de *ius cogens* del Derecho Internacional. Así, el art. 23.4 de la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial (en adelante, LOPJ), atribuye jurisdicción a los tribunales españoles, siempre que exista la concreta conexión que la Ley establece en cada caso (entre otras, víctima española, procedimiento dirigido frente a un español o frente a una persona que resida en territorio español) en delitos tan dispares como genocidio, lesa humanidad o contra las personas y bienes protegidos en caso de conflicto armado, tráfico ilegal de drogas tóxicas, estupefacientes o sustancias psicotrópicas o, entre otros, corrupción entre particulares. El precepto mencionado recoge así tanto las tesis universalistas como las pragmáticas, en la configuración del llamado principio de Justicia universal (Menéndez Rodríguez, 2014).

Aunque el art. 23.4 de la LOPJ española, incluya delitos propiamente internacionales como aquéllos que pueden calificarse de transnacionales, podemos definir los delitos internacionales, diferenciándolos de los segundos, como aquéllos afectantes a bienes jurídicos de carácter universal, teniendo su fundamento en los derechos humanos, afirmados por las normas imperativas de Derecho Internacional, tanto consuetudinarias como convencionales.

Por delito transnacional entendemos, sin embargo, aquellas acciones u omisiones que, siendo definidas como delito por las normas de cada uno de los Estados, se cometen o producen efectos en el territorio de más de un Estado. Los delitos transnacionales, por ende, no vienen definidos por el Derecho Internacional Público, sino por los ordenamientos jurídicos internos, lo que

sucede es que, a diferencia de los delitos nacionales, se cometen o repercuten en más de un ordenamiento jurídico. Se suelen caracterizar, además, por cometerse por medio de una estructura organizada, de ahí que se hable de una delincuencia transnacional organizada. Los delitos transnacionales más conocidos son el narcotráfico, el tráfico de armas, la trata de seres humanos, el blanqueo de capitales, etc. Su fundamento no radica en la afirmación de los derechos humanos inherentes a la dignidad del ser humano, sino en razones prácticas: el interés de los Estados en llegar a acuerdos para perseguir hechos delictivos que escapan de sus fronteras, pues se cometen en un ordenamiento jurídico, pero producen sus efectos en otro distinto o incluso se cometen allá donde su jurisdicción no alcanza (Zúñiga Rodríguez, 2016).

Hoy en día, resulta imposible aplicar los viejos cánones del Derecho Penal sobre los que éste se construyó, basados en la soberanía de los Estados, en la territorialidad de la norma penal y en la titularidad exclusiva de los Estados del *ius puniendi* (Zúñiga Rodríguez, 2016). La represión de los delitos de carácter transnacional requiere de la cooperación entre los Estados. Dado que se producen o tienen sus efectos en diferentes ordenamientos jurídicos, no es posible ni la prevención ni su castigo, si no es contando con la colaboración de todos los Estados. Manifestación concreta de la delincuencia transnacional, es la llamada ciberdelincuencia o, en inglés, *cybercrime*.

Se entiende por ciberdelincuencia aquélla en la que está involucrada un equipo informático o *Internet* y en la que el ordenador, el teléfono, la televisión (*smart tv*), el reproductor de audio o vídeo o el dispositivo electrónico puede ser usado para la comisión del delito o puede ser objeto del mismo delito (Rayón Ballesteros y Gómez Hernández, 2014).

Cabe trazar una línea diferenciadora entre el concepto de ciberdelito y el de delito informático. El primero está estrechamente vinculado a las tecnologías de la Información y la Comunicación (TIC). En ellos, interviene la comunicación telemática abierta (pública), cerrada (privada) o de uso restringido. El delito informático es el aquél que se vale de elementos informáticos para su perpetración (Romero Casabona, 2016). Por tanto,

implica el uso indebido de elementos informáticos o sistemas computacionales: se vale de elementos informáticos, como computadoras, dispositivos de almacenamiento, *software*, redes, para perpetrar la actividad delictiva, pero no tiene que ir ligado a la comunicación telemática, aunque puede utilizarla como medio para cometer el hecho.

De lo que se ha dicho en relación con la delincuencia transnacional queda claro que, en la actualidad, las fronteras no son un límite para la comisión de crímenes, siendo uno de los ámbitos donde más se plasma lo que cabe llamar la realidad «líquida» de las fronteras del ciberespacio (Zúñiga Rodríguez, 2016).

Si se unimos los conceptos de delincuencia organizada y ciberdelincuencia, obtenemos el término ciberdelincuencia organizada (Oficina de las Naciones Unidas Contra la Droga y El Delito, 2022). Tal y como reconoce Naciones Unidas no existe consenso para definir este nuevo término, ahora bien, hay ciertos parámetros de obligado cumplimiento como son los siguientes: el acto ilícito tiene que tener una dimensión cibernética, teniéndose que tratar bien de un delito facilitado por la cibernética o bien basado en la misma[2] y entrañar ya sea la participación de un grupo delictivo organizado (art. 2 de la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional) o un delito tipificado, conforme al art. 5 de la misma Convención (confabulación o asociación delictuosa).

Los ciberdelincuentes se amparan en la continua transformación digital del mundo, y de la sociedad, en el aumento vertiginoso de las transacciones económicas que se realizan a través de *Internet*, en el anonimato en la navegación, en el efecto multiplicador de sus acciones en la red, en el desconocimiento de los

2. La Oficina de las Naciones Unidas Contra la Droga y el Delito diferencia los delitos facilitados por la cibernética y los delitos basados en la cibernética. Los primeros son delitos tradicionales facilitados (de alguna manera) por las *TIC*. Así, «(…) las *TIC* desempeñan un papel fundamental en el método de operación, (es decir, el modus operandi) del delincuente o los delincuentes». Sin embargo, los delitos basados en la cibernética (quedan incluidos aquellos que solo se pueden cometer utilizando computadoras, redes informáticas u otras formas de tecnología de comunicación de la información, el objetivo de ese tipo de delitos son las *TIC*.

ciudadanos de las medidas mínimas de ciberseguridad que deben adoptar en su vida diaria y en la gran volumen de datos que se producen e intercambian en el mundo cada día, para delinquir. Son muchos y, como veremos a continuación bien organizados y ven multiplicadas sus acciones delictivas por el gran impacto que tienen en el ciberespacio.

Gracias a la investigación y a la cooperación internacional, podemos conocer los caracteres esenciales que definen a los grupos que cometen ciberdelitos de carácter transnacional, aunque ciertamente la ciberdelincuencia organizada es todavía muy desconocida. Ciertamente, los grupos de ciberdelincuentes muestran conductas similares a los de los grupos organizados que pueden calificarse de tradicionales, por cometer delitos no cibernéticos, pues usan una estructura y se valen de unos procedimientos especiales que tienden a preservar el anonimato de sus miembros y a evitar la detección por parte de la policía. Es tal la protección que crean para no ser vistos por las fuerzas policiales que, de hecho, los foros utilizados por los ciberdelincuentes (por ejemplo, los empleados para compartir fotografías sexuales de menores), tienen más protección y más medidas de seguridad que otras[3]. Pero, a diferencia de los grupos organizados tradicionales, las TIC permiten la agrupación de personas que no se conocen entre ellos y que nunca se han visto cara a cara y, por ende, se unen personas que residen en cualquier parte del mundo. La misma tecnología les dota de una infraestructura, de productos, de personal y de clientes, sin las barreras geográficas que existen en los delitos tradicionales. El anonimato es una característica propia de estos delitos, cometidos a través o por la red[4].

La investigación demuestra que los grupos varían en virtud de la complejidad estructural (Oficina de las Naciones Unidas Contra la Droga y el Delito, 2022): los hay con mayor jerarquización, que centralizan y dividen su trabajo, con líderes identificables,

3. A veces se obliga a una persona que quiere entrar en esos foros a hacerse miembro, exigiéndoles que aporten ellos mismos fotografías sexuales de menores, incluso se les exige pagar una cuota.
4. Véase a este respecto *Compendio de ciberdelincuencia organizada,* emitido por Oficina de las Naciones Unidas Contra la Droga y el Delito, 2022, pp. 1-3.

mientras que otros tienen redes transitorias, sin una naturaleza nítida, no vertical, sino lateral, sin una estructura fija y descentralizada. Ya sean de una clase o de otra utilizan foros y plataformas en línea para regular y controlar el suministro de bienes y servicios ilícitos. Esto quiere decir que entienden la delincuencia como un servicio y se basan en las aptitudes de sus individuos para realizar sus actividades.

Los grupos de ciberdelincuentes se pueden dividir en tres: los que operan principalmente en línea y cometen delitos cibernéticos; los que lo hacen fuera y en línea y cometen delitos cibernéticos y; los grupos que operan predominantemente fuera de línea y se dedican a la ciberdelincuencia para ampliar y facilitar sus actividades fuera de línea.

Dentro del primer grupo, a su vez se pueden distinguir los «enjambres» y los «nodos». Un «enjambre» es una fusión durante un espacio de tiempo de personas que se agrupan para realizar tareas para cometer un delito cibernético, pero después, una vez terminan y cumplen sus objetivos, desintegran el grupo. Son redes descentralizadas, que se componen por grupos efímeros de personas, y mínimas cadenas de mando. Cometen los delitos por razones ideológicas. Los «nodos» se integran por un núcleo de delincuentes, a los que se unen unos que se asocian, tienen más estructura y son más jerarquizados.

Los grupos que operan fuera de línea y en línea y se dedican a cometer delitos y delitos cibernéticos son llamados «híbridos», habiendo «híbridos agrupados» o «híbridos extendidos». Los primeros realizan determinadas actividades o utilizan métodos específicos para cometer ciberdelitos; se organizan como los «nodos», pero realizan sus actividades fuera y en línea, teniendo capacidad para ello. Tienen una táctica y operan en una ubicación concreta. Los grupos extendidos son mucho más especializados, menos centralizados y con un núcleo menos evidente; su composición es más compleja y su ámbito de operaciones es la llamada «red oscura».

Por último, el tercer grupo tienen una fuerte estructura jerárquica, se integran por grupos organizados tradicionales, pero amplían sus actividades ilícitas operando en línea, por ejemplo,

a través de los juegos de azar, extorsión, prostitución o trata de personas.

La estructura de todos los grupos supone que operen como una auténtica empresa con «trabajadores» que prestan sus servicios en ella. Existe personal técnico, personal de apoyo, personal de comercialización; encargados de pagar y cobrar los servicios y cuentan con reglas de conducta por las que se rigen. La organización depende de a la actividad ilícita que se dediquen. Los que se basan para delinquir en la cibernética se nutren de codificadores, piratas informáticos, responsables de apoyo técnico y anfitriones (los que alojan actividades ilícitas en servidores o en ubicaciones físicas fuera de la red.

Después de esto, podemos afirmar que son muchos y muy bien organizados.

Debe tenerse en cuenta que, en el año 2023, del total de delitos, 2 459 659, cometidos de enero a diciembre, 470 388 son ciberdelitos, lo que representa un 19,1 % del total. De este número 426 744 son ciberestafas. Para entender el aumento vertiginoso que la ciberdelincuencia ha tenido en nuestro país, debemos comparar ese dato con las 70 178 estafas cibernéticas registradas en el año 2016. En sólo ocho años ha habido un aumento de un 508,1 %[5].

Los ciberataques más frecuentes son los que tienen que ver con alguna de estas conductas: robo de identidad, piratería, *phishing*, *botnets*, ciberespionaje, extorsión en la red, *malware*, *ransomware*, pornografía infantil, acoso y amenazas cibernéticas.

El robo de identidad sucede cuando una persona se apropia de la identidad de otra, en beneficio propio, actuando en el tráfico jurídico simulando ser la persona a la que suplanta.

La piratería supone una entrada ilegal en un sistema informático o la ruptura de las protecciones que impiden la copia de un programa. Se utiliza también para hacer referencia a las

5. Véase https://www.interior.gob.es/opencms/export/sites/default/.galleries/galeria-de-prensa/documentos-y-multimedia/balances-e-informes/2023/Balance-de-Criminalidad-Cuarto-Trimestre-2023.pdf (Consultado el 29/04/2024. Hora: 13:00).

copias ilegales de programas, discos o *DVDs*. El término inglés es *cracking*[6].

El *phishing* supone extraer información confidencial mediante suplantación de identidad por correo electrónico, sitios *web* o llamadas.

También es necesario explicar el término *botnet*, que tiene lugar cuando una red de computadoras es infectada con *malware*, conectándolas a un centro de comando y control central. Los ciberatacantes lo utilizan para enviar correos electrónicos no deseados o realizar ataques *DDoS*, que consisten en producir una denegación de servicio por una sobrecarga en un sitio *web*, un servidor o un recurso, lo que lleva a un bloqueo o falta de funcionamiento y, al mismo tiempo, a una denegación de un servicio a los usuarios legítimos.

Las *botnet* se utilizan también para hacer lo que se denomina *clic* en fraude, esto es *clics* falsos que tienen como objetivo aumentar la calificación de búsqueda de una página *web* o inflar de manera artificial la popularidad de una publicación en las redes sociales.

El ciberespionaje es aquella actividad a través de la cual se obtiene información confidencial, secreta o estratégica de individuos, organizaciones, o gobiernos a través de medios electrónicos y digitales. Esto puede incluir la infiltración en sistemas informáticos, el robo de datos, el monitoreo de comunicaciones en línea, y el uso de *malware* u otras técnicas de *craking* para acceder a información sensible. Por ejemplo, a través de un programa se espían las comunicaciones de *Internet*, para encontrar números de tarjetas de crédito.

La ciberextorsión es un tipo de delito por el que se amenaza a una persona, empresa u organización con revelar información comprometedora, filtrar datos sensibles, dañar sistemas informáticos o realizar otras acciones perjudiciales a menos que se cumpla con una demanda específica, normalmente el pago de una cantidad de dinero, generalmente en criptomonedas u otra

6. El término hacking hace referencia a una habilidad, pero no supone ilegalidad.

forma de pago digital, aunque también puede incluir otras condiciones, como la realización de acciones específicas o la entrega de bienes o servicios. Los métodos utilizados para llevar a cabo la extorsión en línea pueden variar, desde el envío de correos electrónicos amenazantes (conocidos como «emails de sextorsión»), hasta el uso de *ransomware* para cifrar archivos y exigir un rescate por su liberación.

La ciberextorsión puede tener graves consecuencias tanto para individuos como para empresas, ya que puede causar daños financieros, reputacionales y emocionales significativos.

El *malware* es un *software* malicioso que se utiliza para dañar computadoras y sistemas informáticos sin el conocimiento del propietario, por ejemplo, a través de *spyware*, virus, gusanos o troyanos.

El ciberataque que, con más frecuencia se produce, es el que se conoce como *ransomware*. El año 2023 ha supuesto un récord y es que, en el tercer trimestre de ese año, se constataron 1278 víctimas de este tipo de ataque, lo que ha supuesto un aumento del 11,22 % con respecto al segundo trimestre del mismo año y un aumento interanual del 95,41 %[7].

Este *software* está diseñado para bloquear el acceso a un sistema informático, archivos o datos, generalmente mediante su cifrado, para luego exigir un rescate económico a cambio de restaurar el acceso. Una vez que el *ransomware* infecta un sistema, muestra mensajes intimidatorios o instrucciones sobre cómo pagar el rescate, siendo habitual que sea solicitado en forma de criptomonedas, con la finalidad de dificultar el rastreo del pago.

Los *ransomware* suelen propagarse a través de correos electrónicos de *phishing*, descargas de archivos maliciosos, vulnerabilidades en el *software* o sistemas desactualizados, y en algunos casos, a través de *exploits* de seguridad. Una vez que el

7. Véase el Informe presentado por CORVUS (2023, 24 d octubre), en https://www.corvusinsurance.com/blog/q3-ransomware-report (Consultado el 24/04/2024. Hora: 13:00).

ransomware infecta un sistema, puede cifrar archivos de gran importancia para el usuario o la organización, como sucede con los documentos, las fotos, las bases de datos o incluso con todo el disco duro.

El *ransomware* puede causar graves daños y pérdidas económicas, además de afectar la reputación de las organizaciones que son víctimas de estos ataques. La prevención del *ransomware* implica la adopción de buenas prácticas de seguridad cibernética, como la actualización regular del *software*, la concienciación sobre seguridad entre los empleados, el uso de *software* de seguridad confiable y la realización de copias de seguridad frecuentes y almacenadas de forma segura.

La pornografía infantil se produce cunando se distribuye, produce y consume material sexualmente explícito que involucra a menores de edad. En *Internet* puede manifestarse en diversas formas, como imágenes, videos o cualquier otro tipo de material que muestre a menores en situaciones sexualmente explícitas o sugestivas. Esta actividad criminal suele estar asociada con redes de explotación sexual infantil, donde los perpetradores pueden producir este tipo de contenido para su propio beneficio o con fines de lucro.

El acoso y amenazas como ciberdelitos son formas de abuso que se llevan a cabo a través de medios electrónicos, *Internet*, redes sociales, mensajes de texto, correo electrónico, entre otros. Estas acciones pueden tener graves repercusiones emocionales, psicológicas y, en algunos casos, físicas para las víctimas. Aquí hay una definición detallada de cada uno.

A continuación, se enumeran los posibles ciberdelitos que pueden cometerse y que están tipificados en la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal (en adelante, CP[8]):

A) Descubrimiento y revelación de secretos: estos delitos lesionan la intimidad personal, familiar o la propia imagen

8. Para un conocimiento más profundo de los ciberdelitos, no ceñido exclusivamente al ordenamiento jurídico español, véase *Compendio de ciberdelincuencia organizada.* Incluso dicho Compendio incluye Resoluciones dictadas en distintos países.

de la víctima, mediante el apoderamiento de documentos o interceptación de telecomunicaciones (art. 197.1 del CP); o, el acceso, apoderamiento, utilización o modificación (sin permiso) de datos informáticos de carácter personal (197.2 CP); o, la difusión sin permiso de imágenes o documentos audiovisuales, obtenidos con autorización de la víctima en un lugar fuera del alcance público, cuando la difusión menoscabe gravemente la intimidad de ésta (197.7 CP); a este delito se le llama *sexting*.

B) Acceso ilícito a sistemas informáticos: se trata de los delitos que tienen que ver con el de revelación de secretos, bien por la permanencia o facilitación del acceso a un sistema informático vulnerando las medidas de seguridad impuestas por éste y contra la voluntad de un usuario legítimo (art. 197. Bis 1 del CP), bien por la interceptación de datos informáticos mediante herramientas o mediante expertos (*snifer)*, según lo previsto en el art. 197 bis 2 del CP. También se produce este delito por el acceso ilícito, por producción o facilitación de programas y/o contraseñas (art. 197 ter del CP).

C) Daños informáticos, como son borrar, dañar, deteriorar, alterar, suprimir o hacer inaccesibles datos informáticos, programas o documentos ajenos, sin autorización y de manera grave (264 del CP); obstaculizar o interrumpir el funcionamiento de un sistema informático (art. 264 bis del CP); producir, adquirir o facilitar programas (art. 264 ter del CP) y; facilitar contraseñas destinadas a cometer alguno de los delitos anteriores (art. 400 del CP)

D) Falsedades informáticas, como es la falsificación de moneda y timbre (386 a 389 CP); la de documento público, oficial y mercantil (390 a 394 del CP); de documento privado (395 a 396 del CP); de certificado (397 a 399 del CP); de tarjetas de crédito, débito o cheques de viaje (399 bis del CP) o; la fabricación, recepción, obtención o tenencia de instrumentos, datos o programas informáticos destinados a la comisión de los delitos indicados (400 del CP)

E) Estafa informática: es la utilización de un engaño, con ánimo de lucro y con la finalidad de obtener un beneficio o perjuicio a un tercero (art, 248 a 251 del CP). Es el art. 248.2 del CP el que recoge de forma expresa la llamada estafa informática, que consiste en valerse de manipulaciones

informáticas o mecanismos, como el *phishing,* para obtener de forma no consentida una transferencia patrimonial en perjuicio de un tercero. Tal y como hemos indicado es, con mucho, el ciberdelito más cometido en los últimos años. También se comete este delito por la fabricación, posesión o facilitación de programas informáticos, con el objetivo de realizar operaciones bancarias en perjuicio de su titular o de un tercero; esto es lo que en términos informáticos se llama *ransomware*.

F) Defraudaciones de telecomunicaciones y es que éstas, igual que sucede con el fluido eléctrico o agua, pueden ser objeto de defraudaciones a través de mecanismos que se utilizan al efecto, por ejemplo, alterando los contadores (art. 355 del CP); también cuando se utiliza un terminal de telecomunicaciones sin permiso de su titular, si se le causa un perjuicio económico.

G) Ciberdelitos sexuales: destaca el llamado *child grooming*, que consiste en ponerse en contacto con un menor de 16 años, para tener un encuentro con el fin de cometer los actos previstos en los arts. 181 a 189 del CP (art. 183.1 del CP). También, recibe esa denominación el delito cometido cuando el menor de 16 años facilita al autor material pornográfico o le muestra imágenes pornográficas en las que se represente o aparezca un menor (art, 183.2 del CP).

Cabe el acoso sexual, efectuado a través de las TIC (art. 184 CP) o el exhibicionismo ante menores de edad o discapacitados necesitados de especial protección (art. 185 del CP).

Asimismo, entra dentro de esta categoría la venta o difusión de material pornográfico a menores o discapacitados de especial atención (art. 186 del CP) o la prostitución, explotación sexual y corrupción de menores del art. 187 a 189 bis del CP.

H) Delitos contra la propiedad industrial, pues cabe la reproducción, plagio, distribución o comunicación pública de una obra con ánimo de lucro y sin autorización de los titulares de los derechos de propiedad intelectual (art. 270.1 del CP); la facilitación activa y con ánimo de lucro del acceso o localización en *Internet* de obras protegidas sin autorización de los titulares de los derechos de propiedad intelectual (art. 270 del CP). También, eliminar, modificar las medidas tecnológicas destinadas a proteger obras para favorecer la

comisión de alguna de las conductas de los tipos comentados (270.5 apartado C). Es posible que se cometa este tipo de delitos por la elusión o facilitación de medidas tecnológicas para facilitar a un tercero el acceso a una obra protegida (art. 270. 5 D).

La fabricación, importación, distribución o posesión con fines comerciales de cualquier medio destinado a neutralizar dispositivos técnicos utilizados para proteger programas informáticos u obras protegidas (270.6 CP) es un delito también cibernético contra la propiedad industrial.

I) Delitos contra el honor: y, dentro de éstos, encontramos la calumnia o la injuria, conductas agravadas por la publicidad, cuando, por ejemplo, se realizan en redes sociales o por grupos de mensajería (art. 208 del CP)

J) Amenazas y coacciones, siempre que se produzcan en el ciberespacio o entorno virtual (art. 271.2 del CP o art. 172 a 172 ter del CP). Tenemos el llamado ciberacoso o *ciberstalking* (art. 172 ter del CP), que supone el contacto de forma reiterada e insistente por parte del autor con la víctima, causándole graves alteraciones en el desarrollo de su vida diaria.

Cuando la acción la realiza un menor que es quien atormenta o amenaza o coacciona se llama bulling. Cabe que sea realizado mediante *Internet*, teléfonos móviles, videoconsolas *online*.

K) Delito de odio (art. 510 del CP) y apología del terrorismo, que tiene especial gravedad, cuando se difunde a través de medios telemáticos (art. 578 del CP)

L) Delito por usurpación o suplantación de la identidad: art. 401 del CP. Supone apropiarse una persona de la identidad de otra, en beneficio propio, actuando en el tráfico jurídico simulando ser la persona a la que suplanta. Este tipo de delitos es muy habitual en las llamadas «estafas del amor», pues como señuelo, se coloca la foto de una persona atractiva que es de otra persona.

El CP se ha ido modificando para adaptarse a la nueva realidad delictiva. La reforma más importante habida en este sentido ha sido la producida por la Ley Orgánica 1/2015, de 30 de marzo, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal.

Como puede entenderse, la cooperación en materia penal para la prevención y lucha contra la delincuencia transnacional y, en particular, contra la ciberdelincuencia, resulta, en virtud de lo anterior, de vital importancia.

La ciberdelincuencia proyecta sus consecuencias directamente sobre el proceso penal. Primeramente, porque la investigación de la ciberdelincuencia requiere de unidades investigación especializadas, dotadas de los medios técnicos necesarios para la efectividad de su trabajo.

En segundo lugar, los rastros que deja esta clase de delincuencia son de carácter electrónico, debiendo entonces referirnos a las evidencias electrónicas, difíciles de conseguir y altamente volátiles. En este sentido, la obtención transfronteriza de pruebas electrónicas se antoja extremadamente difícil, pues los proveedores de servicios de *Internet* suelen tener su sede en lugar distinto al de comisión de los hechos delictivos. La extraterritorialidad dificulta enormemente el acceso a dicha clase de prueba. La rápida alteración y destrucción de las evidencias digitales es uno de los grandes escollos que existen para el castigo de estos delitos.

Aunque en el seno de la Unión Europea (en adelante, UE) se ha legislado para evitar que los servidores de servicios de *Internet* impidan el acceso a la prueba electrónica, aún muchos Estados miembros se amparan en el necesario respeto de los derechos fundamentales para intentar impedir la obtención de las pruebas electrónicas.

Por último, tal y como se expondrá posteriormente, se hace necesaria la intervención de peritos especializados en la obtención y análisis de las evidencias encontradas.

A todos estos retos se une el uso de la Inteligencia Artificial (en adelante, IA) fundacional. Hemos pasado de la IA predictiva a la generativa y, dentro de ella, ya se habla del modelo fundacional. Que ¿de qué se trata? De redes neuronales *deep learning*. La IA que sigue este modelo se desarrolla a partir de un modelo fundacional que se utiliza como punto de partida para crear modelos de ML, que permite contar con aplicaciones nuevas de

manera rápida y poco costosa. Estos modelos fundacionales son entrenados a través de datos generalizados y sin etiquetar y que son capaces de realizar una gran variedad de tareas generales, entre ellas comprender el lenguaje, generar texto e imágenes y conversar en lenguaje natural.

Estos modelos fundacionales permiten crear archivos de voz o vídeos con imágenes como si fueran reales. ¿Qué les espera a los juzgadores si se les presenta una evidencia creada por IA fudacional sin que tengan posibilidad de conocer que dicha evidencia no es real?

2 Marco legal internacional de la delincuencia transnacional y de la ciberdelincuencia organizada

En diciembre de 2000, se firmó, en la ciudad de Palermo, la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional. La Comunidad internacional se percató de que la delincuencia transnacional se había convertido en un problema mundial, al atravesar las fronteras, siendo imposible atajarla a través de medios nacionales.

Dos Resoluciones de la Asamblea General fueron el origen de dicha Convención. En primer lugar, la Resolución 53/111, de 9 de diciembre de 1998, en la que decidió establecer un Comité especial intergubernamental de composición abierta, con la finalidad de elaborar una Convención internacional amplia contra la delincuencia organizada transnacional y de examinar, si procedía, la posibilidad de elaborar instrumentos internacionales sobre la trata de mujeres y niños, la lucha contra la fabricación y el tráfico ilícitos de armas de fuego, sus piezas y componentes y municiones, y el tráfico y el transporte ilícitos de migrantes, incluso por mar. La segunda fue la Resolución 54/126, de 17 de diciembre de 1999, en la que pidió al Comité Especial encargado de elaborar una Convención contra la delincuencia organizada transnacional que prosiguiera sus trabajos, de conformidad con las Resoluciones 53/111 y 53/114, de 9 de diciembre de 1998, y que intensificara esa labor, a fin de terminarla en el año 2000.

En esta Convención, se definieron conceptos claves tales como: a) grupo delictivo organizado, entendiendo por tal el estructurado por tres o más personas que exista durante cierto tiempo y que actúe concertadamente con el propósito de cometer uno o más delitos graves o delitos tipificados en la Convención, con miras a obtener, directa o indirectamente, un beneficio económico u otro beneficio de orden material; y; b) grupo estructurado, que es un grupo no formado fortuitamente para la comisión inmediata de un delito y en el que no necesariamente se haya asignado a sus miembros funciones formalmente definidas ni haya continuidad en la condición de miembro o exista una estructura desarrollada. La Convención se aplica a la prevención, la investigación y el enjuiciamiento cometidos por grupos organizados, blanqueo de capitales, corrupción y la obstrucción a la Justicia. Intenta que los Estados parte adopten medidas legislativas para el castigo de estos delitos y se decomisen bienes, producto de los mismos. Permite la presentación de la solicitud de la orden de decomiso de un Estado parte a otro, siempre que tenga jurisdicción para conocer de un delito comprendido en el Tratado.

Por otra parte y, ya en un ámbito regional, concretamente referido al Consejo de Europa, contamos con el Convenio sobre Ciberdelincuencia, firmado, en Budapest, el 23 de noviembre de 2001, mediante el cual se propone a los Estados firmantes adoptar las medidas legislativas necesarias para tipificar en sus respectivos ordenamientos jurídicos el acceso deliberado e ilegítimo a toda parte de un sistema informático; la interceptación deliberada e ilegítima por medios técnicos de datos informáticos en transmisiones no públicas dirigidas a un sistema informático, originadas en un sistema informático o efectuadas dentro del mismo, incluyendo las emisiones electromagnéticas provenientes de un sistema informático que transporte dichos datos informáticos; los actos deliberados e ilegítimos que supongan ataques a los datos informáticos; ataques a la integridad de los sistemas; abusos de los dispositivos; la falsificación informática; el fraude informático; los delitos relacionados con la pornografía infantil y los delitos relacionados con infracciones de la propiedad intelectual y otras figuras afines.

Dicho Convenio permite la armonización penal y procesal penal en el ámbito de la ciberdelincuencia, regulando una cuestión

transcendental que provoca múltiples problemas en cuando a la persecución de este tipo de delitos, cometidos a través de servidores que se alojan en Estados diferentes de aquéllos en los produce efectos. Y es que el Convenio dispone que la jurisdicción quedará fijada a favor del Estado cometido en su territorio, incluyendo a bordo de un buque que tenga su pabellón o de una aeronave matriculada según sus leyes cometido por uno de sus nacionales, si el delito es está considerado como tal en el lugar en el que se cometió o si ningún otro Estado tuviera competencia territorial para conocer de aquél.

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.

Ambos Convenios ponen de manifiesto la importancia de la cooperación para la prevención y represión de los delitos transnacionales y de los ciberdelitos. Y es que las características propias de esta criminalidad dificultan enormemente su persecución.

España ratificó el Convenio en 2004 y el Protocolo Adicional en el año 2006. En 2024, son ya 69 Estados los firmantes de dicho Convenio.

3 La cooperación penal en la Unión Europea: especial referencia a la orden europea de investigación y a la obtención de pruebas electrónicas transfronterizas

La cooperación judicial en materia civil y judicial en la Unión Europea (en adelante, UE) comenzó con el Tratado de Maastricht, firmado el 7 de febrero de 1992, el cual que entró en vigor el 1 de noviembre de 1993. Dicho Tratado declaró la cooperación civil y mercantil cuestión de interés común. Fue el Tratado de Ámsterdam, firmado el 2 de octubre de 1997, en vigor desde el 1 de mayo de 1999, el que asoció la cooperación en ese ámbito con la libre circulación de personas.

La cooperación penal se antoja mucho más complicada pues, como sabemos, choca con la política criminal definida por cada Gobierno y, por tanto, con la soberanía de cada Estado. Los Estados son menos reticentes a cooperar en materia civil y mercantil, que en materia penal. Pero es cierto que la eliminación progresiva de las fronteras y la creación del espacio Schengen (1995), conquista de la UE y que nos permite pasar de un país a otro sin controles fronterizos dentro de la Unión, ha facilitado considerablemente la libre circulación de los ciudadanos europeos, pero también ha contribuido a que los delincuentes puedan actuar con mayor libertad a escala transnacional.

La UE, con el fin de afrontar el reto de la delincuencia transfronteriza y asegurar el espacio de libertad, seguridad y justicia ha incluido medidas para promover la cooperación judicial en materia penal.

Recordemos cuáles han sido los hitos conseguidos en la UE en materia de cooperación penal durante los últimos años:

El 29 de mayo de 2000, el Consejo de Ministros de la Unión adoptó el Convenio relativo a la Asistencia Judicial Mutua en materia penal, cuyo propósito es alentar la cooperación entre las autoridades judiciales, policiales y aduaneras dentro de la Unión, complementando las disposiciones relativas a los instrumentos jurídicos existentes y en aplicación del Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales. Este Convenio se antoja clave pues permite la constitución de equipos conjuntos de investigación o la intervención de las telecomunicaciones previa solicitud de una autoridad competente de otro país de la UE, designada para ello en dicho país de la UE. Incluso, la intervención podrá también tener lugar en un país de la UE en que se encuentre la estación terrestre de comunicaciones por satélite correspondiente.

Conseguimos sustituir la extradición por la orden de detención europea, el 13 de junio de 2002, la cual permite, a través de un procedimiento judicial simplificado y transfronterizo, en un plazo de 60 días a partir de la fecha de la detención, la entrega de una persona para el enjuiciamiento y ejecución de pena o medida de seguridad privativa de libertad en otros Estado miembro

de la Unión distinto de aquél en el que se encuentra detenido. Se realiza a través de las autoridades judiciales de los Estados miembros, lo que evita las injerencias políticas propias de las extradiciones. Además, dicha Orden trata de evitar, en treinta y dos categorías de delitos, que el Estado miembro donde se encuentra la persona detenida y a la cual se ha ordenado la entrega, puede denegar la misma por no existir el delito por el que se le acusa tipificado en su ordenamiento jurídico.

Se han dictado Directivas que obligan a los Estados miembros de la UE a legislar sobre el estatuto de la víctima y sobre el estatuto del investigado. Así, tenemos la Directiva 2012/29/UE del Parlamento Europeo y del Consejo, de 25 de octubre de 2012 por la que se establecen normas mínimas sobre los derechos, el apoyo y la protección de las víctimas de delitos. La Directiva 2013/48/UE del Parlamento Europeo y del Consejo, de 22 de octubre de 2013, sobre el derecho a la asistencia de letrado en los procesos penales y en los procedimientos relativos a la orden de detención europea, y sobre el derecho a que se informe a un tercero en el momento de la privación de libertad y a comunicarse con terceros y con autoridades consulares durante la privación de libertad, también es muestra sobre ello.

Asimismo, a través de la Directiva 2014/41/UE, se ha adoptado también la orden europea de investigación en materia penal, aprobada bajo presidencia española, cuyo objetivo es simplificar la obtención de pruebas transfronterizas. A través de un formulario sencillo se permite que un Estado miembro emita una orden para la ejecución de una medida de investigación en otro Estado distinto, sin que éste, salvo en casos tasados, pueda negarse a ello.

La Directiva 2014/42/UE del Parlamento Europeo y del Consejo sobre el embargo y el decomiso de los instrumentos y del producto del delito en la UE, asimismo, establece normas comunes para los Estados miembros respecto al embargo y decomiso del producto de ciertos delitos, así como de propiedades cuya procedencia sea resultado de conductas delictivas, es lo que se denomina decomiso ampliado. Además, en diciembre de 2016, la Comisión propuso la adopción de un nuevo Reglamento sobre el reconocimiento mutuo de las resoluciones de embargo y

decomiso. De hecho, se ha dictado el Reglamento 2018/1805, de 14 de noviembre de 2018, sobre el reconocimiento mutuo de las resoluciones de embargo y decomiso.

Hemos logrado tener instituciones que son el adalid de la cooperación en materia penal. Así mencionamos *Europol*, *Eurojust,* la Red Judicial Europea, los Equipos Conjuntos de Investigación y la Fiscalía Europea. Por ejemplo, el Parlamento Europeo ha reformulado las funciones y estructuras de *Eurojust*, para mejorar la efectividad de este órgano de forma que se permita facilitar las investigaciones transfronterizas y el enjuiciamiento de los delitos graves en el seno de la UE. La Fiscalía europea ha surgido en 2018 para combatir el fraude contra las finanzas de la UE, pudiendo investigar los delitos que afecten a los intereses financieros de la UE y ejercer la acción penal en los procesos penales que se sustancien al efecto.

Los esfuerzos de la UE en cooperación penal se centran en lograr el respeto del principio de reconocimiento mutuo. La realización del espacio de libertad, seguridad y justicia en la Unión se basa en la confianza mutua y en una presunción del respeto, por parte de los demás Estados miembros, del Derecho de la Unión y, en particular, de los derechos fundamentales. Ya, en el Consejo Europeo de Tampere, en octubre de 1999, quedó definido que el reconocimiento mutuo debería constituir la piedra angular de la cooperación judicial en materia penal. El principio del reconocimiento mutuo fue confirmado en los Programas de La Haya, en 2005 y de Estocolmo, en 2009. Sólo a través de este reconocimiento mutuo se podrá logar la superación de los problemas que existen por la existencia de diferentes legislaciones en los distintos miembros de la UE y por las diferencias entre los sistemas judiciales nacionales. Recordemos que el sistema de integración europea no se basa en la uniformidad de las legislaciones, sino en la armonización de las mismas. El principio de reconocimiento mutuo no podrá lograrse si no existe un alto grado de confianza mutua entre los Estados miembros.

En julio de 2018, los ministros de Justicia de los distintos países de la UE trabajaron en la Agenda de Justicia para el año 2020 y dentro de la misma discutieron cómo facilitar la obtención transfronteriza de pruebas.

En 2023, se dicta el Reglamento 2023/1543 del Parlamento Europeo y del Consejo, de 12 de julio de 2023, sobre las órdenes europeas de producción y las órdenes europeas de conservación a efectos de prueba electrónica en procesos penales y de ejecución de penas privativas de libertad a raíz de procesos penales. Para la UE es cada vez más necesario regular las medidas para obtener y conservar pruebas electrónicas de cara a las investigaciones penales.

El Reglamento pone el acento en los prestadores de servicios como punto importante para la obtención de pruebas para procesos penales. A estos efectos, los prestadores de servicios más importantes son los proveedores de servicios de comunicaciones electrónicas y los prestadores de servicios de la sociedad de la información, que permite la interacción entre los usuarios.

Los proveedores de servicios de comunicaciones electrónicas se definen en la 2018/1972 del Parlamento Europeo y del Consejo y son los que prestan servicios de comunicaciones interpersonales, tales como servicios de voz sobre IP, servicios de mensajería instantánea y servicios de correo electrónico.

La Directiva 2015/1535 del Parlamento Europeo y del Consejo se refiere a los servicios que permiten a sus usuarios la capacidad de comunicarse entre sí o les ofrecen servicios que puedan utilizar para almacenar o tratar datos su nombre. Esto incluye a los mercados en línea que proporcionan a los consumidores y las empresas la capacidad de comunicarse entre sí, otros servicios de alojamiento de datos, y también a los datos alojados en la nube y a las plataformas de juegos y a los juegos de apuestas en línea.

Los entidades que prestan servicios de infraestructura de *Internet* y que asigna nombres y números, como ocurre con los registradores y registros de nombres de dominio y los prestadores de servicios de privacidad y representación o registros regionales de direcciones de protocolo de *Internet* (IP), pueden identificar a los creadores de páginas *web* maliciosas o comprometidas, pues poseen datos que permite identificar a la persona física o jurídica responsable de esos sitios y que los utilizan para cometer delitos o, también permite identificar a la víctima de dicha actividad.

El Reglamento define cuándo el prestador de servicios tiene una conexión sustancial con la UE. Esto ocurre si tiene un establecimiento en la Unión o en caso de no tenerlo, existe un número significativo de usuarios en uno o más Estados miembros, o si las actividades se orientan hacia uno o más Estados miembros.

Y es que las direcciones IP, los números de acceso y la información conexa, es sin lugar a dudas, un dato esencial en una investigación penal, cuando no se conoce la identidad del autor del delito. Además, la IP constituyen el registro de una serie de acontecimientos tales como el comienzo y el final de la sesión de acceso de un usuario a un servicio. Es la dirección IP el que indica la interfaz de red utilizada durante la sesión de acceso, aunque a veces se necesita información adicional sobre el comienzo y el fin de una sesión de acceso de un usuario a un servicio, pues resulta habitual que las direcciones IP sean compartidas entre usuarios.

La dirección IP constituye un dato personal y goza de la protección que dispensa la norma. Incluso, las direcciones IP pueden considerarse datos de tráfico. Asimismo, los números de acceso y la información conexa se consideran datos de tráfico en algunos Estados miembros.

Si se produce una investigación en el seno de un proceso penal, las Fuerzas y Cuerpos de Seguridad del Estado pueden solicitar las autoridades policiales una dirección IP y los números de acceso e información conexa, para poder identificar al usuario, antes de que puedan solicitarse al prestador de servicios los datos de los abonados relacionados con ese identificador. Además, la dirección IP puede ser solicitada para conseguir información aún más sensible y que incide más la vida privada, tal es el caso de los contactos y el paradero del usuario, lo que puede suponer establecer un perfil de la persona afectada.

A estos efectos, se crea la orden europea de producción y la orden europea de conservación. En ambos casos, serán emitidas por una autoridad judicial, aunque excepcionalmente, si lo único que se pretende a través de ellas es la identificación del usuario, también puede ser emitida por un fiscal.

La orden europea de producción se utiliza para obtener pruebas específicas, como documentos, objetos o datos almacenados electrónicamente, que sean necesarios para una investigación o un proceso penal en curso. La orden europea de conservación se usa para preservar pruebas o evidencias que puedan ser relevantes para una investigación penal.

Debe tenerse en cuenta que las pruebas de los ciberdelitos únicamente se encuentran en soporte electrónico y éstas, como ya se ha dicho, tienden a desaparecer con mucha facilidad. Esta es la finalidad del Reglamento, y requieren de un tratamiento distinto a las restantes clases de pruebas. Esta norma también se aplica a aquellas actividades delictivas que estén castigadas una pena máxima privativa de libertad inferior a tres años.

Las órdenes europeas de producción, que se tramita a través de un documento que se llama EPOC y las órdenes europeas de conservación, que se tramitan mediante un documento denominado EPOC-PR, se dirigen al prestador de servicios, que actúa como responsable del tratamiento. Una vez recibido, el destinatario debe conservar los datos solicitados durante un máximo de sesenta días, a menos que la autoridad emisora confirme que se ha emitido una solicitud posterior de entrega, en cuyo caso la conservación debe mantenerse.

Los motivos de denegación de una orden europea de protección son tasados. Cabe oponerse, por ejemplo, si supusiese una vulneración manifiesta de un derecho fundamental previsto en el artículo 6 del Tratado de la UE y en la Carta de derechos fundamentales.

En definitiva, el Reglamento permite dirigir de forma segura, peticiones a los prestadores de servicios de comunicaciones electrónicas directamente por las autoridades judiciales nacionales. De esta forma, se garantiza que dicho prestador no pueda negarse a colaborar con la investigación penal, salvo que concurra motivo tasado en el propio Reglamento. Dado el carácter volátil de las evidencias electrónicas de los delitos cibernéticos, la creación de estos instrumentos basados en la cooperación una muestra eficaz de por dónde deben transcurrir los caminos de persecución y represión de los ciberdelitos.

4 Las particularidades de la investigación y de los procesos penales contra la ciberdelincuencia organizada

Como conocemos, *Internet* está constituido por un gran número de ordenadores conectados entre sí, formando pequeñas redes que, a su vez, se enlazan en la llamada «red de redes».

¿Qué hace un usuario para entrar en la red? Pues bien, lo primero es comunicar su equipo con un proveedor de acceso a *Internet* (ISP), a través de un operador de telecomunicaciones. El proveedor es, en definitiva, la compañía que permite a un cliente tener servicios de *Internet*. Esta empresa asignará un identificador, denominado IP (*Internet Protocol*) que identifica a cada usuario. Los números IP son únicos y están compuestos por cuatro grupos de números naturales que puede adquirir el valor de 0 hasta 225, número que están separados entre sí por puntos. Existen unos 4.000 millones de combinaciones diferentes. Ahora bien, como después diremos, a pesar de que nos pueda parecer que esas múltiples combinaciones, permiten casi infinitas direcciones IP, debido al tan número de dispositivos conectados a la red, resultan actualmente insuficientes.

Dos computadores diferentes pueden intercambiar información entre sí a través de unos protocolos de comunicación. Esa información se agrupa en paquetes, que se denominan «datos del tráfico». Y, ahí radica la dificultad, pues estos datos de tráfico no siempre se localizan fácilmente. Normalmente, 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.

Si se ha cometido un delito, para conseguir las evidencias y obtener los datos para poderlos presentar posteriormente en un proceso, en definitiva, para poder comprobar que se ha perpetrado el delito y cómo se ha perpetrado, lo primero que se precisa es conocer el número IP, en el momento de conexión a *Internet*. Además, tendrá que saberse el momento concreto de acceso cuando se cometió el hecho delictivo, será necesario identificar el ordenador, su ubicación y el abonado de la línea telefónica.

Estos elementos permitirán, tras la investigación policial, conocer el equipo desde el cual se realizó la acción, la ubicación del mismo, incluso, identificar al abonado. Pero esta identificación no supone haber encontrado al autor de la acción delictiva. Primeramente, porque el usuario puede ser otra persona distinta a aquélla que contrató los servicios de *Internet*[9]. En segundo lugar, porque la determinación de la dirección del emisor puede haber sido manipulada. Por último, porque se puede haber accedido desde un lugar público. Existen muchos métodos para evitar que se conozca quién es la persona que navega por la red: están las redes privadas virtuales (VPN), TOR, redes *wifi* compartidas en lugares públicos, en los que los usuarios pueden compartir sesión o pueden registrarse con datos falsos (Barrera Ibañez, 2018).

Los proveedores de servicio de *Internet* deben colaborar con la investigación y dar a los peritos informáticos de la policía la dirección IP; los datos contractuales del abonado; la hora, la fecha y la duración de la comunicación; la concreta transacción o intercambio efectuado; la localización geográfica desde la que se conecta el presunto autor con el proveedor; la cuenta corriente con la que se paga el servicio; el número de teléfono de origen y destino de las comunicaciones realizadas por sospechoso; la transacción o intercambio ilícito; la copia de los ficheros del presunto autor en su espacio web; las llamadas perdidas, hora, duración y frecuencia de las misma; los datos de fecha y el momento de activación de la tarjeta prepago de móviles y tantos otros datos necesarios para que el proceso penal pueda llevarse a cabo.

Por otra parte, en la investigación de un ciberdelito será preciso acceder a los servidores de *Internet*, los cuales suelen guardar un registro de sucesos de lo que ocurre en la navegación por la red, llamados *logs*.

9. Traemos en este punto a colación, la resolución del Tribunal de Justicia de la Unión Europea, el 18 de octubre de 2018. Según esta Sentencia, el titular de una conexión a *Internet*, a través de la que se han cometido infracciones de los derechos de autor mediante un intercambio de archivos, no puede quedar eximido de su responsabilidad designando simplemente a un miembro de su familia que tenía la posibilidad de acceder a dicha conexión.

Los profanos en materia informática, nos podemos preguntar qué son esos servidores y qué son esos *logs*. Un servidor es un equipo informático que forma parte de la red y que provee de servicios a otro equipo cliente. Es decir, un ordenador que provee de ciertos servicios a otros ordenadores. Los hay de diferentes tipos: servidor de archivos, de directorio, de impresión, de correo, de fax, *proxy, web,* de base de datos, DNS, etc. El servidor *web* o de *Internet* tiene como función almacenar páginas *web,* normalmente escritas en HTML (*HyperText Transfer Protocol*), poniéndolas al servicio de los usuarios que las necesitan. Así pues, los servidores de *Internet* almacenan ficheros que componen una página *web* y contienen diferentes fragmentos que controlan la forma en la que los usuarios pueden acceder a estos ficheros, información toda ella de vital importancia para la investigación de un ciberdelito.

Se ha dicho que los servidores suelen almacenar un registro de sucesos, llamados *logs*. ¿Qué es un *log*? Un historial o un registro, una grabación secuencial en un archivo o en una base de datos de todos los acontecimientos que se realizan en la navegación por *Internet*. Así, un *log se* constituye en una evidencia del comportamiento del usuario en la red.

Los equipos informáticos personales no suelen guardar, a diferencia de los servidores, *logs*. En este supuesto, si se quisiera investigar los rastros de un delito, directamente en un ordenador personal, será necesario incautar, registrar y realizar un posterior *back-up* de la información contenida en aquél, para investigar las evidencias del mismo.

Además, de todo lo anterior, debemos referirnos a la tecnología *Network Address Translation* (NAT). Expliquemos en breves palabras qué significado tienen estas palabras casi ininteligibles y la dificultad que supone para la investigación penal. Debido al gran número de dispositivos que se conectan a la red y sabiendo que cada usuario necesitará una IP diferente para cada aparato que acceda a *Internet*, en los últimos tiempos, se está produciendo el agotamiento de las direcciones IP. Por ello, se ha ideado un sistema que permite conectar varios terminales a través de una única dirección IP (IP pública). Esto permite que grandes compañías puedan acceder a *Internet* con esa única IP pública,

con independencia de los aparatos que tengan en la misma, incluso que la conexión que realizamos a *Internet* desde nuestros hogares se pueda hacer desde un *router* al cual queden unidos todos los dispositivos ubicados en el mismo. La identificación del ordenador concreto desde el que se cometió el delito, cuando dicho ordenador se conecta a la red a través de NAT, resultará, como puede suponerse, mucho más complejo.

Cuando se trata de conexiones desde dispositivos móviles, los problemas son aún mayores. Un celular es un receptor-transmisor, el cual permite la comunicación entre personas mediante ondas electromagnéticas de radiofrecuencia. En la actualidad, los celulares utilizan tecnología digital, es, por ello, por lo que los mensajes de voz son transformados en códigos de dígitos binarios, quedando convertidas las conversaciones en paquetes de datos agrupados, según un lenguaje preestablecido.

Para que se pueda producir una conexión inalámbrica, es necesario que, en cada tramo de terreno en el que se quiera que exista cobertura, llamado técnicamente «célula», se instale una antena. Esas antenas receptoras-emisoras, junto a la estación base y a otros equipos electrónicos, permiten hablar y conectarse a *Internet* a las personas que estén situadas en el momento de la conexión en el territorio de esa célula (Martil, 2017). En un mundo en continuo movimiento, donde las personas vamos y venimos de un lado a otro, nos podemos preguntar cuántas antenas a lo largo de un día han podido darnos cobertura en nuestras conexiones inalámbricas. A todo ello hemos de unir una dificultad más y es que los celulares se conectan a *Internet* con una IP pública (NAT). La investigación de la comisión de un hecho delictivo cometido desde un celular podrá permitir averiguar la última antena desde la que se conectó este teléfono, pero debemos tener presente que, al mismo tiempo, habrá habido otros miles de celulares conectados desde esa misma antena. Si todos esos miles de celulares se conectan a través de una misma IP pública, resultará del todo imposible individualizar desde cuál fue cometido el hecho delictivo.

La utilización del protocolo IPV6, en lugar del IPV4, permite asignar direcciones IP a cada uno de los dispositivos en cada una

de las conexiones. El protocolo IPV6 permite que un número ilimitado de dispositivos se puedan conectar a *Internet* al mismo tiempo. La UE ha luchado mucho para que sea obligatorio y hoy, ya es una realidad. (Barrera Ibáñez, 2018).

Como puede observarse, el control, el seguimiento y el acceso a los datos de la navegación *web* por parte de la policía supone la limitación de derechos fundamentales de los ciudadanos, en este caso, del derecho a la intimidad y del secreto de las comunicaciones. La policía deberá realizar intervenciones telefónicas, rastrear IP, acceder de forma remota a los dispositivos desde los cuales se realiza la navegación por la red, obtener datos de los proveedores de servicios de *Internet* y de los contenidos en servidores, incluso incautar y registrar dispositivos de almacenamiento masivo de información, para su posterior análisis de su contenido, actuaciones todas ellas que suponen una importante limitación de los derechos fundamentales. Podemos incluso, hablar del derecho a la inviolabilidad del domicilio, puesto que, para incautar un ordenador, será precisa la entrada y registro domiciliario, en el lugar en que se encuentren, para lo que será necesario la correspondiente autorización judicial.

Las dificultades de la investigación penal del cibercrimen no acaban aquí, pues es necesario el análisis de la información, posteriormente, la redacción del correspondiente dictamen pericial y la intervención del perito en el juicio. Para poder realizar el análisis de los datos será ineludible la realización de ciertas operaciones técnicas, entre ellas, el «volcado» de la información obtenida, que se realiza a través de una copia del soporte original, aunque siempre se deberá guardar el original. Asegurar la cadena de custodia es lo más importante en ese momento. Por ello, para garantizar que el original y la copia sean iguales, y no tener después problemas con la nulidad de la prueba, ese volcado se suele realizar en presencia de un fedatario público y de forma simultánea al registro domiciliario e incautación de los ordenadores. El Letrado de la Administración de Justicia, cuya presencia se exige como fedatario público, en una diligencia de entrada y registro domiciliario, podrá acreditar la autenticidad de la copia que se realice, si es que el volcado se efectúa en ese mismo momento. Si no fuera así, el Letrado de la Administración

de Justicia será el que habrá de remover los precintos impuestos durante la entrada y registro domiciliario y en la diligencia de incautación de los distintos equipos informáticos hallados en el lugar. Una vez realizado el volcado, los precintos deben mantenerse, para garantizar la cadena de custodia de la prueba (Rayón Ballesteros y Gómez Hernández, 2014).

La redacción del dictamen pericial y la posterior actuación en la vista oral del perito tiene también sus complejidades, que analizaremos posteriormente. Pero lo que nos importa en este momento es insistir en la necesidad de conservar siempre los dispositivos originales de donde se hayan extraído las pruebas. Por este motivo, deberán estar en custodia del Letrado de la Administración de Justicia, que garantizará su conservación y puesta a disposición del juez, si ésta fuera precisa.

Pero la ciberdelincuencia no sólo plantea problemas en la investigación del delito, sino también en cuanto al proceso mismo. Al tratarse de delitos transnacionales, puede ocurrir que la conducta delictiva produzca resultados en Estados distintos de aquéllos donde se cometió, incluso puede ser que el hecho delictivo tenga su origen en uno o varios países. Obviamente, todo ello afecta a cuestiones tan básicas como la jurisdicción, la competencia jurisdiccional, la ley penal aplicable y al procedimiento que se tramitará para su investigación y enjuiciamiento. Las reglas clásicas, tales como la relativa al principio de territorialidad, según la cual el hecho delictivo se enjuiciará en el lugar de su comisión (*locus comissi delicti*) ya no tienen cabida (Rayón Ballesteros y Gómez Hernández, 2014).

5 La prueba electrónica transfronteriza

5.1 Prueba electrónica: concepto y clases

Entendemos por prueba electrónica toda información que puede ser usada como prueba en un proceso, bien contenida en un medio electrónico o bien transmitida por ese medio (Delgado Martín, 2016).

El motivo por el que hablamos de esta clase de prueba no es otro, como se ha explicado anteriormente, que el hecho de que las evidencias que permiten demostrar la existencia de un ciberdelito son de carácter electrónico.

Resulta indiferente si la información se ha creado, se almacena o se transmite por medios electrónicos y también es intrascendente qué tipo de información sea. Lo relevante es que se encuentre contenida o sea transmitida por medios electrónicos y que sirva para acreditar los hechos dentro de un proceso penal. Como estamos analizando la ciberdelincuencia, hablamos de la prueba electrónica que permite probar la comisión de un hecho delictivo en un proceso penal.

Recodemos que, cuando nos referimos a la prueba, este concepto puede estar referido bien al resultado, bien al medio de prueba o bien a la actividad que realizan las partes para convencer al juez de la certeza de los hechos controvertidos en el proceso. Asimismo, se ha de diferenciar dos términos que no significan lo mismo: fuente y medio de prueba. Concretamente, en el ámbito de la prueba electrónica, se entiende fuente de prueba aquella información contenida o transmitida por medios electrónicos. El medio de prueba es, sin embargo, la forma a través de la que la fuente de prueba accede al proceso penal (Delgado Martín, 2016).

Hoy contamos con muy variados elementos electrónicos, que han ido evolucionando a gran velocidad en los últimos años. Cuando nos estábamos acostumbrando a los *Cd-Rom*, llegaron los *DVD*, para ser sustituidos rápidamente por las memorias *USB* y, éstas, posteriormente, por el almacenamiento de datos en la nube. Igual sucedió en el ámbito de la telefonía móvil. Los teléfonos que sólo servían para llamar, pasaron a mejor vida, pues todo el mundo accedió a los *smartphones* (con sistema *Android* o *iOS*), que permiten realizar llamadas, enviar mensajes, utilizar los sistemas de mensajería instantánea y la navegación por *Internet*. Los ordenadores de consola siguen existiendo, pero comparten vida con los portátiles, con las tabletas, los reproductores de MP3 o MP4 o, las PDAs. Quién de nosotros no lleva en su vehículo un sistema de navegación que le permite ser rastreado a través de GPS y conocer las carreteras y el camino por dónde llegar a los lugares. Estos elementos electrónicos nos

permiten hablar de diferentes fuentes de prueba electrónica, tales como el correo electrónico, el SMS, la mensajería instantánea o las redes sociales.

Por otra parte, los medios de prueba son los tradicionales en cualquier procedimiento: documental, interrogatorio de partes, testifical, pericial, reconocimiento judicial u otros medios que permiten la reproducción de imágenes, sonidos, etc. Tengamos presente, por ejemplo, que en la Ley española 1/2000, de 7 de enero, de Enjuiciamiento Civil (en adelante LEC), el art. 299, diferencia la prueba documental de los medios de reproducción de imágenes, sonido e imagen y otros que permiten archivar y conocer o reproducir palabras, datos, cifras y operaciones matemáticas llevadas a cabo con fines contables o de otra clase.

Además, existen dos clases de prueba electrónica: a) los datos o informaciones almacenados en un dispositivo electrónico; y, b) los que son transmitidos por cualesquiera redes de comunicación abiertas o restringidas como *Internet*, telefonía fija y móvil u otras.

5.2 Fases de la prueba electrónica

Las fases de esta clase de prueba no son diferentes a las de otro tipo. En primer lugar, ha de obtenerse; en segundo lugar, ha de incorporarse al proceso y; por último, ha de valorarse por el juez.

5.2.1 Obtención de la prueba electrónica

Para poder obtener la prueba electrónica, podrá ser precisa la aprehensión y registro del aparato en el que se encuentra la misma. Incluso puede ser necesaria la entrada y registro en lugares no públicos.

En España y, tras la entrada en vigor de la 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, según el art. 588 *sexies* a, la aprehensión de ordenadores o de registro de dispositivos de almacenamiento masivo de información requiere ser

autorizada también por el juez, no estando permitido a las Fuerzas y Cuerpos de Seguridad del Estado aprovechar la entrada y registro domiciliarios para registrar dichos aparatos, sin que el juez haya motivado las razones que legitiman el acceso de los agentes facultados a la información contenida en tales dispositivos.

Otras veces la prueba electrónica de la comisión de un hecho delictivo será fruto del acceso a través de datos de identificación, códigos o por medio de la instalación de un *software*, que permitan, de forma remota y telemática, el examen a distancia y sin conocimiento de su titular o usuario del contenido de un ordenador, dispositivo electrónico, sistema informático, instrumento de almacenamiento masivo de datos informáticos o base de datos. Es aquí donde cobra importancia la obtención de la prueba electrónica en la delincuencia transfronteriza, pues cuando los datos se localizan en un servidor situado fuera del territorio de un Estado surgen las dificultades.

La prueba electrónica no sólo puede ser obtenida por la intervención de las Fuerzas y Cuerpos de Seguridad del Estado, sino en ocasiones por los propios particulares. Tengamos presente que las personas hoy día se comunican a través de correos electrónicos, *whastapps*, redes sociales, etc. Esas informaciones, que pueden contener pruebas de delitos, pueden ser obtenidas por uno de los propios comunicantes, por un tercero o, incluso por el acceso a información contenida en páginas *web*.

Dadas las especiales características de la prueba electrónica, lo importante es no vulnerar derechos fundamentales, pues si así fuera, estaríamos ante una prueba ilícita, que viciaría no sólo las obtenidas de forma directa sino también indirectamente, en aplicación de la teoría del árbol de los frutos envenenados. Son varios derechos fundamentales los que pueden quedar afectados: intimidad personal, propia imagen, secreto de las comunicaciones, la protección de los datos personales o la inviolabilidad del domicilio. En España, según el art. 11 de la LOPJ, no surtirán efecto las pruebas obtenidas, directa o indirectamente, violentando los derechos o libertades fundamentales.

Los derechos fundamentales no sólo deben de ser respetados por los poderes públicos, sino también por los particulares, a

esto se denomina eficacia horizontal de los derechos fundamentales o *Drittwirkung*, expresión alemana que significa eficacia hacia terceros. Nada impide que un sujeto aporte a un proceso judicial como prueba un correo electrónico, un *whastapp* o incluso, una grabación de una conversación telefónica, mantenida entre dos personas, siempre que la aportación se produzca por uno de los intervinientes en el proceso comunicativo. En el ordenamiento jurídico español, el derecho a la aportación al proceso de grabaciones de conversaciones particulares realizadas por uno de sus protagonistas no vulnera el derecho al secreto de las comunicaciones. Y, como han dejado dicho Sentencias, entre otras, del Tribunal Constitucional 114/1984, de 29 de noviembre y del Tribunal Supremo de 9 de julio de 1993, ese derecho no puede esgrimirse frente a los propios intervinientes en la conversación o, podemos decir, comunicación.

Pero para conocer, por ejemplo, si los derechos fundamentales quedan afectados por la obtención de la prueba electrónica y si, por ejemplo, la policía debe solicitar o no autorización judicial para acceder a una prueba electrónica sin que esta intromisión sea ilegítima o ilícita es preciso conocer si la comunicación o el medio a través del cual se está transmitiendo una información es de carácter público o privado. Esto no es tan sencillo como a *priori* pudiera parecer. Lo primero que se necesita es analizar el tipo de comunicación utilizado y determinar si éste es apto para mantener una comunicación privada, existiendo casos realmente dudosos. Pensemos, en una página *web*. En principio, parece una comunicación pública y, aunque el acceso sea restringido, la interceptación por la policía de su contenido sin autorización judicial no vulneraría el secreto de las comunicaciones. Las publicaciones que se realizan en abierto en *Facebook*, por ejemplo, han sido calificadas por algunos Tribunales españoles, como información pública y, por tanto, pueden ser aportadas como pruebas en los procesos[10].

Plantemos también el caso de aquellos supuestos en los que la comunicación es privada, no siendo completamente cerrada,

10. Véase, por ejemplo, la Sentencia del Tribunal Superior del Tribunal Superior de Justicia de Las Palmas de Gran Canaria 19/2016 de 22 de enero, aunque referida al ámbito laboral.

al requerir el conocimiento o intervención de un tercero, como ocurre con el caso de un correo electrónico. Pues bien, la interceptación de un correo electrónico, requiere en todo caso la autorización judicial, pues se trata de una comunicación privada, a pesar de que en esa clase de comunicación deba intervenir el servidor de prestación de servicios de *Internet* (Volpato, 2016).

Todos sabemos que la conversación mantenida entre dos personas a través de un teléfono celular es privada y, por ende, está protegida por el derecho al secreto de las comunicaciones, pero ha de tenerse en cuenta que el aparato también se utiliza para el acceso a páginas *web*, para intercambiar mensajes instantáneos, para realizar fotografías o consultar correos electrónicos. Está en juego el derecho a la intimidad. Por ello, la policía, para poder acceder y registrar el contenido de un teléfono celular y obtener así una prueba electrónica, necesitará igualmente autorización judicial. El juez debe autorizar, en su auto, el posible acceso de la policía a todos aquellos elementos que contiene, pues en ese dispositivo, se albergan datos de contactos, fotografías, mensajes, correos electrónicos, etc. Actualmente, el derecho a la intimidad incluye el «entorno virtual» de una persona, tal y como se afirma en la Sentencia del Tribunal Supremo español 786/2015, de 4 de diciembre. En esta Resolución se nos dice que «La jurisprudencia de esta Sala ha recordado la necesidad de que exista una resolución jurisdiccional habilitante para la invasión del derecho al entorno digital de todo investigado».

5.2.2 Incorporación de la prueba electrónica al proceso

La incorporación de la prueba electrónica en un proceso, en nuestro caso penal, requiere que dicha prueba cumpla con los requisitos generales concretados por la teoría general de la prueba: pertinencia, utilidad y licitud. No es el momento de tratarlos, pues son de carácter general y no sólo aplican a la prueba electrónica. Interesa mucho más referirnos al modo en que la prueba electrónica accede al proceso. Hablemos, pues de los medios de prueba.

Como conocemos, los medios de prueba son: documental, interrogatorio de partes, testifical, pericial, reconocimiento judicial u otros medios que permiten la reproducción de imágenes, sonidos, etc.

Hablemos de la prueba documental y de la prueba pericial que son la que presentan especificaciones más significativas en el ámbito de la prueba electrónica.

Los documentos pueden clasificarse en torno a tres categorías tradicionalmente: públicos, privados y oficiales. Los documentos públicos son aquéllos en los que ha intervenido un fedatario público. Los privados, por el contrario, en los que no hay dicha intervención. Los oficiales en los que ha intervenido un funcionario con facultad certificante de las Administraciones Públicas, en relación con los actos administrativos de éstas.

Una prueba electrónica podría acceder al proceso a través de un documento en formato papel, pero también en forma de documento electrónico. En este caso, la prueba se aporta al proceso en soporte electrónico, bien a través de una memoria *USB*, un *DVD* o cualquier otro medio que permita el almacenamiento de datos. Lo que sucede, por ejemplo, es que, tradicionalmente, por documento se entiende sólo aquél que se encuentra en soporte papel. Según la LEC española entrarían en el proceso, a través del art. 299.2 como otros medios de reproducción de imágenes, sonido e imagen y otros que permiten archivar y conocer o reproducir palabras, datos, cifras y operaciones matemáticas llevadas a cabo con fines contables o de otra clase.

Los documentos electrónicos, por su parte, también pueden ser públicos, privados u oficiales.

Entre los documentos electrónicos públicos se incluyen las resoluciones y diligencias de actuaciones judiciales de toda especie y los testimonios que de las mismas expidan los Letrados de la Administración de Justicia, pues hoy contamos con el procedimiento judicial electrónico y, de hecho en España, tras la entrada en vigor de la Ley 18/2011, de 5 de julio, reguladora del uso de las tecnologías de la información y la comunicación en

la Administración de Justicia, el expediente judicial electrónico es una realidad en nuestro proceso. También existen los documentos notariales electrónicos, los cuales tienen el mismo valor que los expedidos en soporte papel[11]. La copia electrónica de los documentos notariales existe desde el año 2002, en España y, se regulan en el art. 17 *bis* de la Ley de 28 de mayo 1862, Orgánica del Notariado.

La Ley 11/2023, de 8 de mayo, de trasposición de Directivas de la UE en materia de accesibilidad de determinados productos y servicios, migración de personas altamente cualificadas, tributaria y digitalización de actuaciones notariales y registrales; y por la que se modifica la Ley 12/2011, de 27 de mayo, sobre responsabilidad civil por daños nucleares o producidos por materiales radiactivos, es la que regula el nuevo Protocolo electrónico notarial. Hoy día, la matriz digital es una realidad[12].

Los documentos oficiales, como se ha dicho, son los firmados por funcionarios en el ejercicio de sus funciones. Actualmente, podemos relacionarnos con la Administración Pública a través de documentos electrónicos, tal y como sucede en España, des-

11. El artículo 17 *bis* de la Ley de 28 de mayo 1862, Orgánica del Notariado asevera que «Los instrumentos públicos a que se refiere el art. 17 de esta Ley, no perderán dicho carácter por el solo hecho de estar redactados en soporte electrónico con la firma electrónica avanzada del notario y, en su caso, de los otorgantes o intervinientes, obtenida la de aquél de conformidad con la Ley reguladora del uso de firma electrónica por parte de notarios y demás normas complementarias». En el apartado 2, párrafo b), sigue diciendo «Los documentos públicos autorizados por Notario en soporte electrónico, al igual que los autorizados sobre papel, gozan de fe pública y su contenido se presume veraz e íntegro de acuerdo con lo dispuesto en esta u otras leyes».
12. El art. 17 ha sido modificado, adicionando un apartado 4, según el cual: «Las matrices de los instrumentos públicos tendrán igualmente reflejo informático en el correspondiente protocolo electrónico bajo la fe del notario. La incorporación al protocolo electrónico o libro registro de operaciones electrónico se producirá en cada caso con la autorización o intervención de la escritura pública o póliza, de lo que se dejará constancia mediante diligencia en la matriz en papel expresiva de su traslado informático. Los instrumentos incorporados al protocolo electrónico se considerarán asimismo originales o matrices. En caso de contradicción entre el contenido de la matriz en soporte papel y del protocolo electrónico prevalecerá el contenido de aquella sobre el de este».

de la entrada en vigor de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas[13].

Es claro que la comunicación entre particulares ha cambiado significativamente, pues hoy se generan cantidad de documentos electrónicos, como son los correos electrónicos. Esos son documentos electrónicos privados. Existen, también, las facturas electrónicas. El Real Decreto 1619/2012, de 30 de noviembre, por el que se aprueba el Reglamento por el que se regulan las obligaciones de facturación se refiere a las mismas.

Los documentos electrónicos privados presentan una seria dificultad, pues al no haber intervenido en su confección una autoridad que acredite su autenticidad resulta muy fácil alterar su contenido. El correo electrónico se puede aportar como documento en soporte papel o en soporte electrónico. Si se presentase en soporte papel, bastaría con usar una aplicación disponible en el sistema operativo *Windows*, para alterar su exactitud. Pero en ambos casos es muy fácil adulterar la autenticidad, su exactitud o su integridad, debiéndose practicar una prueba pericial, para averiguar todos estos extremos. La única posibilidad que existe para garantizar la autenticidad de un correo electrónico es el *email* certificado, que se envía a través de proveedores, que otorga veracidad al propio correo, al contenido, a la fecha de envío y de recepción, y a las direcciones IP de envío y de recepción[14].

Con el sistema de mensajería instantánea de *whatsapp* ocurre otro tanto de lo mismo. Y es que existen *apps* que, aunque creadas con una finalidad de diversión, permiten sustituir conversaciones reales por otras falsas, alterar la hora de envío, el

13. El art. 14 de dicha Ley contempla: «Las personas físicas podrán elegir en todo momento si se comunican con las Administraciones Públicas para el ejercicio de sus derechos y obligaciones a través de medios electrónicos o no, salvo que estén obligadas a relacionarse a través de medios electrónicos con las Administraciones Públicas. El medio elegido por la persona para comunicarse con las Administraciones Públicas podrá ser modificado por aquella en cualquier momento».
14. En España, existen varios proveedores como son *EGarante, MailCertificado, Lleida.NET.*

estado de recepción, modificar el emisor del mensaje, crear audios, vídeos y fotos como si hubieran sido enviados verdaderamente. También posibilitan alterar los ajustes de los perfiles y estados de las personas implicadas (Picón Rodríguez, 2017). Así, para que las pruebas contenidas en sistemas de mensajería instantánea puedan ser válidas en un proceso, éstas deben estar certificadas y autentificadas y ello sólo se consigue a través de un perito informático. En la Sentencia del Tribunal Supremo 300/2015, se afirma la necesidad de aportar una prueba pericial que identifique el origen real de la conversación, la identidad de los interlocutores y la integridad del contenido.

Los «pantallazos» son también pruebas electrónicas, pues son impresiones digitales de un escritorio o pantalla de un aparato electrónico. Estos pantallazos se puedan aportar en formato papel o bien de forma electrónica, pero sea como fueran aportados son fácilmente manipulables. Como todos conocemos, existen programas informáticos de edición de imágenes con los resulta bastante sencillo alterar esas representaciones.

Refirámonos ahora a la prueba pericial informática. Como se ha visto, las evidencias electrónicas resultan altamente manipulables. Por este motivo, en la mayoría de las ocasiones, resultará necesario practicar una prueba pericial informática en el proceso judicial que permita acreditar la autenticidad, exactitud y la integridad de una prueba electrónica, por ejemplo, de un correo electrónico o de un *whastapp*. Al mismo tiempo, cuando la Policía registra e interviene un ordenador a través del cual se ha cometido un hecho delictivo, se necesitará la intervención de un perito para extraer, preservar, analizar y documentar los datos allí almacenados.

Así la prueba pericial informática puede definirse como aquél medio de prueba, mediante el cual una persona experta en temas informáticos aporta al juez los conocimientos técnicos que le permitan valorar y tener como probados los hechos, en este caso, delictivos, que se encuentran en dispositivos electrónicos o informáticos. Este medio de prueba, tal y como se ha expuesto, puede resultar complementario de otros medios, tal y como sucede cuando lo que se quiere es acreditar la autenti-

cidad, exactitud e integridad de una prueba electrónica o puede ser autónomo.

¿Qué puede analizar un perito informático? Desde un soporte portátil, como puede ser una memoria *USB* o un disco duro extraíble, hasta un ordenador portátil o de sobremesa, incluyéndose los datos almacenados en los discos duros; también celulares, tanto la tarjeta *SIM*, como la memoria interna o memorias adicionales. Asimismo, *GPS* de los vehículos, tarjetas de televisión de pago, lectores de bandas magnéticas, teclados de cajeros bancarios o un clonador de tarjetas bancarias de crédito o de débito.

Esta prueba tiene una especial dificultad, primeramente, porque el perito debe obtener los datos.

Una vez obtenidos, debe realizar un clonado de los mismos, debiendo siempre conservarse el original hasta el momento del juicio. Será sobre la copia clonada, sobre la que el perito podrá realizar las intervenciones que necesite para elaborar el dictamen posterior que después se aportará en el proceso.

¿Qué significa clonar? El clonado supone una copia espejo o *bit a bit* de la información original contenida en el dispositivo. Además, realizará una segunda copia, que quedará en manos del titular de los datos, para que éste pueda seguir realizando su actividad. En definitiva, clonar se refiere al proceso de crear una copia exacta o duplicado de una información digital, pudiendo ser un dispositivo móvil o de un sistema operativo, *software* o conjunto de datos.

Clonar y copiar son términos distintos: clonar implica crear una réplica exacta, de modo que la copia sea idéntica al original, incluyendo configuraciones y datos. Copiar significa duplicar o reproducir un objeto, archivo o información, pero no necesariamente implica que la copia sea idéntica al original en todos los aspectos. En informática, por ejemplo, copiar un archivo simplemente implica duplicar su contenido en otro lugar, pero no necesariamente incluye configuraciones. Esas configuraciones son los llamados metadatos, que todo archivo digital tiene, y van asociados con el archivo original. Los metadatos son datos que

proporcionan información sobre otros datos, es decir, es la información adicional que acompaña a archivos, mensajes o recursos digitales, proporcionando detalles sobre su origen, contenido, formato, autoría y más[15]. Aquí tienes algunos ejemplos de metadatos comunes:

En el ámbito de la ciberdelincuencia, los peritos informáticos suelen pertenecer a unidades especializadas de la policía. En España, contamos con el Departamento de delitos telemáticos de la Guardia Civil y con la Brigada de Investigación Tecnológica de la Policía Nacional, de los cuales forman parte ingenieros o informáticos. Éstos técnicos son diferentes a quienes realizan la incautación de los dispositivos, pues son los que obtienen los datos, realizan el clonado y realizan el dictamen pericial. También son los que averiguan y analizan las IP de los usuarios que navegan por *Internet*.

En la investigación criminal existen tres cuestiones vitales a tener en cuenta. La primera tiene que ver con las actuaciones que realiza la Policía, pues tras la entrada y registro, es preciso que se identifiquen y se aíslen aquellos dispositivos desde los que se ha cometido la acción criminal. Asimismo, los agentes intervinientes deben precintarlos, de modo que cuando se realice el clonado, pueda acreditarse que la copia procede del dispositivo intervenido. Seguramente, la Policía tomará testimonios a los sujetos que puedan conocer datos relevantes, para después poder tener más evidencias sobre los hechos delictivos. La segunda cuestión tiene que ver con la cadena de custodia del material clonado por el técnico. En muchas ocasiones, el clonado se realiza en el mismo acto de la intervención policial, para asegurar la inmediatez y evitar así el borrado de datos que pudieran resultar de importancia para la investigación penal. Junto al técnico,

15. Refirámonos, por ejemplo, a los metadatos de un archivo de imagen: Fecha y hora de la creación o modificación, resolución de la imagen, modelo de cámara utilizado para capturar la imagen, configuración de la cámara (apertura, velocidad de obturación, ISO, etc.) y nombre del autor o fotógrafo. O a los metadatos de correos electrónicos: dirección de correo electrónico del remitente; direcciones de correo electrónico de los destinatarios, fecha y hora del envío; asunto del correo electrónico e información sobre los servidores de correo utilizados en la entrega del mensaje.

suele estar el fedatario público (Letrado de la Administración de Justicia), que es quien acredita que los datos están siendo extraídos del dispositivo que se ha intervenido y sólo cuando dicho fedatario ha removido los precintos. En tercer y último lugar, debe asegurarse que la copia clonada no sufra daños, para que, en caso de ser necesario, pueda accederse a ella. Es por esta cuestión, por la que quedará en custodia del Letrado de la Administración de Justicia, que es el encargado de preservar las piezas de convicción.

Tras todo este proceso el perito deberá redactar su dictamen, en el cual dejará constancia del método científico utilizado y de la fuente del que proceden los datos analizados (ordenador, teléfono celular, memoria *USB*, etc), de las operaciones que ha realizado, de su titulación y currículum, para que el juez pueda valorar la prueba. Como todos conocemos, el perito podrá intervenir en la vista oral, para exponer, explicar, aclarar o responder a preguntas, sobre método, premisas, conclusiones y otros aspectos del dictamen.

5.2.3 Valoración de la prueba electrónica

A la hora de valorar la prueba electrónica, se seguirán los criterios que las leyes procesales establezcan. Recordemos que, en la mayoría de las ocasiones, se aplicará el principio de libre valoración de la prueba, que supone la aplicación de las reglas de la sana crítica y de la experiencia general o especial, dada por el perito. En el ordenamiento jurídico español, el art. 741 del Real Decreto de 14 de septiembre de 1882 por el que se aprueba la Ley de Enjuiciamiento Criminal (en adelante, LECr) nos dice que «El Tribunal, apreciando según su conciencia las pruebas practicadas en el juicio, las razones expuestas por la acusación y la defensa y lo manifestado por los mismos procesados, dictará sentencia dentro del término fijado en esta Ley», pero deja sin concretar las reglas de valoración de la prueba. Hemos de aplicar el derecho fundamental a la presunción de inocencia (art. 24.2 de la Constitución Española) y el principio *in dubio pro reo*.

En el proceso civil español, los documentos públicos, al haber sido intervenidos por fedatario público, se salen del criterio de libre valoración de la prueba y hacen prueba plena de los datos obrantes en ellos (art. 319 de la Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil, en adelante LEC). También, los documentos privados suelen tenerse por válidos siempre que la parte a quien perjudique no impugne su autenticidad. (art. 326 de la LEC).

Entendemos el primer caso de aplicación al proceso penal, dada el carácter supletorio de las normas procesales civiles en el seno de los procesos que se sustancian ante otros órdenes jurisdiccionales. Sin embargo, creemos que, dada la vigencia del principio de oficialidad en los procesos penales, el juez no esperará a la impugnación por la parte contraria de la autenticidad de un documento en papel o electrónico, sobre todo teniendo en cuenta la gran manipulación que puede darse de estos últimos. En la LECr, el art. 729.2 permite al juez o tribunal practicar las diligencias de prueba no propuestas por ninguna de las partes, que el Tribunal considere necesarias para la comprobación de cualquiera de los hechos que hayan sido objeto de los escritos de calificación. Cierto es que este precepto ha sido interpretado por el Tribunal Supremo, en Sentencias de 23 de septiembre de 1995 y de 7 de abril de 1999, según el principio acusatorio, permitiendo al juez practicar prueba cuando sea para corroborar o rebatir las pruebas propuestas por las partes. El Ministerio Público será seguramente el encargado de solicitar al juez practicar prueba sobre la autenticidad y exactitud de la evidencia electrónica.

6 Problemas para la prevención, la investigación y la represión de la ciberdelincuencia transnacional. Dificultades para la obtención de la prueba electrónica en la delincuencia transfronteriza europea

Enumeremos, a continuación, los problemas de la investigación y represión de la ciberdelincuencia organizada y transnacional.

- La tecnología facilita la perpetración de delitos y su rápida propagación, debido a los miles de personas que utilizan *Internet*.

- La tipificación de las conductas ilícitas resulta complicada, pues son hechos nuevos y de carácter tecnológico, que en muchas ocasiones cuentan con el desconocimiento del Legislador.

- El desconocimiento de los jueces, que no tienen conocimientos específicos en la materia. También, el de los demás operadores jurídicos.

- Por mucho que los instrumentos normativos permitan formar equipos conjuntos de investigación, falta de recursos humanos y materiales, para la prevención, la investigación y la represión. Los jueces llevan múltiples asuntos, si además de toda la carga de trabajo tienen que solicitar comisiones rogatorias o, aunque sea dentro de la UE una orden europea de investigación o una orden europea de conservación de una evidencia electrónica dejarán de atender otros asuntos.

- El anonimato de la navegación por la red y la dificultad de la investigación tecnológica y de la obtención, análisis y preservación de las evidencias. La navegación anónima permite, asimismo, la ocultación de los rastros de los delitos. Como se ha insistido las pruebas electrónicas desaparecen con mucha facilidad; en este sentido se habla de la volatilidad de las pruebas digitales.

- La navegación por *Internet* no permite controlar ni el flujo ni la transmisión de información.

- La extraterritorialidad, que supone problemas concretos para determinar la jurisdicción y competencia a la hora de iniciar un proceso penal.

- La falta de homogeneidad de las legislaciones, incluso europeas.

- La estructura y medios con los que cuentan los ciberdelincuentes.

Las dificultades procesales para luchar contra la ciberdelincuencia en Europa son menores, pues las órdenes de investigación europea, de producción y conservación de las pruebas digitales, así como el Convenio de asistencia judicial mutua han ayudado. La cooperación de órganos como *Europol o Eurojust*, también.

Sin embargo, los instrumentos legislativos enunciados no están exentos de problemas. Sin ánimo de ser exhaustivos podemos mencionar la amplitud de plazos para el reconocimiento y ejecución de una orden, pudiendo extenderse dicho plazo hasta ciento cincuenta días, produciendo la dilación del procedimiento y, en definitiva, la ineficacia de dicha orden. La volatilidad de las pruebas electrónicas hace que, por muy rápida que sea la tramitación de la orden europea de investigación, cuando ésta llegue pueda ser que la evidencia no exista (De Hoyos Santo, 2023, p. 102).

La necesidad de traducción de la orden es otra de las dificultades. Pensemos en lo necesario que resulta una clara comprensión o los problemas que pueden darse si se mal interpretan los hechos delictivos descritos.

Además, debe tenerse en cuenta la escasa formación de los distintos operadores jurídicos. Bienvenidos sean los instrumentos legales de cooperación, pero pensemos en quién los utilizan y aplican: jueces y abogados que no están acostumbrados a los mismos. El cambio de paradigma de la delincuencia que responde a los parámetros de transnacional, organizada y ciber hace necesaria la formación jurídica de los distintos operadores jurídicos acorde a ella. No todos los jueces son la Audiencia Nacional, órgano jurisdiccional altamente especializado.

Los problemas no sólo se derivan de la norma europea, pues si nos referimos a la transposición española, realizada a través de la Ley 3/2018, de 11 de junio, por la que se modifica la Ley 23/2014, de 20 de noviembre, de reconocimiento mutuo de resoluciones penales en la UE, para regular la orden europea de investigación. nos encontramos con otras dificultades distintas. En primer lugar, dicha Ley prevé un sistema de competencias que se distribuyen entre jueces y fiscales, tanto para la emisión

como para la ejecución de la orden, aunque ciertamente el sistema español confiere un especial protagonismo al fiscal en la parte de ejecución. Debe tenerse en cuenta que el Fiscal sólo podrá asumir dichas competencias cuando sea el que instruya y esto, en España, solo se produce en el procedimiento penal de menores, regulado por la Ley Orgánica 5/2000, de 12 de enero, reguladora de la responsabilidad penal de los menores.

En otro orden de cosas, se producen problemas en cuanto a la competencia para la ejecución de la orden. ¿Qué ocurre si la autoridad judicial se considera incompetente? Los tribunales españoles han adoptado ante estos problemas diversas soluciones[16].

Además, el régimen de confidencialidad de la orden europea de investigación también plantea interrogantes, pues el Ministerio Fiscal no puede decretar el secreto de las actuaciones. Como bien indica Laro González (2022), la fase de instrucción se caracteriza por el secreto de las actuaciones, en lugar de por el principio de publicidad. El Fiscal queda obligado a respetar dicho principio, aunque la norma no le permita decidir el secreto de las actuaciones[17].

A todo lo anterior, se añade el hecho de que los ordenamientos jurídicos de los distintos Estados miembros son demasiado rígidos o garantistas. No somos partidarios de prevenir, reprimir y castigar los delitos al margen de la Ley, evidentemente. Pero las instituciones y los países, incluso europeos, se atrincheran en el respeto a los derechos fundamentales, tales como la intimidad o el secreto de las comunicaciones, para impedir la investigación criminal. Recordemos que uno de los motivos que permite denegar la orden de protección de una prueba electrónica es justamente la vulneración de un derecho fundamental. De esta manera, a pesar de que, en Europa, todos los Estados están de acuerdo en el respeto y garantía de los derechos fundamentales

16. Ejemplos son Auto nº 1566/2019 del Juzgado Central de Instrucción nº 2, de 14 de junio y Auto nº 344/2019 de la Audiencia Nacional, de 1 de julio; Auto nº 668/2019 de la Audiencia Provincial de Gerona, de 10 de octubre y auto de la Audiencia Nacional nº 483/2021, de 22 de diciembre.
17. Cit., pág. 134. Véase también Aguilera Morales, 2019 y Rodríguez-Medel Nieto, 2014, p. 413.

inherentes a la dignidad del ser humano, el hecho de negarse a entregar una evidencia a una autoridad judicial que sustancia un proceso en un Estado distinto de aquéllos donde se albergan los datos, se convierte en una excusa que dificulta la represión y castigo de los ciberdelitos y para poner obstáculos a la hora de obtener la prueba electrónica.

El debate jurídico está servido: facilidad para obtener pruebas electrónicas o respeto máximo de los derechos fundamentales; en definitiva, lucha contra la delincuencia transfronteriza o garantías.

Creemos que la respuesta está en el principio de confianza mutua. Debemos entender que todos los Estados miembros afirman y respetan los derechos fundamentales y que ningún juez que solicite la prueba electrónica habida en otro Estado miembro quiere ni pretende que resulte conculcado ningún derecho. Todos los Estados de la UE, se sobreentiende, protegen y respetan derechos como el secreto de las comunicaciones y el derecho a la intimidad. Por ello, ningún proveedor de servicios de *Internet* debe negarse a entregar las evidencias electrónicas cuando se requiera por la autoridad judicial en el seno de un proceso penal, pues se debe creer y entender que todos los procesos judiciales seguidos en cualquier país con legislaciones similares son sustanciados según todas las garantías. Podemos decir: quien es un proveedor de servicios de *Internet* para negarse a entregar, por ejemplo, una prueba que obra en su poder a una autoridad judicial española cuando la requiera. ¿Acaso, en España, no se afirman en su Constitución los derechos fundamentales? ¿Acaso no se respetan los mismos por sus autoridades judiciales, igual que en el lugar donde se halla situado tal proveedor? Cuando una autoridad judicial lo exige lo hace a través de una resolución motivada y porque alguien está siendo investigado como sospechoso de haber cometido un delito. Da igual de que Estado hablemos, pues todos somos miembros de la UE y, en todos ellos, se respetan los mismos derechos. Aunque tenemos legislaciones diferentes, son similares, pues existen instrumentos de armonización (Reglamentos, Directivas y Decisiones). Esto permite confiar mutuamente los unos en los otros.

Por otra parte, en caso de resultar vulnerado algún derecho fundamental en un proceso, existe un sistema de recursos y medios extraordinarios. Incluso, como todos los Estados miembros de la UE forma parte del Consejo de Europa, se someten a las decisiones del Tribunal Europeo de Derechos Humanos. No hay, pues, excusa válida para entorpecer los procesos judiciales contra la delincuencia transfronteriza para impedir la obtención de las evidencias electrónicas.

7 Conclusiones y propuestas

Se han dado pasos de gigante, en la UE, pero aún hay mucho por hacer, pongamos sólo algunas propuestas sobre la mesa:

- Se pueden homogenizar aún más las legislaciones de los Estados miembros. Somos partidarios del instrumento legislativo Reglamento más que de la Directiva. Y ello se justifica de la siguiente manera: la libertad que se otorga a los Estados miembros a la hora de trasponer las Directivas de la UE provoca problemas añadidos a los de la misma norma europea, como hemos observado que ocurre en el caso español, en relación a la orden europea de investigación.

- Se deben mejorar los instrumentos legislativos de la UE, anteriormente descritos, perfeccionando aspectos entre otros el de la traducción. ¿Cómo no va a poderse facilitar la traducción, si hoy contamos con la IA que permite automatizar este proceso? Insistimos que la agilización en la tramitación de las órdenes de investigación, producción y conservación es fundamental dada la volatilidad de las evidencias digitales y su pronta desaparición

- Debe existir mayor cooperación policial y judicial. Refuércense las instituciones *Europol* y *Eurojust* o la Fiscalía Europea.

- Debe formarse a todos los operadores jurídicos (jueces, fiscales, abogados, procuradores) para que estén capacitados para utilizar las herramientas creadas por la UE. Pensemos que

una orden europea de investigación podría ser necesaria en un procedimiento penal por un abogado, que podemos denominar de «a pie» o por un juez de instrucción de un partido judicial cualquiera. Formemos no sólo a las Fuerzas y Cuerpos de Seguridad del Estado de las unidades especializadas, sino a cualquier agente. La ciberdelincuencia es tan habitual que cualquier abogado puede personarse en una causa como acusador particular o cualquier juez puede estar inmerso en su persecución.

- Sigamos ahondando en la fijación de criterios de jurisdicción que faciliten la sustanciación de los procedimientos lo más cerca posible del lugar de comisión del hecho delictivo o del lugar de localización del servidor en donde se encuentra la evidencia de la comisión del delito. De esta manera, se evitará tener que solicitar la entrega de pruebas cuando el servidor esté alojado en un Estado distinto.

- Hagamos uso de las figuras del decomiso y de los embargos preventivos. Si las organizaciones de ciberdelincuentes no cuentan con medios económicos tendrán más obstáculos para seguir delinquiendo.

- Proponemos que exista un Reglamento de la UE sobre ciberdelincuencia, a través del cual se regulen los medios de investigación y de prueba en los procesos judiciales abiertos contra la ciberdelincuencia organizada. Debido a que la vigilancia electrónica es una medida intrusiva y restrictiva de derechos fundamentales o la entrega vigilada o las operaciones encubiertas son medidas cuestionadas por la incitación al delito, su aplicación puede ocasionar reticencias en algunos Estados miembros. Inclúyase en dicho Reglamento la posibilidad de utilizar medios tales como *exploits* (códigos que permiten, gracias a la vulnerabilidad de los programas informáticos o defectos de seguridad, meter intrusos que tengan acceso a distancia a una red y adquieran privilegios elevados), o programas maliciosos. La investigación de la ciberdelincuencia organizada requiere medidas de investigación tecnológicas altamente especializadas y agresivas. Es lo que se denomina en EE. UU., «técnicas de investigación de redes» (Oficina de las Naciones Unidas Contra la Droga y el Delito, 2022).

Fuera de la UE, el panorama es considerablemente mucho más sombrío. Los instrumentos legislativos de la UE no existen fuera de este ámbito regional. Tampoco resulta tan eficaz la cooperación internacional. Los estándares de protección de los derechos fundamentales son diferentes; los ordenamientos jurídicos muy dispares; los procedimientos penales distintos; la formación de los operadores jurídicos diversa, los niveles de opacidad en la represión criminal obviamente también varían. La investigación se torna más compleja, al tener que solicitar la entrega de una prueba a través de comisiones rogatorias, lo que permite su rápida destrucción. Los decomisos ni los embargos son tan sencillos y la extradición también complica la situación. La asistencia judicial recíproca y la cooperación se torna imprescindible.

Comenzamos este artículo relacionando los términos de ciberseguridad y de ciberdelincuencia: relacionados entre sí, pero diferentes. Ante la complejidad de la lucha contra la ciberdelincuencia, enarbolamos la bandera de la prevención. Estamos seguros de que la ciberseguridad es el camino ideal y preventivo para evitar o, al menos minimizar, los ataques de los ciberdelincuentes.

En el caso de los ciudadanos, no cabe otra solución que la formación: unas cuantas reglas de conducta habituales (contraseñas variadas y seguras, vigilancia de los permisos que se otorgan a las *apps*, no abrir *whatsapp*, correos electrónicos, mensajes o no contestar llamadas sospechosas) son la mejor prevención.

En el caso de las empresas, la cuestión tiene que ver con la prevención y el análisis de riesgos: no sólo grandes empresas, sino también las medianas y pequeñas deben contar con un *chief information security officer* (CISO). Importante a este respecto resulta la Directiva NISS 2 (Directiva 2022/2555 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022 relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión, por la que se modifican el Reglamento (UE) nº 910/2014 y la Directiva (UE) 2018/1972 y por la que se deroga la Directiva (UE) 2016/1148[18]. Además, todas las

18. Esta Directiva se aplica a las empresas públicas y privadas, no sólo grandes, sino también medianas que presten sus servicios o lleven sus actividades en la UE y, por

empresas deberían tener unas *compliance guides*, idóneas y adecuadas en materia de ciberseguridad y de protección de datos, pues estos dos ámbitos forman parte inescindible del *compliance* de una empresa y es garantía de seguridad para todos[19].

En definitiva, la mejor forma de enfrentarse a la ciberdelincuencia organizada es transformar el deber y la sanción en una cultura *behaviour*. Se habla ya de *behavioral compliance*, esto es, de aquella forma de pensar que entiende la ética como punto fundamental en la transformación de la cultura corporativa.

¿Seremos capaces de lograrlo? El presente no es sencillo y el futuro una incógnita y es que la IA plantea nuevos y complejos retos para la ciberseguridad.

Referencias bibliográficas

Aguilera Morales, M. (2019). La implementación de la orden europea de investigación: el dolor de la lucidez. En I. González Pulido y F. Bueno de Mata (dirs.), *La cooperación procesal internacional en la sociedad del conocimiento* (pp. 209-224). Atelier.

Barrera Ibáñez, S. (2018). Perseguir el rastro digital en la red: once años sin medidas legislativas. *Revista del Consejo General Abogacía española, 11*.

CORVUS (2023, 24 de octubre). Q3 Ransomware Report: Global Ransomware Attacks Up Over 95% in 2022. *Corvus*. https://www.

tanto, afecta a empresas de más de 50 empleados o con un volumen de negocio mayor de 10 millones de euros, incluidas aquellas que puedan tener inversiones públicas. Pero también se aplica a empresa pequeñas y microempresas, que tengan que un papel fundamental para la sociedad, la economía o para determinados sectores o tipos de servicios.

19. Véase la Circular de la Fiscalía General del Estado 1/2016 y la Sentencia del Tribunal Supremo de 29 de febrero de 2016, en relación al código de cumplimiento normativo que deben tener las personas jurídicas para quedar exoneradas de responsabilidad penal, conforme al art. 31 *bis* del CP.

corvusinsurance.com/blog/q3-ransomware-report (Consultado el 24/04/2024. Hora: 13:00).

De Hoyos Santo, M. (2023). Novedades en materia de obtención transfronteriza de información electrónica necesaria para la investigación y enjuiciamiento penal en el ámbito europeo. *Revista de Estudios Europeos, número Extraordinario monográfico 1*, 99-128.

Delgado Martín, J. (2016). *Investigación tecnológica y prueba digital en todas las jurisdicciones*. Wolters Kluwer. Extracto en «La valoración de la prueba digital», http://diariolaley.laley.es/home/DT0000245603/20170411/La-valoracion-de-la-prueba-digital (Consultado 1/04/2024. Hora: 12:00).

Laro González, E. (2022). Luces y sombras de la Orden Europea de investigación. *Revista de Estudios europeos, Número Extraordinario monográfico 1*, 129-144.

Martil, I. (2017). Cómo función las redes inalámbricas de telefonía móvil. *Público.* https://blogs.publico.es/ignacio-martil/2017/02/24/como-funcionan-las-redes-inalambricas-de-telefonia-movil/?doing_wp_cron=1541448078.7565820217132568359375 (Consultado 1/04/2024. Hora: 12:00).

Menéndez Rodríguez, C. (2014). Los delitos de pertenencia a organización criminal y grupo criminal y el delito de tráfico de drogas cometido por persona que pertenece a una organización delictiva. Crónica de un conflicto normativo anunciado y análisis jurisprudencial. *Estudios Penales y Criminológicos, 34*, 511-560.

Messuti, A. (2013). *Un deber ineludible. La obligación de los Estados de perseguir penalmente los crímenes internacionales*. Buenos Aires: Ediar.

Oficina de las Naciones Unidas Contra la Droga y el Delito. (2022). *Compendio de ciberdelincuencia organizada.* Viena.

Picón Rodríguez, E. (2017). *¿Por qué no es válida una conversación de Whastapp en juicio?* https://elderecho.com/por-que-no-es-valida-una-conversacion-de-whatsapp-en-juicio. (Consultado 1/04/2024. Hora: 12:00)

Rayón Ballesteros, M. C. y Gómez Hernández, J. A. (204). Cibercrimen: particularidades en su investigación y enjuiciamiento. *Anuario Jurídico y Económico Escurialense, 47,* 209-234. http://www.rcumariacristina.net:8080/ojs/index.php/AJEE/article/view/189/158

Rodríguez-Medel Nieto, C. (2014). *Prueba penal transfronteriza: su obtención y admisibilidad en España* (Tesis doctoral).

Romero Casabona, C. M. (2016). Delitos cometidos con la utilización de tarjetas de crédito, en especial en cajeros automáticos. *Nuevo Foro Penal, 12*(52), 147-169.

Volpato, S. (2016). *El derecho a la intimidad y las nuevas tecnologías de la información*. http://hdl.handle.net/11441/52298 (Consultado 1/04/2024. Hora: 12:00).

Zúñiga Rodríguez, L. (2016). El concepto de criminalidad organizada transnacional: problemas y propuestas. *Nuevo Foro Penal, 86*, 62-114. https://doi.org/10.17230/nfp.12.86.2