Revista de Pensamiento Estratégico y Seguridad CISDE

Recibido: 02-07-2019 / Revisado: 21-09-2019
Aceptado: 21-09-2019 / Publicado: 30-11-2019

CISDE Journal, 4(2), 2019

Dificultades jurídicas ante las conductas delictivas contra y a través de medios informáticos y electrónicos

Legal difficulties between criminal conduct against and through of computer and electronic tools

Emilio L. Tejero[1]

[1] Universidad de Sevilla, España

elteyal@gmail.com

RESUMEN. El desarrollo de las TIC y la generalización de su uso han determinado que cada vez sean más numerosos los ataques criminales a bienes jurídicos que deben ser objeto de protección. En 2018 se ha dado un máximo histórico de crecimiento progresivo y proliferación de constantes ataques, nuevas amenazas y vulnerabilidades detectados, tanto a equipos convencionales, como a dispositivos móviles en aplicaciones fraudulentas, dada la expansión y uso constante y variado de estos terminales y de las aplicaciones y nada hace prever que esta tendencia se reduzca en los años venideros, sino todo lo contrario.

ABSTRACT. The development of the ICT and the generalization of its utility, have determined that there are more and more criminal attacks on legal goods and rights, object of protection. There has been a historic peak of progressive growth and proliferation of constant attacks, new hazards and vulnerabilities detected in 2018, for electronics devices (conventional equipment, mobile devices and celular smartphones) for fraudulent applications, if you observe the expansion and constant and varied use of these terminals and the applications. Nothing makes to feel that this trend is reduced at the next years, rather the opposite.

PALABRAS CLAVE: Amenazas y vulnerabilidades, TIC, Criminalidad informática y delitos cibernéticos, Delitos informáticos y electrónicos, Procesamiento jurídico.

KEYWORDS: Hazards and vulnerabilities, ICT, Computer crime and cybercrime, Computer and electronic delinquency, Legal prosecution.

Tejero, E. L. (2019). Dificultades jurídicas ante las conductas delictivas contra y a través de medios informáticos y electrónicos. *Revista de Pensamiento Estratégico y Seguridad CISDE*, 4(2), 39-54.

1. Introducción

Las violaciones de seguridad en la red, que se van sucediendo, causan tanto perjuicios económicos, como bloqueo al desarrollo electrónico. Pero no son sólo los ataques lo único que preocupa, sino que ha puesto de manifiesto la vulnerabilidad de los sistemas de información y de las redes de comunicación. Un fallo en las mismas pone en peligro el suministro de numerosos servicios, algunos de ellos vitales, alcanzado, en 2018, un máximo histórico de vulnerabilidades reportadas. Acciones ilícitas que, entre otros problemas analizados, van desde correos electrónicos fraudulentos a intentos de estafa a través de videojuegos o extorsión,

A pesar de existir técnicas de infección mucho más elaboradas, el correo electrónico se presenta como la herramienta de ataque preferida de los delincuentes (CCN-CERT, 2019). La facilidad de generar campañas masivas de envíos y el razonable "éxito" que siguen teniendo son motivos más que suficientes para comprender el uso del correo electrónico como medio de propagar amenazas y como puerta de entrada a los sistemas operativos de las víctimas mediante variantes de troyanos combinados, para ser aún más efectivos[1].

El año 2018 ha sido en el que más vulnerabilidades se han logrado detectar y reportar, 16.216 vulnerabilidades (que no significa que sean todas), lo que supone un incremento del 9% respecto al año anterior (aunque algunas previsiones lo elevaban al 13%), de las cuales 745 fueron de criticidad máxima, un 4´60% del total[2], que no es una cuestión menor (no debe confundirse la cantidad de vulnerabilidades con la gravedad de la criticidad de esas vulnerabilidades[3]).

Una de las amenazas más destacadas de este pasado año, además de las bancarias, han sido los correos electrónicos de extorsión, que coaccionan con difundir entre los contactos de las víctimas supuestos vídeos y/o fotografías comprometidos, existan o no. Desde mediados del 2018 se han descubierto varias campañas de esta modalidad, (aunque algunas sin contener ningún tipo de malware)[4]. El malware busca, generalmente dañar o alterar el comportamiento de los sistemas infectados (como p. ej. el malware dedicado recopilar datos o a mostrar publicidad molesta en todo momento). El comportamiento básico del malware había sido, hasta ahora,

[1] Así, tres de los riesgos de seguridad más importantes, en diciembre de 2018, utilizaron la última variante descubierta del troyano bancario Danabot, combinándose con el conocido troyano GootKit como aliado. Estos troyanos utilizan los sistemas que infectan para reenviar correos electrónicos maliciosos a otros usuarios, por lo que su propagación se incrementa conforme aumenta el número de víctimas, teniendo especial impacto en países de la U.E. en los últimos meses.

Otro troyano bancario, que se ha propagado últimamente mediante correo electrónico, ha sido Emotet. Se han detectado varias campañas que suplantan diferentes servicios online (entre los que destacan servicios bancarios, postales oficiales e incluso Amazon), donde se adjuntan datos personales de la víctima —como nombre, apellidos, etc.—. Los delincuentes intentan con este sistema que las víctimas abran un archivo adjunto que descarga y ejecuta el malware propiamente dicho.

[2] (INCIBE-CERT, 2018); empleando el estándar de nomenclatura CVE (Common Vulnerabilities and Exposures), recogiendo, entre otros, la información del NVD (National Vulnerability Database) del NIST (National Institute of Standards and Technology), U.S.

[3] Los productos con mayor número de vulnerabilidades en 2018 fueron: Debian (889), Android (549), Ubuntu (451), Enterprise Linux Server de Red Hat (en quinto lugar) y Windows 10 (en décimo).

Las aplicaciones con más vulnerabilidades fueron: Firefox (333), Acrobat DC y Acrobat Reader DC (285) y PhantomPDF (223).

Las empresas de las que se han reportado más, han sido: Debian (890), Google (712), Oracle (690) y Microsoft (673).

En cuanto a los tipos de CVE que más se reportaron fueron: la ejecución de código no deseado (23%, de las que el 79% fueron graves: criticidad mayor o igual a 7), los ataques por desbordamiento (overflow) (18%) y los ataques de XXS (15%) y de DoS (11%).

Por su parte, los menos reportados fueron la elevación de privilegios (2,5%), la inserción de archivos (0,2%) y la división de respuesta HTTP (0,1%).

Respecto a la gravedad de los tipos de CVE reportadas, menos del 10% fue superior a nivel 8 y poco más del 41% inferior al nivel 5.

Los fabricantes con el promedio histórico de criticidad de vulnerabilidades más alto son: Adobe (8,80), Qualcomm (8,50) y RealNetworks (8,50); y aquellos con el histórico de mayor cantidad de vulnerabilidades son: Debian (823), Oracle (690) y Microsoft (664). [CVE Details].

[4] Los correos electrónicos de este tipo incluyen un enlace a un pretendido vídeo de la víctima, que contiene un ransomware que cifra los archivos del sistema operativo, pidiendo un rescate, sin ninguna garantía de que, una vez efectuado el pago, puedan recuperarse.

CC BY NC

"atacar" al sistema y al usuario de dicho equipo[5]. El incremento de la expansión y desarrollo de la difusión de los videojuegos son también una modalidad que ha atraído a los delincuentes[6].

La detección de proliferación de constantes nuevas amenazas, tanto a equipos convencionales, como a dispositivos móviles en aplicaciones fraudulentas[7], se han disparado, dada la expansión y uso constante y variado de estos terminales y de las aplicaciones[8] (Figura 1).

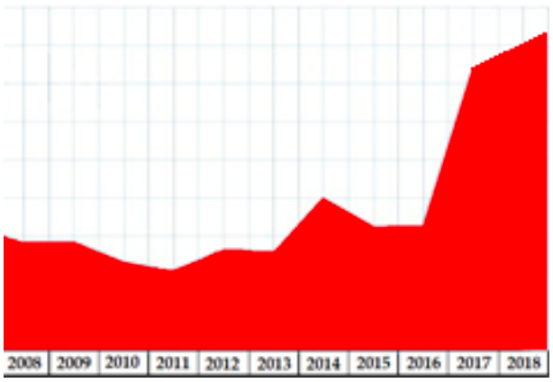

Figura 1. Incremento de Vulnerabilidades detectadas en los últimos 10 años Hasta diciembre 2018. Fuente: (INCIBE-CERT, 2018).

El inconveniente radica en que nada hace prever que esta tendencia se reduzca en los años venideros, sino todo lo contrario, y que muchas vulnerabilidades puedan quedar sin resolver o no se apliquen los parches correspondientes[9]. La detección de vulnerabilidades seguirá acrecentándose año tras año, porque, según "argumenta" el sector, «son inevitables e inherentes al software como producto per se», en un intento de "lavarse las manos" de las posibles responsabilidades.

[5] Sin embargo, el creciente interés y auge de las criptomonedas, por el aumento de su valor, ha generado nuevas tendencias de delincuencia, como fuente de ingresos ilegítimos, como el criptojacking, diseñando y diseminando un malware que aproveche los fallos de vulnerabilidades, conocidas —o desconocidas—, de los sistemas operativos (convirtiéndose en una forma muy extendida de "minería" ilícita), con un enfoque absolutamente distinto del uso del malware, como herramienta para violentar la seguridad y poder obtener ganancias, consistente en un ataque e infección de los sistemas operativos y usar su poder computacional, creando una red de nodos que pueda controlar, generando altas capacidades de procesamiento, no siendo necesario, ya, destruir o dañar al objetivo del ataque, sino pasar desapercibido, permaneciendo oculto su funcionamiento de bajo perfil en segundo plano y con poco impacto, manteniendo a la víctima activa, que proporciona ganancias con la "minería". Es la víctima, sin darse cuenta de que ha sido infectado, quién hace, para el atacante, de "mina de la criptomoneda", sin ningún permiso, con la finalidad de generar ganancias al actor malicioso.

[6] Fortnite: Battle Royale, videojuego del año, ha sido un fenómeno de masas que ha reunido a millones de jugadores en todo el mundo, lo que ha sido aprovechado por los delincuentes, conocedores del alcance de este videojuego, con intentos de estafas, extorsiones e instalación de malware entre los seguidores. El retraso de varios meses, para dispositivos Android, del lanzamiento de Fortnite, con respecto a la versión para iOS, provocó que Google Play se llenase de aplicaciones falsas. Cuando la desarrolladora decidió no distribuir el juego en la plataforma de Google, aparecieron aún más versiones.

Además del robo de cuentas o fraudes, para supuestamente conseguir potenciadores o cantidades de moneda usada en el juego (u otras estafas de este tipo o modalidad elaboradas por los delincuentes), y más peligroso son los casos de acosadores que aprovechan la popularidad del juego para entrar camuflados en los grupos de jugadores ofreciendo códigos o métodos para subir de nivel que, tras ganar la confianza de forma sencilla de las víctimas, solicitan envío de imágenes privadas que posteriormente utilizan para extorsionar a los jugadores menos precavidos (en muchos casos a menores).

[7] Mediante troyanos camuflados en herramientas (como p. ej. optimizar el rendimiento de batería, aplicaciones de fitness, aplicaciones de juegos para dispositivos móviles, etc.).

[8] Refugiándose en conocidas plataformas como Google Play Store, para Android, o App Store de Apple, para iOS, y utilizando plataformas de pago legítimas como PayPal, para el envío de dinero a cuentas de los atacantes, de forma que algunos usuarios realizan pagos sin darse cuenta, al utilizar estas herramientas. A lo que se suman las indetectables fugas de datos personales que, pretendidamente, no ocasionan perjuicio económico directo y que son usados ilegítimamente incluso por compañías legalmente establecidas.

[9] Se han creado herramientas de descifrado para algunas familias de ransomware (como HiddenTear, ransomware de código abierto con variantes desarrolladas desde su aparición), para que todos los afectados puedan recuperar los archivos sin tener que pagar la extorsión a los delincuentes.

Sin embargo y por contra, a pesar de haber pasado más de un año desde la detección de la vulnerabilidad del fallo identificado en el protocolo SMBv1 (Server Message Block) de Windows, aprovechado por WannaCry y el ataque de este ransomware, las detecciones del exploit SMB/Exploit.DoublePulsar, han experimentado un incremento de afectados del 213% en 2018.

El impacto de todas estas vulnerabilidades es notable para estados, entes gubernamentales, administraciones, grandes corporaciones, empresas de sectores estratégicos, bancos, industria, …, todos ellos con grandes recursos; pero … ¿qué ocurre con los usuarios particulares, con el ciudadano "de a pie"?

2. Delitos informáticos más comunes [10]

Eso, que se ha dado en denominar, ciber delincuencia y ciber delito no es más que aquella actividad delictiva que se realiza a través de un sistema informático o que utiliza como medio las redes informáticas, ya sean públicas o privadas, y que «tenga como objetivo atentar contra la confidencialidad, la integridad y la disponibilidad de los sistemas informáticos, las redes o los datos, así como el uso fraudulento de tales sistemas, redes y datos»[11].

Siendo muchas las conductas delictivas que se instrumentan a través de medios informáticos y electrónicos (entre los que podrían encontrarse incluidos delitos como la suplantación de identidad, el acoso o la estafa)[12], los delitos cibernéticos o criminalidad informática (como ha sido denominado oficialmente por la fiscalía en España[13]), por tanto, no dejan de ser una tipología más del delito y así serán denominados en este trabajo[14].

Las amenazas asociadas a la criminalidad informática más común, sobre las que habría que poner especial precaución serían:

Delito tipo 1. Estafa telemática e informática. (Podría considerarse el delito informático más extendido).

La estafa se encuentra definida en el art. 248 del Código Penal, Título XIII, que trata sobre los delitos contra el orden socio económico y contra el patrimonio, formando parte del Capítulo VI "De las defraudaciones".

Se entiende por estafa aquella acción con ánimo de lucro por la que un sujeto utiliza un engaño para tratar y conseguir que otro cometa un error que le induzca a cometer un acto de disposición en perjuicio propio o ajeno. En esta definición hay una serie de elementos indispensables, que deben tenerse en cuenta, para que se produzca la comisión del delito: el engaño —expreso o tácito— (fundamental, sin el cual no hay delito), que exista ánimo de lucro, el acto de disposición patrimonial, el error, y el perjuicio. En cualquier proceso judicial por esta causa, es habitual añadir, además, el nexo causal y los otros factores y exigencias propios de la

[10] Entre la tipología de las figuras delictivas más habituales encontraríamos las relacionados con falsedades documentales, revelación de secretos, publicidad engañosa, vulneración de derechos de autor, daños informáticos, estafas electrónicas, delitos contra la intimidad y la libertad de expresión, vulneraciones de protección de datos y correos electrónicos, etc. También hay conductas que, si bien no se encuentran tipificadas en el Código Penal, suponen, éticamente, un mal uso de las redes, como son los casos de los usos comerciales abusivos (como el spam), las prácticas parasitarias de competencia desleal, las que interrumpen las comunicaciones, los comentarios obscenos de amplia expansión en las comunicaciones, tanto públicos como privados, etc.

[11] Sección 1ª (Derecho penal sustantivo) del Capítulo II del Instrumento de Ratificación del Convenio sobre la Ciberdelincuencia, Consejo de Europa, Budapest, 23 de noviembre de 2001, BOE núm. 226, de 17 de septiembre de 2010 (50 págs.); corrección de errores: BOE núm. 249, de 14 de octubre de 2010; consentimiento de España: Instrumento de Ratificación de 11 de noviembre de 2014, BOE núm. 26, de 30 de enero de 2015 (11 págs.) (BOE 249, 14 de octubre de 2010).

[12] Clasificación en la Sección 1ª del Capítulo II (Derecho penal sustantivo) del Convenio sobre la Ciberdelincuencia: Título I. Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos (acceso ilícito, interceptación ilícita, interferencia en los datos, interferencia en el sistema, abuso de los dispositivos); Título II. Delitos informáticos (falsificación informática, fraude informático); Título III. Delitos relacionados con el contenido; Título IV. Delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines.

[13] Creación del Fiscal de Sala de Criminalidad Informática; Fiscal General del Estado; Real Decreto 255/2019, de 12 de abril, por el que se amplía la plantilla orgánica del Ministerio Fiscal para adecuarla a las necesidades existentes; BOE núm. 89, de 13 de abril de 2019, (19 págs.).

[14] Estos tipos de criminalidad informática pueden darse tanto de rango mundial, como local. A modo de ejemplos de cada uno de ellos, podrían citarse la destacada paralización de cientos de empresas por el ataque del WannaCry (cit. supra), que se autoinstalaba en los ordenadores de trabajadores de distintas compañías produciendo la encriptación de los archivos almacenados en los ordenadores conectados en la misma red; así como el caso de los estudiantes, alumnos de instituto, que instalaron un software que monitorizaba las pulsaciones del teclado en los ordenadores del centro, permitiendo descifrar las contraseñas de autenticación de las distintas cuentas, accediendo, así, a los correos electrónicos de los profesores, obteniendo los exámenes que tenían que realizar.

CC BY NC

imputación[15].

En esta tipología de delito se enmarca también:

— la falsa venta o alquiler fraudulento de bienes
— las del tipo "estafa nigeriana", donde el autor remite un correo electrónico a la víctima prometiendo una gran cantidad de dinero a cambio de un ingreso de una determinada cantidad por adelantado, variante de la conocidísima modalidad de los clásicos "tocomocho" o "timo de la estampita".
— el phising: obtención fraudulenta de contraseñas bancarias con el fin de transferir dinero a otras cuentas. En estos casos la jurisprudencia ha admitido la responsabilidad del proveedor del servicio de pago (el banco), salvo que se aprecie fraude o negligencia grave en la víctima.
— el carding: que consiste en un copiado de las tarjetas de crédito de la víctima para realizar posteriormente adquisición de bienes con ellas.

Delito tipo 2. Delitos informáticos de daños.

Entrarían en este tipo delictivo los casos de virus informáticos destructivos, consistente en borrar, dañar, deteriorar, hacer inaccesibles, alterar o suprimir datos informáticos sin autorización y con un resultado gravoso para el perjudicado. También la destrucción de datos o equipos que pudieran contener pruebas de otros delitos. Lo relevante en este tipo de delito es que no exigen una cuantía mínima para que se entienda cometido.

Delito tipo 3. Defraudación en las telecomunicaciones.

Y uso no consentido de terminales de telecomunicación (arts. 255 y 256 del C.P.)[16]. Este tipo delictivo requiere que se cause un perjuicio económico a la víctima, sea otro usuario, sea el suministrador del servicio.

Delito tipo 4. Delitos contra la intimidad, la propiedad industrial e intelectual.

Son abundantes los casos en que se instala un software en determinados dispositivos para acceder así a información personal o corporativa (espionaje industrial) sin autorización de su propietario. Podrían ser acusado en estos casos, también, de un delito de descubrimiento y revelación de secretos.

Delito tipo 5. Delitos de amenaza, coacción y extorsión.

En concurrencia, combinación o en conjunción con los anteriores (p. ej. con el delito informático de daños o con los delitos contra la intimidad)[17], se dan las figuras delictivas de amenazas, coacción y extorsión, todas ellas o alguna de ellas.[18]

Como prevención básica a futuros ataques de conductas delictivas de este tipo, las recomendaciones, en las que coinciden los especialistas, pasan por estar alerta, dentro de lo posible, y tomar algunas medidas, como:

— Realizar actualizaciones periódicas de los sistemas operativos.
— Contar con un buen antivirus.

15 Algunas de las últimas modificaciones del Código Penal se centraron en recoger los "delitos informáticos", aquellos que se llevan a cabo haciendo uso de las herramientas tecnológicas informáticas, añadiendo puntos a determinados artículos como el 248, que parece era innecesario (cuestión distinta es si se hubiera convertido en agravante, lo que no se hizo) pues para la calificación de la comisión, cuya finalidad es el engaño, da igual "el medio" utilizado, ya que, en sí mismo, no varía la naturaleza del delito (sigue siendo estafa sea presencial, por correo postal, telefónico o informático).

16 Sección 3ª del Capítulo VI, Título XIII, Libro II° del Código Penal, "De las defraudaciones de fluido eléctrico y análogas".

17 En muchos de los delitos contra la intimidad, concurren también los delitos de amenazas, coacción y extorsión; o como en el conocido caso del Wanna Cry (cit. supra), junto al delito informático de daños.

18 Delito de amenazas, arts. 169 a 171; Capítulo II, Título VI Delitos contra la libertad, Libro II° del Código Penal. El contenido esencial de este delito es el anuncio de hechos o expresiones que revelan la intención de causar un mal futuro, determinado y posible, cuya realización dependa del amenazante, originando intimidación con la intención de ejercer fuerza sobre la víctima, el amenazado, causándole temor o privándole de tranquilidad o libertad. Delito de coacciones, art. 172; Capítulo III, Título VI, Libro II°. El elemento característico de la coacción es la violencia, que puede ser tanto física como psíquica o moral. Delito de extorsión, art. 243
Capítulo III, Título XIII, Libro II°; lo que caracteriza este tipo delictivo es el ánimo de lucro.

— Mantener las funciones de wifi, bluetooth y geolocalización de smartphones, tablets o equipos portátiles desactivadas mientras no se usan.
— Mantener las cámaras de los equipos tapadas mientras no se usan.
— No conectar los dispositivos a wifi pública.
— Hacer frecuentes y periódicas copias de seguridad del material más sensible o importante.
— Trasladar los archivos más sensibles o importantes a un disco duro externo.

Sin embargo, no es de recibo, ni justificable, trasladar la carga de la "culpa" al usuario particular, achacándole "la escasa conciencia de los usuarios de la necesidad de mantener unas mínimas medidas preventivas de seguridad" ya que los ataques se dan tanto a ciudadanos particulares, como a importantes corporaciones (con gran cantidad de medios y recursos) y hasta a administraciones gubernamentales (con ilimitada cantidad de medios y recursos).

3. Dificultad en la persecución de los delitos

Que estas conductas delictivas no son algo nuevo en sí mismas y que la particularidad estriba sobre el medio en que actúan y dónde y cómo se cometen, ha sido ya expuesto arriba. Es decir, radica en la ejecución delictiva, que hace, de los medios informáticos y electrónicos, más que un lugar o espacio, una posición circunstancial, una esfera de actividad que genera un nuevo ámbito de posible exposición para perpetrar variados ataques a determinados bienes jurídicos protegidos, lo que les confiere una especial configuración que debía haber obligado a la adopción de medidas ad hoc para su investigación y enjuiciamiento hace ya tiempo[19]. El desarrollo de la red y de las tecnologías asociadas —referidas a los datos, la información y las comunicaciones— han ido parejas de una inexcusable falta de prevención y dejación[20].

Se ha pretendido diferenciar, en un intento de elucubración teórica, entre "ciberdelito", "cibercrimen", "delito informático" (oficialmente como criminalidad informática), etc.[21], lo que no dejan de ser denominaciones de modalidades de los medios utilizados, que no afectan a la naturaleza misma del delito. Así se identifican como delitos informáticos aquellos en los que el nexo común, alrededor del cual se producen, es un equipo informático (p. ej. ordenador) o un dispositivo electrónico con conexión a red, bien porque el objeto sobre el que recae la conducta es el propio sistema, el equipo o el programa informático, bien porque el sistema es utilizado como medio por el cual se realiza la conducta delictiva, o bien porque el bien jurídico protegido sea la integridad de la información, la confidencialidad de la misma o los datos y los sistemas o programas informáticos.

El Derecho Penal (Queralt Jiménez, 2008), y muy especialmente el Derecho Procesal Penal, no han parecido adaptarse al ritmo marcado por el reto del desarrollo de este nuevo tipo de ejecución delictiva, para enfrentarse a ella adecuadamente. Fundamentalmente por eso es necesario considerar indagar sobre las particularidades en la investigación y enjuiciamiento de este tipo de ejecución delictiva, desde el punto de vista procesal.

Uno de los "mantras" repetidos es que, para hacer frente a esta forma de delincuencia es necesario un enfoque "supranacional", término cuya utilización parece poco acertada en estos casos, pues su significado real es el de «entidades que estén por encima del ámbito de los gobiernos e instituciones nacionales y que actúen con independencia de ellos», lo que implicaría, por un lado, una cesión de soberanía innecesaria y por otro un

[19] Los poderes públicos no pueden excusarse en que la evolución que se ha dado haya sido una "sorpresa que nadie esperaba", aún al contrario, desde los inicios del desarrollo informático y de la red eran conocidas y previsibles las posibles amenazas a los bienes jurídicos.

[20] (González Rus, 1999); Protección penal de sistemas, elementos, datos, documentos y programas informáticos; en Revista Electrónica de Ciencia Penal y Criminología, nº. 1, Universidad de Granada, 1999; págs. 1 a 14. Versión revisada de ponencia presentada en las Jornadas sobre delincuencia informática, Centro de Estudios Jurídicos de la Administración de Justicia, del 2 al 4 de junio de 1997 (el texto provisional fue publicado en Estudios Jurídicos. Ministerio Fiscal. III., Madrid, 1997).

[21] Vid. ROMEO CASABONA, Carlos; De los delitos informáticos al cibercrimen. Una aproximación conceptual y político-criminal; en El cibercrimen. Nuevos retos jurídico-penales, nuevas respuestas político-criminales. AA.VV. (2006); Editorial Comares; Granada, 2006, págs. 1 a 42.

perjuicio para el particular, al que le sería imposible acudir a ella por la propia configuración del Derecho Internacional Público, cuando lo que parece que quiere expresarse es la evidente necesidad de que existan procedimientos rápidos, efectivos y dotados de medios técnicos adecuados de cooperación para la investigación —policial y judicial— de carácter internacional[22]. La "política penal común", con la dificultad que supone adaptar y armonizar legislaciones en todos los países y el mantenimiento de una política de cooperación internacional, en caso de darse algún día, está todavía muy lejana, máxime si se tiene en cuenta que se habría de contar con el beneplácito de los estados de las principales potencias informáticas[23].

Pero aún y así, mientras se desvía la atención sobre la necesidad de grandes soluciones internacionales, es injustificable que no se dé solución a los casos de ámbito estrictamente nacional que se encuentren exactamente con la ineficacia del mismo problema de estricta territorialidad de la competencia jurisdiccional. Si la mayoría de ciudadanos tuvieran el más mínimo conocimiento del funcionamiento interno cotidiano del sistema judicial se darían cuenta de sus patentes deficiencias[24].

La L.O. 15/2010, de 22 de junio de 2010, una de las muchas modificaciones a la L.O. 10/1995 (Ley Orgánica 10/1995), de 23 de noviembre, del Código Penal, introdujo algunos cambios[25], pudiéndose hablar, en la actualidad, de estos tipos de delitos en esta materia, siempre y cuando se utilice un mecanismo para la realización del mismo, se alteren maliciosamente las indicaciones o se empleen medios clandestinos. Aunque para algunos supuestos, que no se encuentran específicamente tipificados en el Código Penal, habría que acudir a legislación complementaria administrativa[26] que regula eso que se ha dado en llamar la "sociedad de la información"[27].

Ciertamente la regulación legal y las correspondientes sanciones punitivas se dan como reacción a nuevas

[22] En este sentido el Convenio sobre Ciberdelincuencia del Consejo de Europa, Budapest, 23 de noviembre de 2001, ha supuesto más una cuestión formal (refiere tipologías de delitos: de acceso ilegal, interceptación ilegal, violación de la integridad de datos y sistemas, violación de dispositivos, falsificación informática, fraude informático, pornografía infantil, violaciones del derecho de autor, más el Protocolo Adicional de 2003 al incluir actos de racismo y xenofobia), que una respuesta efectiva a la necesidad de cooperación eficaz para la lucha contra estos tipos delictivos, sin tener en cuenta que desde la propuesta pasan más de diez años hasta su publicidad y quince para su ratificación por España. Es más que evidente que, en esta materia, lo planteado en 2001 y 2003, está más que desfasado en 2015.

[23] Como p. ej. EE.UU. (donde se alojan gran cantidad de empresas de servicios no obligados a respetar legislaciones locales), Rusia, China, India o Israel.

[24] Pongamos el ejemplo de un individuo en Irún que, con nombre falso, en un portal de segunda mano, pone en venta un bien inexistente por cantidad que sea considerada menor (de 200 o 300€) y sus víctimas, entre muchos, sean de San Fernando (Cádiz), Dos Hermanas (Sevilla) o Alcantarilla (Murcia). En contra de lo que el común de ciudadanos cree, no se da orden a la policía para que investigue en Irún (eso sólo sucede en casos que sean considerados de determinada relevancia), sino que cada una de las victimas tiene que interponer denuncia individual (que son consideradas como de menor gravedad), y que entrarían en cada uno de los juzgados de instrucción, abriéndose procedimiento (sin conocimiento unos de otros), en el que se debe tomar declaración al investigado, que al presuponerse está en Irún, ha de enviarse exhorto por correo certificado al decanato correspondiente para que lo reparta a un juzgado de Irún que cite a su vez, por correo, al investigado para que declare en él. Si éste no se presenta o no es localizado, se devuelve el exhorto indicando que no ha podido cumplimentarse el trámite … y vuelta a empezar.

[25] La citada reforma del Código Penal introduce en este ámbito: las estafas, las amenazas, los delitos contra la intimidad, los delitos contra el honor, los delitos de exhibicionismo y provocación sexual, los delitos relativos a la prostitución y corrupción de menores (incluidos en el Capítulo II bis, De los abusos y agresiones sexuales a menores de dieciséis años, Título VIII, Libro IIº, debido al creciente empleo de la red para estos abusos), las defraudaciones de fluido eléctrico y de las telecomunicaciones, los daños, los delitos relativos a la propiedad intelectual, los delitos relativos a la propiedad industrial, los delitos relativos al mercado y a los consumidores, incorporando, así, los delitos informáticos como conducta tipificada y clasificando las conductas punibles en dos grupos, respecto al descubrimiento y revelación de secretos y las relativas a los daños.

[26] Ley de Servicios para la Sociedad de la Información y de comercio electrónico, la Ley de impulso a la Sociedad de la Información, Ley General de Telecomunicaciones, la L.O. de Protección de Datos, la Ley sobre conservación de datos de comunicaciones electrónicas, Ley de Propiedad Intelectual, Ley de Firma Electrónica, etc., dónde, a pesar de que se encuentren mejor tipificadas algunas infracciones (en materia de protección de datos personales, de envío de correos electrónicos o en cuestiones de la sociedad de la información, etc.), no dejan de ser más que faltas administrativas a juicio del órgano competente, en las que al perjudicado final, en la mayoría de los casos, no se le da traslado de notificación, ni tiene conocimiento del hecho.

[27] Hay que llamar la atención sobre el hecho de que se ha divulgado, como verdad inmanente, que la "sociedad de la información" «se caracteriza por la ausencia de fronteras y la inmaterialidad de la comunicación, con lo que los límites temporales y espaciales no existen», lo que no es del todo cierto, sino que, en virtud de la ideología de la globalización, se ha querido crear lo que podríamos denominar "paraísos T.I.C.", —al modo de los "paraísos fiscales"—, en los que, en realidad, se utilizan "empresas instrumentales" para evadir las responsabilidades y legislaciones locales, pues todo aparataje T.I.C., necesariamente cuenta de operadores y servidores con base física.

conductas y actividades que los poderes públicos competentes, en determinado momento, entienden como delictivas y reprobables. Sin embargo, la cada vez más variada y abundante casuística delictiva vinculada a esta materia (como queda constatado arriba por los informes), hace que cualquier regulación, que pretenda ser excesivamente específica, quede pronto superada por las formas de perpetración de los delitos, que se van transmutando y adaptando a nuevas posibilidades.

Pero en estas cuestiones no es tanto la insuficiencia de la propia regulación que, como se ha visto, es aplicable independientemente del medio material utilizado, como de los obsoletos, lentos e ineficaces procedimientos de investigación y enjuiciamiento (por los trámites establecidos en practicar las pruebas para identificar el rastro de las conductas delictivas), para la efectiva persecución de las mismas, lo que, en estos casos, dificulta muchísimo la detección y persecución de las conductas dañosas de este tipo de delitos, dada la rapidez del desarrollo tecnológico, el carácter transnacional de estas conductas delictivas por la facilidad de intercambio de comunicación inmediata entre lugares físicamente alejados, la dificultad para identificar las huellas digitales por la fugacidad de las acciones y la facilidad de alteración de los rastros de la comisión de hechos que facilitan el anonimato. Todos estos factores facilitan la impunidad de estas conductas[28].

La persecución de estos delitos, en los que intervienen las T.I.C., encuentran el obstáculo de presentar toda esta serie de particularidades especiales citadas, tropezando, entre otras, con las cuestiones tocantes a la dificultad probatoria, a lo que habría de sumarse los espinosos problemas en la colaboración procesal, por lo que trataremos de prestar especial atención a la forma de realizar las necesarias averiguaciones en la concreción de la prueba con relación a la certeza del hecho punible y la responsabilidad de su autor ante los tribunales. En este sentido, y a efectos procesales, habría que señalar que la conducta delictiva, pudiendo tener su origen en uno (o varios) países y el acto delictivo concretarse en otro, u otros, incluso podría resultar difícil determinar dónde se ha cometido o por parte de quién. Indudablemente esto afecta, a la competencia jurisdiccional, a la ley aplicable y al procedimiento que se tramitará para su investigación y enjuiciamiento, ya que la regla general refiere al principio de territorialidad, lex loci delicti commissi o ley del lugar de comisión del delito que, en España, viene determinada por la L.O.P.J.[29].

—En los delitos en que la acción y la consecuencia se producen dentro de un mismo estado resulta aplicable la ley de ese estado[30], cualesquiera que sea la nacionalidad del autor. Aún en estos casos la complejidad es considerable, pues para determinar el juzgado competente hay que establecer el criterio aplicable: el domicilio del querellado, el lugar en el que se ejecutó el delito, el de ubicación del servidor, aquel en el que se averiguaron las pruebas materiales, el lugar en que se iniciaron las actuaciones procesales, el lugar en el que se produjeron los daños, etc. En estos casos suele resolverse la competencia respecto del lugar en que se consumó la acción[31].

—Se plantean serios problemas, cuando la actividad se perpetra en otro estado, pero tiene sus consecuencias en España, ya que la gran mayoría de países rechazan el enjuiciamiento de su nacional por tribunales de otro estado, no autorizando la extradición.

— En los delitos perpetrados telemáticamente, a distancia (frecuentes por la red, pero que también puede entenderse cometidos por teléfono o por correo postal clásico), surgen mayores problemas, cuando la acción

[28] Sin embargo, ha quedado demostrado, en más de una ocasión, que ataques a importantes entidades gubernamentales o grandes corporaciones y servicios son investigados y perseguidos hasta dar con los autores, por muy complejo que sea.

[29] Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial.

[30] Principio de territorialidad. Las leyes penales españolas se aplican a hechos sucedidos en el territorio español (arts. 8.1 CC y 23.1 LOPJ).

[31] Vid. nota 25 supra.

y el resultado se producen en diferentes estados. Doctrina y jurisprudencia se decantan por apreciar la teoría de la ubicuidad[32] que tiene en cuenta, como lugar de comisión del delito, tanto el lugar en el que se ha producido la acción como el del resultado del perjuicio dañoso.

—En los casos en que la acción se produce en un estado y el resultado en otro, los datos en tránsito (datos de la comunicación que atraviesa los países), se consideran irrelevantes, así como también se considera irrelevante el lugar en que radique el prestador de servicios o el proveedor de acceso a la red, no aplicándose el principio de territorialidad en estos casos, exigiéndose un punto de conexión en el país en el que se ha producido el resultado, existiendo la posibilidad de aplicar el principio de oportunidad[33], que implica que el delito no sea juzgado en otro país.

— En alguna ocasión, la conducta delictiva puede haberse llevado a cabo en / o desde un país con una incompleta o muy permisiva legislación respecto de las conductas perniciosas cometidas a través de las T.I.C.[34], que no poseen medios de detección y persecución o no han ratificado tratados de extradición, lo cual dificulta mucho más aún el proceso de investigación y enjuiciamiento.

Pero todo esto, al fin y al cabo, no dejan de ser más que cuestiones de complejidad técnica que, por otro lado, se dan también en otro tipo de delitos internacionales que pueden presentar similares características (p. ej. el tráfico internacional de obras de arte robadas, el de blanqueo de capitales, secuestro internacional de menores, etc.), o incluso en casos jurídicos no penales que entran en el ámbito del Derecho Internacional Privado.

4. Procedimiento de Investigación

La fase de investigación criminal es común a todos los delitos y presupone el conjunto de actuaciones encaminadas a la comprobación y averiguación para esclarecer el hecho delictivo y, en su caso, aportar pruebas para su valoración, calificación, determinación de responsabilidades y autores, abriéndose las diligencias previas de la instrucción judicial[35] y preparatorias del juicio.

Las diligencias de averiguación judicial, suelen iniciarse o de oficio por la policía judicial[36] (o cuerpo asimilado), que haya llevado a cabo una investigación previa; por una denuncia realizada por los afectados de la conducta delictiva ante la policía (o cuerpo asimilado); o por denuncia directamente ante juzgado de guardia.

[32] En este caso podrían aplicarse:

la teoría de la actividad (lugar en el que se realiza la conducta);

teoría del resultado (lugar de producción del resultado);

teoría de la ubicuidad (conducta y resultado, ambos indistintamente. Seguida de forma mayoritaria, para evitar la impunidad de ciertos supuestos como p. ej. el caso de paquete bomba remitido desde un país a otro, si en el primero rige la teoría del resultado y en el segundo la de la actividad).

[33] Principio de oportunidad: Instrumento de conciliación en Derecho Procesal Penal que permite, en determinados delitos, se llegue a un acuerdo sobre la reparación civil, a efectos de que el fiscal se abstenga del ejercicio de la acción penal y el Juez dicte auto de sobreseimiento.

[34] Vid. nota 28 supra.

[35] L.E.Cr., Título IV De la instrucción Capítulo I Del sumario y de las autoridades competentes para instruirlo.

art. 299. Constituyen el sumario las actuaciones encaminadas a preparar el juicio y practicadas para averiguar y hacer constar la perpetración de los delitos con todas las circunstancias que puedan influir en su calificación y la culpabilidad de los delincuentes, asegurando sus personas y las responsabilidades pecuniarias de los mismos.

[36] Ley de Enjuiciamiento Criminal, Título III, De la Policía judicial.

art. 282. La Policía Judicial tiene por objeto y será obligación de todos los que la componen, averiguar los delitos públicos que se cometieren en su territorio o demarcación; practicar, según sus atribuciones, las diligencias necesarias para comprobarlos y descubrir a los delincuentes, y recoger todos los efectos, instrumentos o pruebas del delito de cuya desaparición hubiere peligro, poniéndolos a disposición de la autoridad judicial. Cuando las víctimas entren en contacto con la Policía Judicial, cumplirá con los deberes de información que prevé la legislación vigente. Asimismo, llevarán a cabo una valoración de las circunstancias particulares de las víctimas para determinar provisionalmente qué medidas de protección deben ser adoptadas para garantizarles una protección adecuada, sin perjuicio de la decisión final que corresponderá adoptar al Juez o Tribunal.

Si el delito fuera de los que sólo pueden perseguirse a instancia de parte legítima, tendrán la misma obligación expresada en el párrafo anterior, si se les requiere al efecto. La ausencia de denuncia no impedirá la práctica de las primeras diligencias de prevención y aseguramiento de los delitos relativos a la propiedad intelectual e industrial.

Seguidamente el tribunal iniciará el procedimiento que determine corresponda.

En algunos casos, pueden librarse mandamientos judiciales dirigidos a los proveedores de acceso a las redes para que informen sobre los datos que posean para identificar a los usuarios de las direcciones IP, las líneas desde las que se efectúan las conexiones, así como sus titulares[37], si bien las propias compañías nacionales son bastante reticentes a facilitar información —no digamos las extranjeras, que en muchos casos ni los atienden, amen que el procedimiento de Cooperación Jurídica Internacional[38], mediante el Auxilio Judicial Internacional Penal[39] es harto complicado— y para cumplir estos mandamientos suelen ser extremadamente exigentes en cuanto a la especificidad y concreción de lo solicitado (muchas veces en base a datos de geolocalización facilitados por el sistema SITEL[40]), pudiéndose llegar a autorizar diligencias de entrada y registro en domicilios o sedes del titular de la línea, levantando acta, el Letrado de la Administración de Justicia (antiguos secretarios judiciales), accediéndose con estas diligencias de investigación a ordenadores, discos duros y archivos. Si bien, estas son acciones que se adoptan solamente y únicamente en la investigación de delitos que tengan la consideración de especialmente "grave", es decir, generalmente inasequible.

Parece comprensible que, en el ámbito de las T.I.C., para dar las respuestas y soluciones que la sociedad demanda contra la delincuencia informática, se hace necesario que policía judicial y cuerpos de seguridad del estado dominen conocimientos y herramientas, mediante la especialización de agentes, para detectar y hacer seguimientos de las conductas delictivas e identificar a sus autores.

Asimismo, se hace necesario también, que se tenga que recurrir a expertos y peritos que dirijan el modo de llevar a cabo determinadas investigaciones que destacan por su carácter extraterritorial, que obstaculiza las actuaciones de las autoridades policiales y judiciales, incrementándose, por tanto, tiempo y costes, ya que, por otro lado, los infractores suelen conocer muy bien el medio que emplean para la comisión de los delitos (convirtiéndose ellos mismos en auténticos especialistas, intentando borrar las huellas y rastros en la red, tratando de conseguir el completo anonimato que les de impunidad).

Debido al incremento exponencial de perpetración de estos delitos tecnológicos, tímidamente, se han creado unidades especiales de investigación en la Policía Judicial, tanto en la Guardia Civil (el GDT - Grupo de Delitos Telemáticos, dentro de la Unidad Central Operativa - UCO, con equipos de Investigación Tecnológica - EDITE,s en cada una de las provincias de España); como en el Cuerpo Nacional de Policía (la UIT - Unidad de Investigación Tecnológica con dos brigadas, la Brigada Central de Investigación Tecnológica - B.C.I.T. y la Brigada Central de Seguridad Informática) y en algunas Policías Autonómicas. En 2011 el Fiscal General del estado crea una fiscalía especializada en delitos informáticos[41].

Sin embargo, la otra cara de la moneda es que estas unidades cuentan con medios materiales y especialmente humanos extremadamente reducidos, lo que finalmente se traduce en que su actuación se

[37] Los proveedores de servicios pueden prestar una información determinante a una investigación, ya que, fundamentalmente, los técnicos policiales, necesitan los datos de tráfico y los rastros de navegación que aportan información primordial sobre el origen de la comunicación y sus itinerarios a través de la red, que se almacenan y conservan en los sistemas y aplicaciones informáticas. Aunque no se localizan fácilmente, generalmente, a partir de estos datos reservados obtenidos con la investigación se puede llegar a ubicar el lugar de comisión de los hechos, el equipo de origen y a identificar al abonado, que no tiene porqué ser el autor material.

[38] La Cooperación Jurídica Internacional se ejerce en España sobre la base de Tratados o Acuerdos Internacionales, ya sean de carácter bilateral o multilateral, o, a falta de dichos tratados, a través del principio de reciprocidad. El Ministerio de Justicia, actúa como Autoridad Central para la recepción y remisión de las solicitudes de Asistencia Judicial Internacional en materia penal.

[39] Acuerdo de 27 de septiembre de 2018, del Pleno del Consejo General del Poder Judicial, por el que se aprueba el Reglamento 1/2018, sobre auxilio judicial internacional y redes de cooperación judicial internacional; BOE núm. 249, de 15 de octubre de 2018, (14 págs.) (BOE 249, 15 de octubre de 2018).

[40] SITEL es un sistema de interceptación de las comunicaciones y escuchas telefónicas del Ministerio de Interior de España utilizado por la Policía Judicial (CNP, Guardia Civil y Servicio de Vigilancia Aduanera) que comparte los equipos electrónicos con el Centro Nacional de Inteligencia. También es conocido como Sistema Integrado de Interceptación de Telecomunicaciones, Sistema Integrado de Interceptación Legal de Telecomunicaciones y Sistema Integral de Interceptación de las Comunicaciones Electrónicas.

[41] Instrucción 2/2011, de 11 octubre, dictada por el Fiscal General del Estado, sobre el Fiscal de Sala de Criminalidad Informática y las secciones de Criminalidad Informática de las Fiscalía.

restringe únicamente a casos de "especial relevancia". Pero peor aún es la actuación de la fiscalía en multitud de casos, en que ni siquiera ejerce la acusación al considerarlos de "escasa importancia"[42], obligando con ello, prácticamente, al sobreseimiento de la causa e incluso a que se archive sin que se abra procedimiento[43].

5. La cuestión de los medios de prueba en el procedimiento

Todo proceso judicial requiere que se demuestre lo pretendido y para ello, en los ordenamientos jurídicos, se admiten una serie de medios de prueba. La finalidad de la prueba es convencer al juzgador de la certeza de los hechos que fundamentan las pretensiones de parte[44].

Existen tres fases en el procedimiento probatorio: la proposición de los medios de prueba, la resolución del tribunal sobre la admisión o desestimación motivada y la práctica de la prueba admitida.

Ley de Enjuiciamiento Civil[45] enumera como medios de prueba de las que se podrá hacer uso en juicio:

« 1.º Interrogatorio de las partes.
2.º Documentos públicos.
3.º Documentos privados.
4.º Dictamen de peritos.
5.º Reconocimiento judicial.
6.º Interrogatorio de testigos.

2. También se admitirán, conforme a lo dispuesto en esta Ley, los medios de reproducción de la palabra, el sonido y la imagen, así como los instrumentos que permiten archivar y conocer o reproducir palabras, datos, cifras y operaciones matemáticas llevadas a cabo con fines contables o de otra clase, relevantes para el proceso.

3. Cuando por cualquier otro medio no expresamente previsto en los apartados anteriores de este artículo pudiera obtenerse certeza sobre hechos relevantes, el tribunal, a instancia de parte, lo admitirá como prueba, adoptando las medidas que en cada caso resulten necesarias».

«Ni el Código Penal ni la Ley de Enjuiciamiento Criminal contienen una enumeración similar para el campo penal, que, en principio, está abierto a un más amplio abanico de posibilidades probatorias». No obstante, «Los

[42] La instrucción, negando la evidencia, dictamina «[…] no debe llevarnos sin más a considerar que cualquier conducta delictiva en cuya ejecución se haga uso de las tecnologías de la información y la comunicación ha de incluirse en la categoría que nos ocupa […]», reduciendo el "catálogo de delitos a los que se extiende el marco del área de criminalidad informática", a tres categorías:

«2.A) Delitos en los que el objeto de la actividad delictiva son los propios sistemas informáticos o las TICs.

2.B) Delitos en los que la actividad criminal se sirve para su ejecución de las ventajas que ofrecen las TICs.

2.C) Delitos en los que la actividad criminal, además de servirse para su ejecución de las ventajas que ofrecen las TICs, entraña especial complejidad en su investigación que demanda conocimientos específicos en la materia».

[43] Cuando todos los índices de criminalidad informática se disparan, resulta que los casos en esta materia en los que interviene la fiscalía, descienden nada más y nada menos que casi un 17%, según el último informe de la Fiscalía General del Estado (datos de 2017) Memoria Elevada al Gobierno de S. M. Presentada al Inicio del Año Judicial por la Fiscalía General del Estado, Madrid, 2018; 8 (Segarra Crespo, 2018). Criminalidad Informática […] 8.2 Análisis de las diligencias de investigación y procedimientos judiciales incoados y acusaciones formuladas por el Ministerio Fiscal en 2017.

« […] hemos constatado que, en el año 2017, se incoaron en el conjunto del Estado un total de 6.676 procedimientos judiciales por ese tipo de delitos. Dicho dato da cuenta de un descenso en un 16,91 %, concretado en 1.359 registros, respecto de la cifra obtenida por este concepto en el año 2016, en el que dimos por incoados 8.035 procedimientos, y –lo que es más llamativo– en un 70,42 % respecto de los 22.575, iniciados en el año 2015» (pág. 732).

[44] El procedimiento probatorio será el conjunto de normas que regulen la actividad probatoria y también el conjunto de actividades dirigidas a convencer al tribunal de la certeza de determinados hechos y actos, que deberá contar con todas las garantías legales (art. 24 de la CE), por tanto, ha de permitir a las partes proponer con total y absoluta libertad los medios de prueba pertinentes que estimen oportunos. La ejecución de la prueba debe estar tutelada por los principios de contradicción, de "igualdad de armas" y de publicidad de las actuaciones judiciales (con las excepciones que prevean las leyes de procedimiento art. 120 de la CE).

[45] L.E.Cv., Libro II, Título I, Capítulo VI, De los medios de prueba y las presunciones, art. 299. (Ley de Enjuiciamiento Civil, 1/2000).

medios de prueba previstos en la Ley de Enjuiciamiento Criminal, en todo caso, son los siguientes: a) Declaración del acusado; b) Prueba testifical; e) Careo; d) Prueba pericial; e) Prueba documental; f) Inspección ocular. Por lo demás, debe citarse también como prueba válida en el campo penal la denominada "Prueba por indicios"(v. s° T.C. 107/1989, de 8 de junio)» (Puerta Luis, 1995).

Para acreditar la autoría concreta de hechos por un infractor, en los delitos a través de las T.I.C., serian especialmente aplicables:

- la pericial, mediante la determinación de pruebas electrónicas
- la documental
- la testifical
- la confesión y
- la prueba indiciaria o indirecta

Se puede definir la prueba electrónica[46] como cualquier información obtenida a partir de dispositivos electrónicos, o medio digital, que sirva para adquirir convencimiento de la certeza del hecho. La prueba electrónica pericial consistirá en la realización de los análisis de dispositivos o sistemas, que examinen su contenido para llegar a acreditar que los hechos delictivos han sido perpetrados. La incertidumbre característica de la prueba electrónica hace necesario que se mantengan protocolos de actuación seguros que garanticen su inalterabilidad y no manipulación, fortuita o intencionada, por los implicados en la comisión de un delito, para ocultar su autoría. Para realizar este análisis no existen herramientas establecidas judicialmente, sino que cada cuerpo policial de seguridad del estado utiliza las suyas propias, generándose, así, inseguridad jurídica tanto para los investigadores, como para los propios investigados, ya que, en el proceso penal, el peritaje informático de este tipo de prueba va a ser determinante.

Debido a la falta de regulación en numerosas de estas cuestiones, la materia es imprecisa, con contradicciones y lagunas, generando disparidad de criterios, de manera de que, a pesar de su importancia en este tipo de causas, la prueba electrónica sigue siendo un instrumento bastante obviado en el ámbito judicial, por lo que no es fácil precisar el concepto de perito informático. Siguiendo la regla general, podemos considerar como tal a la persona designada por el tribunal en base a sus conocimientos que, sin ser parte en el proceso, emite informe técnico sobre la determinación de hechos con carácter procesal.

Hay que advertir que las pruebas, en este tipo de delitos, suelen ser realizadas por organismos oficiales dependientes de las policías judiciales y cuerpos de seguridad al servicio de la fiscalía y que, paradójicamente, gozan de "presunción de neutralidad e imparcialidad", siempre y cuando se confeccionen por ingenieros o informáticos distintos de los que hacen las intervenciones materiales de la investigación[47]. En cuanto al informe pericial, realizado por la policía judicial, debe contener como mínimo, para poder constituir prueba en fase de juicio, la descripción de los elementos sometidos a análisis, las operaciones realizadas y fundamentación motivada obtenida de las operaciones realizadas. En el caso de tener que ratificarse este informe en sede judicial, el perito deberá utilizar un lenguaje claro y conciso.

[46] La prueba electrónica se convierte en elemento fundamental de cualquier procedimiento en el que se hayan empleado medios electrónicos para la comisión del delito. Deberá reconstruirse la cadena de acontecimientos (tanto lícitos, como ilícitos) que hubieran producido un resultado dañino, lo que suele comportar cierta complejidad técnica.

[47] La Asociación de Técnicos de Informática (la más importante de este tipo en nuestro país) establece un gran margen de cualificación de peritos en este ámbito. Sin embargo, en recientes normativas publicadas se entiende por técnicos informáticos únicamente al Ingeniero Informático e Ingeniero Técnico Informático (lo que ha causado diversos recursos por aquellos cuya Universidad emitía titulación de Licenciado Informático o Diplomado en Informática y aquellas titulaciones oficiales de Grado Superior en Informática). Aunque, en teoría, cualquier especialista con conocimientos técnicos informáticos podría comparecer en el proceso para aportar su experiencia, existe una queja de los peritos judiciales habilitados y con titulación en esta materia que, a diferencia de otras, no son denominados por los juzgados, que únicamente se basan en informes policiales, paradójicamente, la gran mayoría, efectuados por personal, que a pesar de su experiencia, carecen de titulación académica y que además puede entenderse forman parte, al servicio de la parte acusatoria de la ficalía, no imparcial en el proceso, comprometiendo una característica fundamental del perito. Vid. L.E.Cr. Libro II, Título V, Capítulo VII, Del informe pericial, arts. 456 a 485.

A pesar de que para que el informe pericial sea considerado como prueba de cargo, a efectos de destruir el principio de presunción de inocencia, se deben seguir todas las formalidades del procedimiento dictado por los arts. 723 a 725 de la L.E.Cr., siendo necesario que se practique en la fase de juicio oral, donde se realizará ratificación del informe por su autor, en dicho acto, a efectos de valor probatorio y sea tenido en cuenta en el procedimiento[48], se ha buscado "la forma" de otorgar a estos informes policiales, efectuados por órganos oficiales, eficacia probatoria sin necesidad de la obligada comparecencia judicial mediante los siguientes artificios:

1.- Sólo puede prescindirse de la ratificación cuando los informes sean emitidos por gabinetes u organismos de policía con ámbito estatal[49].

2.- Esos informes constituyen prueba documental, por lo que deben recibir el tratamiento contenido en el art. 726 de la LECrim.

3.- Doctrina de la "aceptación tácita", según la cual, los informes periciales pueden desvirtuar la presunción de inocencia sin necesidad de la obligada comparecencia, cuando las partes acepten tácitamente el contenido de los citados informes, no contradiciéndolos en el juicio.

Los dos primeros pueden considerarse desechados en la actualidad, adquiriendo, hoy, mayor relevancia y vigencia la "doctrina de la aceptación tácita"[50]. Por contra, la STS de 29 de marzo de 2010, señala que «la pericial es una prueba de carácter personal donde el principio de inmediación personal particularmente cuando esta prueba se practica en el juicio oral, tiene una relevancia que no aparece en la documental» y STS de 5 de mayo de 2010 «Se trata de prueba personal documentada de contenido técnico científico llamada a facilitar la labor del tribunal en el momento de valorar la prueba, y opera como una suerte de auxiliar del juez que suple su falta o insuficiencia de conocimientos especializados para tener, de ese modo, un adecuado conocimiento de los hechos sometidos a su enjuiciamiento».

Respecto de la prueba pericial, podemos deducir, que la jurisprudencia, ha redefinido los criterios en el sentido de:

—A las pruebas periciales, aportadas a las diligencias previas, practicadas con anterioridad al juicio oral (incluso en fase de investigación, antes de iniciado el proceso) se les da consideración de "pruebas preconstituidas", confiriéndoseles validez, si no son impugnadas por alguna de las partes.

—Los informes periciales, emitidos por órganos oficiales, practicados en trámite de instrucción, deben entenderse como de "aceptación tácita" por las partes, si ninguna propone expresamente impugnación o prueba contradictoria sobre el particular, lo que posibilita que la diligencia de que se trate produzca efectos de prueba de cargo, siendo asimilada a prueba documental.

—Las pruebas periciales, o alguno de sus elementos, practicados en el sumario, deben ser sometidos a contradicción cuando alguna de las partes lo solicite en momento procesal oportuno. De no ser así, el tribunal podrá determinar tenerlas en consideración para formar su convicción sin la necesaria ratificación de los peritos, cuando no sea requerido, o no se cuestione el resultado, la neutralidad o la competencia de los autores, renunciándose a solicitar las aclaraciones que fueren pertinentes.

[48] STC 22/1988, de 18 de febrero, tomando la doctrina jurisprudencial dominante en las sentencias del T.C. establece que no se puede tomar en consideración ni valorar como prueba los dictámenes periciales que no sean ratificados o practicados, como tales pruebas, en el juicio oral, pues sólo de esa manera se pueden salvar los principios constitucionales de inmediación y contradicción.

[49] Las primeras sentencias del T.S. para "saltarse" las sentencias del TC, son inmediatas, de 21 de abril de 1988, 25 de septiembre de 1988 y 12 de julio de 1989.

[50] La STS 24/1991, de 11 de febrero, sostiene que «cuando se trata de informes periciales o cuasi periciales sobre circunstancias de hecho fundamentales en la causa penal concreta que se tramite, practicados durante el sumario o diligencias previas, máxime cuando son realizados por organismos oficiales o por funcionarios públicos especializados al respecto, y ninguna de las partes propone prueba sobre ese extremo, lo que motiva que en el acto del juicio oral nada se practique sobre tal particular, ha de entenderse que hay una aceptación tácita por todas las partes sobre la mencionada pericial y ello permite que el juzgado o tribunal en la instancia pueda considerar como probado el hecho al que se refieren esas diligencias realizadas durante la fase de instrucción».

En algunos casos de delincuencia informática hay que acudir a lo que la doctrina denomina "prueba indiciaria o indirecta", que vincula mediante indicios al investigado con el hecho delictivo para realizar la incriminación concreta. Con la "prueba indiciaria" es necesario que el órgano judicial precise exactamente cuáles son los indicios tomados en consideración y cómo se ha deducido de ellos la implicación del investigado, de tal modo que cualquier otra instancia judicial, con posterioridad, pueda comprender y constatar la argumentación formulada, siendo necesario que se expliquen minuciosamente todos los elementos de prueba conducentes a las conclusiones y el razonamiento lógico que ha llevado a la convicción de que la prueba de cargo ha sido capaz de contrarrestar la presunción de inocencia.

Según la jurisprudencia se requerirán una pluralidad de indicios acreditados y conexos entre sí, que mantengan un vínculo preciso y directo entre el indicio y el acto criminal, conforme a las reglas de la lógica y el conocimiento del hecho delictivo, argumentado en la STS 4667/2017, Sentencia de la Sala de lo Penal 844/2017, de 21 de diciembre de 2017[51].

6. Conclusiones

El desarrollo de la tecnología de la información y la generalización de su uso han determinado que cada vez sean más numerosos los ataques criminales a bienes jurídicos que deben ser objeto de protección. En todo estado, el sistema judicial es el poder público encargado de impartir Justicia en una sociedad, cuya finalidad eficiente es la protección de los bienes jurídicos, resolviendo los conflictos, mediante la aplicación de normas y principios jurídicos por órganos jurisdiccionales a los que se les presupone ecuanimidad, autonomía e imparcialidad.

Se da el dato objetivo del incremento, en números absolutos, de las actividades delictivas en materia de criminalidad informática que, por un lado, sacan partido de los medios que ofrecen las T.I.C., y por otro explotan las vulnerabilidades de los medios informáticos y electrónicos, pero que, sobre todo y principalmente, se benefician de la indolencia de los poderes públicos, poniendo de manifiesto las incapacidades del sistema judicial y una ausencia total de autocrítica[52].

La alegación de dificultad o complejidad de un problema, no puede disculpar la ineficacia e ineficiencia en la resolución de ese mismo problema. Se podría inferir que las dificultades en la investigación y enjuiciamiento, en materia de criminalidad informática, son efecto ad extra de una causa ad intra.

En muchas ocasiones se trata de disculpar, justificar, o incluso de disimular, dicho incremento, invocando una serie de tópicos, que no se corresponden con la evidencia, y que son repetidos hasta la saciedad:

— "La tecnología facilita la perpetración de nuevas conductas dañosas y la ocultación de los rastros de las mismas" o "Los continuos avances de las T.I.C. dificultan, cada día más, la investigación y el enjuiciamiento de estos delitos". Si se hace una analogía con cualquier otro tipo de delito clásico podremos comprobar lo absurdo y falaz de estos dos juicios. Sería como afirmar que los vehículos (tecnología) facilitan la huida de los ladrones (porque les perseguimos a caballo) o que Los avances de las T.I.C. dificultan la investigación, cuando en

[51] Vid. STC 146/2014, de 22 de septiembre; STC 133/2014, de 22 de julio; STC 126/2011, de 18 de julio; STC 109/2009, de 11 de mayo; STC 111/2008, de 22 de septiembre; STC 300/2005, de 21 de noviembre; STC 229/2003, de 18 de diciembre; STC 124/2001, de 4 de junio; STC 220/1998, de 16 de noviembre; STC 169/1989, de 16 de octubre y STC 174/1985, de 17 de diciembre.

[52] Vid. notas 40, 41 y 42, supra. Dice la Instrucción 2/2011, de 11 octubre, del Fiscal General del Estado, op. cit.:

«No obstante, esta circunstancia no debe llevarnos sin más a considerar que cualquier conducta delictiva en cuya ejecución se haga uso de las tecnologías de la información y la comunicación ha de incluirse en la categoría que nos ocupa, pues ello daría lugar a una desnaturalización del concepto, tal y como viene siendo considerado internacionalmente, e incluso a un desbordamiento del propio planteamiento de la especialización en este ámbito. Exigencias mínimas de operatividad y eficacia demandan, por tanto, una mayor concreción en la delimitación del objeto de actividad en esta área de trabajo de tal forma que únicamente alcance su competencia, cuando, en los indicados supuestos, la utilización de dichas tecnologías resulte ser determinante en el desarrollo de la actividad delictiva y/o dicha circunstancia implique una elevada complejidad en la dinámica comisiva y, en consecuencia, una mayor dificultad en la investigación del hecho e identificación de sus responsables». En román paladino, esta instrucción viene a decir que, en esta categoría, hay que reducir las calificaciones sólo aquellos casos que sean más graves, más "mediáticos" o más importantes, para no "desbordar el sistema".

realidad lo que "dificulta las investigaciónes" es la reducida cantidad de personal dedicado a esta materia y los medios con los que se cuenta[53].

—Otro de esos mitos es que "la actividad criminal más importante se desarrolla en un lugar virtual indeterminado, llamado ciberespacio, con unas coordenadas temporales y espaciales difíciles de delimitar", lo cual es absolutamente inexacto. Todo "espacio virtual" necesita de aparataje técnico físico, enclavado en algún lugar y al que se le tiene que suministrar energía, sin lo cual no puede tener existencia, exactamente igual que ocurría con una comunicación radiofónica, telefónica o telegráfica, con o sin hilo. Cuestión diferente es su localización.

—Otra de las frases más repetidas es que "la realidad siempre va por delante de la regulación legal y la correspondiente sanción punitiva de las conductas reprobables y en definitiva existen grandes dificultades del legislador y de la judicatura para conocer y comprender el mundo digital". La naturaleza delictiva no ha variado en sí mismas —como ya se ha argumentado sobradamente arriba—, robo, estafa, sabotaje, coacción, extorsión, etc., cuestión distinta es que se tenga la voluntad para modificar el anquilosado y formalmente encorsetado sistema burocrático judicial, incapaz de dar respuesta. Es cierto, que hace algunos años, el mundo digital era absolutamente desconocido para la gran mayoría de jueces y fiscales, pero hoy en día, aunque sólo sea como cualquier otro ciudadano medio usuario, no se puede negar que tengan algún conocimiento, aunque sí sería deseable una cierta formación en esta materia porque la sociedad se enfrenta a una criminalidad que demanda una mayor complejidad técnica.

Al objeto de una mayor eficacia en la lucha contra este tipo de delitos, debería establecerse una significativa agilidad y disposición de fiscales y tribunales encargados de instruir este tipo de causas, tratando de adecuarse a la realidad social. Al igual que debería procurarse una dotación de personal y recursos suficientes para la investigación de este tipo de conductas, con la correspondiente cualificación técnica profesional y de medios materiales a la altura de los utilizados por los autores de conductas delictivas y se debería abrir el ámbito (al igual que los forenses son médicos y no cuerpos de seguridad, la ciencia forense informática no puede estar únicamente monopolizada por escasas unidades policiales).

Una cuestión relevante es que, dada la estructura no jerarquizada, descentralizada y la extraterritorialidad de la red (características incompatibles con un sistema de control institucional) y que este tipo de acciones delictivas, frecuentemente, utilizan servidores interpuestos en distintos y diversos territorios nacionales, en algunos casos, las conductas delictivas alcanzan, al mismo tiempo, numerosos objetivos en todo el mundo, de forma inadvertida, masiva y con efectos altamente lesivos, por lo que se hace indispensable una política de arduo trabajo diplomático multilateral de acuerdos y tratados internacionales para dar solución a los problemas de jurisdicción y operatividad, con la agilización de trámites y colaboración internacional, tratando de limitar, especialmente, lo que hemos denominado arriba "paraísos informáticos" refugio.

Por otro lado, existe en el ciudadano medio una sensación generalizada de que, ante ataques a importantes entidades gubernamentales, servicios o grandes corporaciones industriales o financieras, se ponen en marcha inmediatamente y con recursos materiales, medidas de neutralización e investigación que se saldan con la localización de los autores y que, sin embargo, en cuestiones más domésticas y aparentemente más sencillas, que le afectan mayoritariamente y directamente, se escatiman medios y se llevan (cuando se llevan), investigaciones altamente deficientes.

A modo de epílogo final, podemos concluir que la criminalidad informática que se despliega en la sociedad de las T.I.C., según todas las previsiones, continuará desarrollándose, al margen de las fronteras convencionales, con gran impunidad, mientras no exista una voluntad real de los poderes públicos, tanto nacionales como internacionales, de ponerle cota. El problema estriba en cuantos acabaran afectados hasta que esa voluntad se mueva y si cuando se mueva se estará a tiempo.

[53] Supongamos que, ante una gran cantidad de hurtos menores, como no pueden perseguirse todos, se da instrucción de perseguir sólo y únicamente los robos mayores y más importantes, destinando, una unidad centralizada, para toda España, de 8 o 10 personas (dotación para la unidad central de delitos informáticos de la G.C.), que, comparados con la dotación destinada a la seguridad de cargos públicos, resulta ridículo.

Cómo citar este artículo / How to cite this paper

Tejero, E. L. (2019). Dificultades jurídicas ante las conductas delictivas contra y a través de medios informáticos y electrónicos. *Revista de Pensamiento Estratégico y Seguridad CISDE*, 4(2), 39-54. (www.cisdejournal.com)

Referencias

AA.VV. (2006). El cibercrimen. Nuevos retos jurídico-penales, nuevas respuestas político-criminales. Granada: Editorial Comares.

BOE 249 (15 de octubre de 2018). Acuerdo de 27 de septiembre de 2018, del Pleno del Consejo General del Poder Judicial, por el que se aprueba el Reglamento 1/2018, sobre auxilio judicial internacional y redes de cooperación judicial internacional; BOE núm. 249, de 15 de octubre de 2018, (14 págs.).

BOE 249 (14 de octubre de 2010). Consejo de Europa; Instrumento de Ratificación del Convenio sobre la Ciberdelincuencia, Budapest, 23 de noviembre de 2001, BOE núm. 226, de 17 de septiembre de 2010 (50 págs.); corrección de errores: BOE núm. 249, de 14 de octubre de 2010; consentimiento de España: Instrumento de Ratificación de 11 de noviembre de 2014, BOE núm. 26, de 30 de enero de 2015 (11 págs.) y Protocolo Adicional de 2003.

CCN-CERT (2019). Informe de Amenazas y Tendencias. resumen ejecutivo; Edición 2019.

González Rus, J. J. (1999). Protección penal de sistemas, elementos, datos, documentos y programas informáticos. Revista Electrónica de Ciencia Penal y Criminología, (1), 1-14.

INCIBE-CERT (2018). CVE Details, 2018.

Instrucción 2/2011, de 11 octubre, sobre el Fiscal de Sala de Criminalidad Informática y las secciones de Criminalidad Informática de las Fiscalías. Fiscal General del Estado. Recuperado de https://www.fiscal.es/fiscal/PA_WebApp_SGNTJ_NFIS/descarga/memoria2012_vol1_instru_02.pdf?idFile=6311c525-d23a-45d7-9e50-458f6f8c3406

Ley 2/2019, de 1 de marzo, por la que se modifica el texto refundido de la Ley de Propiedad Intelectual, aprobado por el Real Decreto Legislativo 1/1996, de 12 de abril, y por el que se incorporan al ordenamiento jurídico español la Directiva 2014/26/UE del Parlamento Europeo y del Consejo, de 26 de febrero de 2014, y la Directiva (UE) 2017/1564 del Parlamento Europeo y del Consejo, de 13 de septiembre de 2017; BOE núm. 53, de 2 de marzo de 2019, (59 págs.).

Ley 5/1998, de 6 de marzo, de incorporación al Derecho español de la Directiva 96/9/CE, del Parlamento Europeo y del Consejo, de 11 de marzo de 1996, sobre la protección jurídica de las bases de datos; BOE núm. 57, de 7 de marzo de 1998, (6 págs.).

Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones; BOE núm. 251, de 19 de octubre de 2007 y modificaciones posteriores.

Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico; BOE núm. 166, de 12 de julio de 2002 y modificaciones posteriores.

Ley 59/2003, de 19 de diciembre, de firma electrónica; BOE núm. 304, de 20 de diciembre de 2003 y modificaciones posteriores.

Ley 56/2007, de 28 de diciembre, de Medidas de Impulso de la Sociedad de la Información; BOE núm. 312, de 29 de diciembre de 2007 y modificaciones posteriores.

Ley 9/2014, de 9 de mayo, General de Telecomunicaciones; BOE núm. 114, de 10 de mayo de 2014 y modificaciones posteriores.

Ley de Enjuiciamiento Civil 11/2000, de 7 de enero, BOE núm. 7, de 8 de enero de 2000 y modificaciones posteriores.

Ley de Enjuiciamiento Criminal, aprobada por Real Decreto de 14 de septiembre de 1882; Gaceta de Madrid núm. 260, de 17 de septiembre de 1882 y modificaciones posteriores.

Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales; BOE núm. 294, de 6 de diciembre de 2018 y modificaciones posteriores.

Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial; Legislación consolidada, BOE, núm. 157, de 02 de julio de 1985 y modificaciones posteriores.

Ley Orgánica 10/1995, de 23 de noviembre; Código Penal; Legislación consolidada, BOE núm. 281, de 24 de noviembre de 1995 y modificaciones posteriores.

Puerta Luis, L. R. (1995). La prueba en el proceso penal. Aldaba, (24), 47-80.

Queralt Jiménez, J. J. (2008). Derecho Penal Español. Parte especial, 5ª ed. Atelier, Barcelona.

Real Decreto 255/2019, de 12 de abril, por el que se amplía la plantilla orgánica del Ministerio Fiscal para adecuarla a las necesidades existentes; BOE núm. 89, de 13 de abril de 2019, (19 págs.) (creación del Fiscal de Sala de Criminalidad Informática). Fiscal General del Estado.

Segarra Crespo, M. J. (2018). Memoria Elevada al Gobierno de S. M. Presentada al Inicio del Año Judicial por la Fiscalía General del Estado; Ministerio de Justicia, Madrid, 2018. Fiscal General del Estado.