Ciberdelincuencia: perspectiva penal, procesal y criminológica

Coordinadores

Daniel González Uriel
Alfredo Abadías Selma
Laura Cristina Morell Aldana

LA LEY

ARANZADI LA LEY, S.A.U.
C/ Collado Mediano, 9
28231 Las Rozas (Madrid)
www.aranzadilaley.es
Atención al cliente: https://areacliente.aranzadilaley.es/

Primera edición: Marzo 2025

Depósito Legal: M-4565-2025
ISBN versión impresa: 978-84-10292-54-3
ISBN versión electrónica: 978-84-10292-55-0

Diseño, Preimpresión e Impresión: ARANZADI LA LEY, S.A.U.
Printed in Spain

ÍNDICE SISTEMÁTICO

II. PERFIL DE LOS CIBERESTAFADORES

El Director de la multinacional Kaspersky, Fabio ASSOLINI, o el Country Manager de Bolivia y Perú de Palo Alto Networs, Kenneth TOVAR ROCA, sendas empresas multinacionales en ciberseguridad, han destacado en diversas intervenciones cómo el perfil de los ciberdelincuentes ha evolucionado con el paso de los años, destacando actualmente los jóvenes autodidactas, curiosos, proactivos, duchos en el manejo de las nuevas tecnologías, que adquieren sus habilidades a través de recursos gratuitos en Internet o a través de foros y grupos cerrados de comunicación donde se reúnen virtualmente numerosos ciberdelincuentes que comparten ideas, y «métodos», término que en su argot es utilizado para designar los procedimientos necesarios que hay que llevar a cabo para ejecutar un ataque informático tras haber encontrado una vulnerabilidad en un sistema o una brecha de seguridad desde la que se puede acceder al servidor central que contiene datos sensibles de la corporación afectada, sus empleados o clientes.

La motivación de estos jóvenes ciberdelincuentes suele ser de tipo económico, ya que saben que con una mínima inversión y esfuerzo desde su teléfono móvil u ordenador pueden obtener ganancias muy elevadas sin necesidad de formarse y trabajar en una actividad legal, además de lo que ese estatus de poder les proporciona dentro de su entorno juvenil, así como es el puente hacia una vida de lujos y derroches que de otro modo no podrían permitirse.

En cambio, el perfil de las personas que ejercen como muleros dista un poco de la imagen que se ha ido conformando en torno a los ciberestafadores, ya que en base a la experiencia policial y los numerosos casos investigados y analizados, se puede observar, en líneas generales, que las mulas bancarias son personas con escasos recursos económicos y escasa formación, con aspiraciones limitadas y que o bien tienen deudas contraídas o bien tienen adiciones vinculadas al consumo de alcohol o drogas y el dinero que obtienen al servicio de organizaciones criminales vinculadas al fraude online, es invertido en satisfacer esas necesidades creadas.

No obstante, es complejo establecer un perfil genérico que describa a todas las personas que de una u otra forma están relacionadas con fraudes online, ya que son muchos los factores que pueden llevar a una persona a cruzar la línea de la legalidad, pero sí podría decirse que todos ellos tienen en común la búsqueda de beneficios económicos, aunque ello implique la comisión de delitos.

III. DIFICULTADES INVESTIGATIVAS Y PROCESALES

Atendiendo a las dificultades que presenta una investigación en la que acontece un fraude informático, los problemas ya se presentan desde el inicio, al encontrar multitud de hechos delictivos interconectados, por tratarse del mismo sujeto pasivo, las mismas «cuentas mula[4]», idénticos números de teléfono utilizados —o aun tratándose de diferentes números de abonado se comprueba que pertenecen a la misma persona—, fotogramas que muestran a los mismos sujetos realizando extracciones bancarias en cajero o de cambio de cripto activos, o incluso por el uso de los mismos números de imei, que es el identificador único de particulariza cada terminal móvil. Si bien, ante la presencia de más de un centenar de hechos relacionados, la pregunta que le surge a todo investigador es ¿dónde judicializar? ya que la respuesta a esa pregunta marcará el futuro de la investigación y de ello dependerá que prospere o quede inmersa la misma en una rueda de conflictos de competencias.

El Convenio sobre el Cibercrimen, conocido como «Convenio de Budapest»[5], por haberse celebrado en esa ciudad el día 23 de noviembre de 2001, y que fue ratificado por España el día 27 de septiembre de 2010, establece en su artículo 22.5, entre otras cosas, que el Estado competente para llevar a cabo una investigación es el que se encuentre en mejores condiciones para ejercer la persecución del delito, remarcando la necesidad de aplicar, con carácter prioritario, una política penal común.

Esa política común europea es un objetivo ambicioso y complejo de implementar más aun cuando se observan diferentes criterios competenciales como nación, dado que no todos los órganos jurisdiccionales entienden la competencia de la misma manera en el ámbito de la ciberdelincuencia y eso genera muchas dificultades en el desarrollo exitoso de una operación policial.

La competencia jurisdiccional[6] se entiende como «la atribución de potestades a un determinado órgano jurisdiccional para tramitar y resolver un litigio con exclusión de otros tribunales», y el artículo 14.2 de la Ley de Enjuiciamiento Criminal atribuye la competencia al juzgado del partido judicial en el que se haya cometido el delito. Por ende, es preciso concretar el lugar de comisión del ilícito. En términos

(4) SEPBLAC, Alerta sobre el uso de cuentas mula. URL: https://www.sepblac.es/es/2024/06/10/alerta-mula/ (08/10/2024).

(5) BOE, *Instrumento de Ratificación del Convenio sobre la Ciberdelincuencia, hecho en Budapest el 23 de noviembre de 2001*. URL: https://www.boe.es/eli/es/ai/2001/11/23/(1) (08/10/2024).

(6) Diccionario Panhispánico del español jurídico, *competencia jurisdiccional*. URL: https://dpej.rae.es/lema/competencia-jurisdiccional (08/10/2024).

de cibercriminalidad determinar inicialmente que esa cuestión es prácticamente inviable dado que los elementos del tipo de la estafa informática se desarrollan, consuman o surten efectos en distintos lugares geográficos, lo cual ocasiona a diario numerosas dudas sobre qué Juzgado es competente para conocer de un determinado hecho.

En relación con esta problemática, la Sala 2.ª del Tribunal Supremo se ha pronunciado en numerosas ocasiones, dictando diversas sentencias(7) sobre qué tribunal sería competente territorialmente para investigar delitos de estafa informática, ya que hasta el momento prevalecía el principio de la ubicuidad(8), que entiende que el delito se comete en todas las jurisdicciones en las que se haya realizado algún elemento del tipo siendo competente para la instrucción de la causa el Juez o Magistrado que primero haya iniciado las actuaciones procesales en cualquiera de las jurisdicciones implicadas. Si bien, el Tribunal Supremo, según su doctrina jurisprudencial consolidada, se une al razonamiento del Convenio de Budapest y establece como válido el criterio de la eficacia de la instrucción que permite atribuir la competencia al órgano judicial que se encuentre en mejores condiciones de abordar la persecución del delito, y para ello es necesario tener en cuenta otros aspectos relevantes como el lugar donde se urdió el plan criminal para llevar a cabo la acción típica, el lugar donde haya pruebas del delito, la residencia del delincuente, o incluso donde se haya constituido la estructura de la organización.

No obstante, pese a que el Alto Tribunal, ha indicado en numerosas ocasiones su postura laxa respecto de la teoría de la ubicuidad y su aplicación en los delitos tecnológicos, especialmente relacionados con el fraude online, todavía son muchos los Juzgados españoles que se muestran reticentes a valorar los hechos en su conjunto y magnitud real y evitan instruir causas que engloben ilícitos penales cuyas víctimas han interpuesto denuncia en otro partido judicial, pese a que en los oficios y atestados policiales quede acreditado que se trata de un mismo grupo u organización criminal, todo ello por miedo a que esos procedimientos den lugar a macro causas con instrucciones complejas que colapsen el Juzgado por la falta de medios y recursos para hacer frente a estos ciberdelitos que han aparecido como un volcán en continua erupción sin dar tiempo a que el Poder Judicial y las Fuerzas y Cuerpos de Seguridad se

(7) Sentencia del Tribunal Supremo, Sala Segunda, de 17 de febrero de 2022 (Roj: ATS 2739/2022 - ECLI:ES:TS:2022:2739A, Roj: ATS 2736/2022 - ECLI:ES:TS:2022:2736A) y Sentencia del Tribunal Supremo, Sala Segunda, de 7 de noviembre de 2018 (Roj: ATS 11424/2018 - ECLI:ES:TS:2018:11424A).

(8) Sentencia del Tribunal Supremo, Sala Segunda, de 17 de marzo de 2005 (STS 341/2005).

preparen y conciencien de que la investigación y persecución de estos ilícitos penales absorbe muchos recursos tanto judiciales como policiales y requieren una respuesta más rápida y contundente que quizá otros que forman parte de la conocida «delincuencia tradicional».

Es cierto que el aglutinar todas las denuncias relacionadas en un mismo procedimiento judicial puede dar lugar a las ya nombradas macro causas inabarcables que, a su vez, colapsen los juzgados, lo cual incrementaría los tiempos de instrucción y generaría dificultades a nivel procesal, siendo entendible la reticencia de muchos juzgados de acoger más denuncias en unas mismas Diligencias Previas que las que tienen lugar en su partido judicial, pero el hecho de no abarcar todos los hechos en su totalidad en el mismo procedimiento puede dar lugar a que la pirámide organizacional quede incompleta o lo que es peor, que sólo se pueda identificar a las mulas que se encuentran en el escalón más bajo de la organización, quedando impunes los ideólogos del fraude, programadores, vendedores clandestinos y líderes del entramado criminal, siendo importante tener en cuenta que estas personas continuarán llevando a cabo los delitos investigados con los mismos muleros o con otros, porque en los canales cerrados de comunicación de diversas aplicaciones de mensajería instantánea existe un auténtico «mercado de mulas»[9] que no cesa, y pese a acumular en su historial numerosas detenciones policiales y reseñas judiciales continúan ofreciendo su colaboración a los cibercriminales a cambio de una pequeña contraprestación económica.

Hay que tener en cuenta que esa dificultad que puede generar a un Juzgado de Instrucción el acoger un procedimiento con multitud de denuncias parejas en distintas provincias de España puede acarrear una tarea ardua que también es difícil para los investigadores policiales, quienes deben de coordinarse con sus homólogos de otras plantillas para recopilar todos esos hechos antes de que algún grupo investigador trate la denuncia como un caso aislado y lo remita al Juzgado, generando que una misma investigación tenga diferentes Diligencias Previas abiertas por toda España.

Si bien, en muchas ocasiones, hasta que no se realizan las primeras actuaciones policiales —que en la mayoría de los casos requieren habilitación judicial— no se pueden establecer relaciones objetivas con otras denuncias interpuestas en otras provincias y que es posible que, a su vez, hayan dado lugar igualmente a la apertura de un procedimiento judicial.

(9) SANZ ROMERO, Marta, «Así se recluta a un mulero bancario: el compinche incauto de los hackers que podrías ser tú sin saberlo», publicada en el periódico online *El Español*. URL: https://www.elespanol.com/omicrono/software/20220424/recluta-bancario-compinche-incauto-hackers-podrias-sin/666433593_0.html (08/10/2024).

Por ello, es necesario partir de la base de que, en la investigación de delitos tecnológicos, y concretamente relacionados con el fraude informático, esta situación es muy habitual que suceda, dado que Internet no tiene fronteras ni límites espaciales y, por tanto, los perjudicados de una misma acción típica pueden encontrarse en cualquier parte del territorio nacional, incluso en cualquier país del mundo.

Es fundamental la concienciación tanto de los órganos judiciales como de los cuerpos policiales sobre cómo investigar este tipo de delitos, ya que, partiendo de la base de que en los delitos de estafa bancaria lo más importante es la celeridad, las primeras actuaciones, el poder solicitar a la entidad bancaria el destino de ese dinero. Por la experiencia de los grupos de investigación de policía judicial, el dinero no acaba en una única cuenta bancaria sino que se va distribuyendo entre diferentes cuentas controladas por la organización para finalmente acabar en una extracción en cajero o desviarlo a una tarjeta que permite la conversión en criptoactivos, de ese modo, se perdería la trazabilidad física y comenzaría una trazabilidad virtual, lo que implica que la investigación debe de estar judicializada porque bien para seguir la vía física o bien para seguir la virtual, es necesario contar con habilitaciones judiciales así como con Órdenes Europeas de Investigación, ya que la mayoría de los Exchange que controlan el flujo de las criptomonedas y las «*wallet*» o monederos virtuales de criptomonedas, se encuentran en países de la Unión Europea o incluso en terceros países que requieran una Comisión Rogatoria Internacional para aportar los datos solicitados.

Todas estas gestiones son completamente necesarias para poder investigar delitos económicos y, por tanto, es fundamental contar con el plácet de Jueces y Fiscales, siendo muy importante que los Juzgados conozcan la necesidad y urgencia de que la policía lleve a cabo este tipo de peticiones de información.

IV. HERRAMIENTAS DE INVESTIGACIÓN CON HABILITACIÓN JUDICIAL

Igualmente, cuando el fraude online se lleva a cabo mediante las técnicas de «vishing», un tipo de estafa de ingeniería social por teléfono en la que, a través de una llamada, se suplanta la identidad de una empresa, organización o persona de confianza, con el fin de obtener información personal y sensible de la víctima, o «spoofing», técnica más sofisticada que el vishing que además suplanta el número de teléfono real de un tercero generando mayor confianza en la víctima objeto del fraude, es muy importante para el grupo investigador poder acceder a la observación

de las comunicaciones del terminal telefónico que realiza las llamadas fraudulentas, cuya petición se realizará de manera urgente y, por supuesto, gozará de la oportunidad y necesidad que la Ley requiere, dado que la observación de las comunicaciones aportará información muy útil para poder identificar a los presuntos autores, ya que teniendo intervenida la línea se puede realizar una localización in situ con medios técnicos, verificar los datos que aporten en las conversaciones con terceros o consortes, incluso obtener un pasaporte vocal de los investigados que permita posteriormente un cotejo pericial por si su voz ya obrase en las bases de datos policiales, así como el estudio permitirá conocer determinados rasgos de su personalidad, estado de ánimo o región geográfica a la que pertenece.

Por tanto, es fundamental la celeridad en solicitar y aplicar esta medida judicial dado que, con base en la experiencia investigativa de este tipo de redes criminales, se puede afirmar que es habitual por parte de los cibercriminales el constante cambio de líneas y terminales telefónicos, para evitar, precisamente, cualquier tipo de intervención policial durante la comisión delictiva. Igualmente, es importante tener en cuenta que esa medida no siempre registra el tráfico de llamadas, puesto que el grueso de las conversaciones que intercambian los investigados entre ellos son encriptadas y las ejecutan a través de canales cerrados de comunicación, utilizando aplicaciones cifradas de extremo a extremo «end to end encryption o E2EE[10]», por lo que para conocer el contenido de esas llamadas que no utilizan la red de telefonía convencional, sino que utilizan el cifrado mediante VoIP[11] —abreviatura por la que se conoce a los servicios de comunicaciones vocales basados en el protocolo IP—, es necesario por parte de los grupos investigadores solicitar a la Autoridad Judicial el uso de medidas judiciales más contundentes y efectivas en este tipo de casos, como lo son por ejemplo el registro remoto o el agente encubierto virtual.

En cuanto al registro remoto, su regulación se encuentra en el artículo 588 septies de la Ley de Enjuiciamiento Criminal, que dice que «*El juez competente podrá autorizar la utilización de datos de identificación y códigos, así como 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*

(10) INCIBE, *Estudio de ciberseguridad en redes TETRA*. URL: https://www.incibe.es/sites/default/files/2023-05/INCIBE-CERT_ESTUDIO_CIBERSEGURIDAD_EN_REDES_TETRA_2023_v1.0.pdf (09/10/2024).

(11) COMISIÓN DEL MERCADO DE LAS TELECOMUNICACIONES, DT 2008/1650, *Informe SETSI sobre VoIP*.

datos (...)». Esa medida, pese a que Ley de Enjuiciamiento Criminal contempla su aplicación como última ratio en la escala de medidas restrictivas de derechos fundamentales, podría describirse en la práctica policial como un volcado anticipado de un terminal telefónico incautado en una entrada y registro, con la diferencia de que la información que se puede obtener del registro remoto es a tiempo real, lo que permite observar las comunicaciones no solo que se producen vía VoIP sino también por escrito a través de aplicaciones de mensajería instantánea, lo que resulta sumamente útil para avanzar en el esclarecimiento de los hechos, y para conocer la estructura criminal y los roles de cada uno de sus miembros que en muchas ocasiones ni siquiera se conocen físicamente sino que la relación que les une es virtual, llevando a cabo sus reuniones y reparto de tareas en canales cerrados de comunicación, creados al efecto por ellos mismos, y accesibles desde sus terminales telefónicos; así como se puede conocer qué herramientas informáticas han utilizado o están empleando para llevar a cabo las estafas mediante ingeniería social que, en la mayoría de los casos, los ciberdelincuentes tienen igualmente instaladas en sus teléfonos móviles.

En cuanto al agente encubierto informático, está regulado en el artículo 282 bis de la Ley de Enjuiciamiento Criminal, concretamente en su apartado sexto, y reza así:

> *(...)6. El juez de instrucción podrá autorizar a funcionarios de la Policía Judicial para actuar bajo identidad supuesta en comunicaciones mantenidas en canales cerrados de comunicación con el fin de esclarecer alguno de los delitos a los que se refiere el apartado 4 de este artículo o cualquier delito de los previstos en el artículo 588 ter a.*
>
> *El agente encubierto informático, con autorización específica para ello, podrá intercambiar o enviar por sí mismo archivos ilícitos por razón de su contenido y analizar los resultados de los algoritmos aplicados para la identificación de dichos archivos ilícitos (...)*

Teniendo en cuenta que el grueso de las comunicaciones entre ciberestafadores transcurren en los referidos canales cerrados de comunicación, tener presente el uso de la figura del agente encubierto virtual resulta completamente necesario a fin de poder desarrollar investigaciones de calidad, deteniendo a toda la cadena de mando de las organizaciones criminales y poniéndolos a disposición judicial. Para ello es necesario que desde el inicio de la investigación, y tras conocer los canales de comunicaciones donde interactúan los ciberdelincuentes, se haga uso de esta figura con la habilitación judicial correspondiente, en aras a poder extraer toda la información posible que permita la plena identificación de las personas que se

encuentran en la cúspide delincuencial y que no solo «trabajan» integrados en una organización criminal sino que dotan de herramientas delictivas a diferentes grupos criminales, extendiendo la idea del «crime as a service[12]», crimen como un servicio.

También hay que tener en cuenta en este tipo de delitos, que se ha extendido mucho la figura delictiva conocida como «dropper»[13], que si bien el Instituto Nacional de Ciberseguridad lo define como «*un tipo de malware que se caracteriza por contener un archivo ejecutable, como puede ser un .exe, .msi, .docm, etc. En ocasiones, únicamente está compuesto por un código inofensivo a simple vista que se activará cuando reciba la orden para descargar el malware que se encargará de infectar la máquina»,* en el argot delincuencial, sirve para designar a las personas que, dentro de esa idea de «crime as a service» proporcionan a los cibercriminales el blanqueo de capitales del dinero estafado, dándole salida a través de criptomonedas. De ese modo, su labor sería la de canalizar el dinero desde una cuenta mula hasta una cartera virtual de criptomonedas, para de ese modo, moverlo entre diferentes blockchain[14], tratando de que se pierda cualquier rastro de ese dinero, para posteriormente depositarlo o ponerlo en manos de los cibercriminales que lo contrataron, totalmente blanqueado, todo ello a cambio de un porcentaje de las ganancias.

Para poder llevar a cabo la trazabilidad de esas criptomonedas y descubrir el destino final que tienen, es necesario contar con la aprobación de los Jueces y Fiscales para emitir Órdenes Europeas de Investigación o Comisiones Rogatorias Internacionales, pues la mayor parte de los Exchange por donde pasan las criptomonedas objeto del fraude, se encuentran fuera de España y requieren de habilitación judicial para facilitar datos a las Fuerzas y Cuerpos de Seguridad, amparándose en la normativa internacional de Protección de Datos, resultando estos instrumentos de cooperación internacional completamente necesarios para poder avanzar en las investigaciones económicas que se desarrollan en el plano online.

Por tanto, es fundamental que en la lucha del cibercrimen se utilicen todos los medios y herramientas al alcance de jueces, tribunales y policía para poder llevar a cabo una acción contundente y desarticular la cúpula de

(12) CC-DRIVER, *Drivers, Trends, and Technology Evolution in Cybercrime*. URL: https://cordis.europa.eu/project/id/883543/results#:~:text=Drivers%2C%20trends%20and%20technology%20evolution%20in%20cybercrime (09/10/2024).

(13) INCIBE, *Dropper, la amenaza silenciosa*. URL: https://www.incibe.es/empresas/blog/dropper-amenaza-silenciosa (09/10/2024).

(14) INCIBE, *Blockchain: de A a B sin intermediarios humanos*. URL: https://www.incibe.es/sites/default/files/docs/c10-pdf-infografia-blockchain-sin-intermediarios.pdf (09/10/2024).

las organizaciones criminales que son las que controlan el escenario virtual y se valen de los muleros y otros actores para completar su acción criminal sin exponerse. Teniendo en cuenta que la policía siempre va un paso por detrás de los cibercriminales, ya que cuando se tiene conocimiento de un hecho criminal el mismo ya ha ocurrido, es muy difícil, casi imposible, anticiparse a este tipo de acciones delincuenciales que tienen lugar en el campo virtual, por ello, y teniendo en cuenta la presente desventaja que tiene la policía al investigar estos delitos es necesario usar medidas que aseguren y garanticen la efectividad policial y jurídica en el proceso penal que se inicie en contra de los autores materiales.

V. CONCLUSIONES

La delincuencia está cambiando, no se trata de un fenómeno estático sino dinámico, en constante evolución. Las estafas tradicionales se han reconvertido al plano digital aprovechando la facilidad de acción que ofrecen las nuevas tecnologías, aportando anonimato e interconectividad, sin siquiera ser necesario mantener reuniones físicas con sus consortes, sino que existen verdaderos mercados criminales al alcance de cualquier persona, donde los ciberdelincuentes entran en contacto con otros en cuestión de minutos o segundos. En esos foros de cibercriminales las herramientas de hacking para cometer fraudes online están al alcance de cualquiera, así como los datos bancarios o personales de las víctimas son tratados con verdadero desprecio, regalándolos incluso cuando ya han sido utilizados para múltiples fines. En esos canales de comunicación aparecen todo tipo de actores con los que montar «*la obra de teatro*»: muleros, captadores de mulas, falsificadores, blanqueadores, programadores... cada uno con su tarifa de precios y hoja de servicios, elevando al máximo exponente el lema de «crime as a service» expuesto en párrafos anteriores.

Sin duda, los mayores perjudicados de este apogeo de fraudes online son las víctimas, quienes lo son de manera indefinida e indeterminada, convirtiéndose en muchas ocasiones en presuntos cooperadores necesarios o muleros, ya que tras ser víctimas de una estafa, esas identidades son «*reutilizadas*» por los cibercriminales para abrir cuentas bancarias a nombre de esas personas, usurpando su identidad y convirtiéndoles de ese modo en responsables del presunto fraude, ya que los titulares de las «cuentas mula» serán los primeros sobre los que recaerán las primeras sospechas y acusaciones.

Este hecho implica que los fraudes informáticos provoquen una «multi victimización» y miedo continuo en las personas que han sido perjudicadas

por algún delito de este tipo, pues la indefensión y la desconfianza son sentimientos que se han vinculado a las nuevas tecnologías en los últimos años, ya que el que ha visto comprometidos sus datos bancarios y/o personales vive con el desasosiego continuo de pensar que en cualquier momento puede volver a ser víctima de otro fraude o, lo que es peor, verse relacionado en algún ilícito penal del que no forma parte.

Para combatir el fenómeno de la cibercriminalidad se requiere unión en todos los sentidos: como nación, uniendo fuerzas entre el poder ejecutivo y judicial así como con las Fuerzas y Cuerpos de Seguridad, para poder exteriorizar esa acción conjunta en el ámbito internacional y luchar contra esta delincuencia desplegando todas fortalezas como país, ya que no existe otro modo de combatir la universalidad, transversalidad y atemporalidad que caracterizan a este tipo de delitos cometidos en el plano online. Es fundamental esa unión internacional y la coordinación policial y judicial para acabar con estas redes criminales que día tras día atentan contra la paz pública y contra la sociedad en general, sin hacer distinciones de clases, ya que cualquier persona puede ser víctima de un delito de estafa informática, por muy formada y concienciada que esté al respecto.

Por ello, y junto con la unidad de acción es imprescindible actuar con celeridad y responder de manera contundente, aprovechando el mínimo descuido que hayan podido cometer los cibercriminales, antes de que ese rastro se pierda o desaparezca, ya que, a diferencia de los delitos cometidos en el plano físico, estos delitos apenas dejan huella o si la dejan permanece intacta por tiempo muy limitado, de ahí que sea importante ejecutar las medidas investigativas tan pronto como sea posible.

La lucha contra los fraudes informáticos parece *a priori* una batalla perdida pero no lo es, solamente hay que ser persistentes y no dejar de avanzar, poniendo el foco de atención en la cúspide del crimen organizado, ya que en el ámbito tecnológico no hay ningún hecho que se cometa de manera aislada por una sola persona, sino que la inmensa mayoría de las denuncias de fraude online, por pequeñas que parezcan en cuantía, forman parte de un plan preconcebido donde hay múltiples actores que hacen posible su materialización. Poniendo a disposición de la justicia a los líderes de esos grupos y organizaciones criminales dedicadas a cometer estafas informáticas, se conseguirá poco a poco ir haciendo de Internet un lugar un más seguro.

CAPÍTULO 15

COOPERACIÓN JUDICIAL CONTRA LA CIBERDELINCUENCIA. LA PRUEBA DIGITAL INTERNACIONAL

Joaquín Delgado Martín
Magistrado de la Sala Penal de la Audiencia Nacional
Doctor en Derecho. Experto en Derecho Digital
Miembro de la Red de Especialistas en Derecho UE (REDUE)

I. NECESIDAD DE LA COOPERACIÓN JUDICIAL INTERNACIONAL FRENTE A LA CIBERDELINCUENCIA

En la investigación y enjuiciamiento de los ciberdelitos concurren una serie de dificultades y complejidades, especialmente en su dimensión internacional, que implica que la cooperación entre autoridades judiciales de diferentes países resulta clave para obtener las evidencias digitales para su persecución.

1. Desafíos para la persecución de los ciberdelitos

La ciberdelincuencia presenta dificultades para su investigación y prueba por los órganos públicos del sistema penal.

1.1. Volatilidad. Peligro de pérdida de datos

Efectivamente, nos encontramos con un tipo de delincuencia cuyo rastro (huella digital) se transforma y desaparece con rapidez **(volatilidad)**. Existe una volatilidad de los datos en poder de los proveedores de servicio, que se deriva de dos elementos: muchos Estados no tienen normativa que obligue a la retención de datos para la investigación penal; y los requisitos de minimización de datos obligan a los proveedores a eliminar datos más rápidamente (protección de datos personales). Y la pérdida de datos también se relaciona con los desafíos relacionados con la gobernanza de Internet, la encriptación de comunicaciones, y el uso de criptomonedas[(1)]. Por tanto, los medios de investigación del sistema penal han de ser lo suficientemente ágiles como para acceder a los datos y conservarlos a disposición judicial con las suficientes garantías.

(1) EUROJUST-EUROPOL, «Common challenges in combating cybercrime as identified by Eurojust and Europol», June 2019; https://www.europol.europa.eu/publications-documents/common-challenges-in-combating-cybercrime

1.2. Complejidad técnica. Desafíos de las novedades tecnológicas

El acceso a los datos y su incorporación al proceso exige la realización de determinadas operaciones técnicamente complejas **(complejidad técnica)**, para lo cual es necesario que el sistema penal cuente con los recursos necesarios: formación de profesionales, instrumentos tecnológicos adecuados para la obtención de la información y su ulterior preservación, y normativa que regule de forma adecuada la obtención de datos y los medios probatorios (prueba digital).

Los autores de ciberdelitos también pueden utilizar **técnicas que dificultan aún más la investigación y prueba del delito**: el cifrado de datos, Darknet, VPN (Virtual Private Network), el Snapchat..., así como los sistemas de anonimización, la tecnología NAT móvil, etcétera. Muchos proveedores utilizan la **encriptación** para sus servicios, frecuentemente de manera predeterminada, permitiendo el cifrado personal y el anonimato de las comunicaciones. Constituye un elemento esencial en la sociedad digitalizada, ayudando a garantizar la protección de nuestros derechos humanos más fundamentales y a proteger la seguridad de nuestra economía digital; pero también es verdad que facilita oportunidades significativas para los delincuentes. En definitiva, dificulta la utilización de las medidas de investigación tecnológica, lo que resulta especialmente preocupante en materia de explotación sexual infantil o de terrorismo.

También existen obstáculos a la investigación que derivan de la utilización por los proveedores de la **tecnología Carrier-Grade Network Address Translation** (CGN o Carrier Grade NAT), que permite compartir una sola dirección IPv4 pública entre múltiples suscriptores (usuarios finales) al mismo tiempo (posiblemente varios miles). Se trata de una solución tecnológica utilizada por el 95% de los proveedores móviles (operadores de red y operadores de redes virtuales móviles) y cerca del 50% de los proveedores de servicios de Internet tradicionales (ISP: cable, fibra y ADSL) en todo el mundo. Téngase en cuenta que, para que los proveedores puedan identificar técnicamente a un usuario final tras un CGN basado en un IPv4 público, es necesario conocer una dirección IPv4, la hora precisa de conexión y el número de puerto de origen. Sin embargo, el número de puerto de origen no suele ser conservado por los proveedores de servicios electrónicos, las plataformas de redes sociales, los servicios de correoweb, los servicios de alojamiento de datos, etcétera; por lo que no se podrá individualizar al usuario final, sino que hay que investigar todos los usuarios asociados a esa dirección IPv4 [(2)].

(2) EUROJUST-EUROPOL, «Common challenges in combating...».

1.3. Localización de los datos. Internacionalización

Frecuentemente resulta difícil conocer la ubicación de la infraestructura del grupo criminal o del autor del delito, y/o la propia localización de los datos; lo que se complica cuando los investigados utilizan instrumentos de encriptación y/o anonimización de sus comunicaciones, las criptomonedas y la Dark Web. Téngase en cuenta que éstos van perfeccionando sus medidas de seguridad y adaptando su «modelo de negocio ilícito» a los avances tecnológicos y al resultado exitoso de investigaciones policiales. En estos casos será complicado establecer la concreta jurisdicción competente y el régimen jurídico aplicable para la obtención de los datos mediante medidas de investigación tecnológica.

Cabe destacar la frecuente presencia de un **componente internacional**[3]: por un lado, pueden desplegar efectos en un Estado sin que el autor se encuentre físicamente presente en el territorio sometido a su jurisdicción y/o encontrándose los datos en servidores localizados en otro país **(internacionalización)**; y, por otra parte, los autores se benefician de las posibles lagunas de punibilidad que pueden existir en ciertos Estados **(transnacionalidad)**.

2. Complejidad de la prueba digital internacional

En la propia prueba digital concurren con frecuencia elementos internacionales, que también aportan importantes dificultades para la investigación y prueba en los procesos judiciales[4]: los proveedores de servicios y sus bases de datos se encuentran frecuentemente fuera de nuestro territorio nacional (Apple, Facebook, Instagram, Twitter, WhatsApp....), y en concreto los sistemas de almacenamiento cloud suelen localizar sus servidores en otros países; existen casos en los que el autor del acto ilícito está en un país, mientras que las víctimas se encuentran en otro u otros Estados[5]; los autores buscan en ocasiones alojar los datos en servidores sometidos a legislaciones más permisivas en la materia, beneficiándose de las posibles lagunas de punibilidad que pueden existir en ciertos países (transnacionalidad); los actos ilícitos

(3) Moisés BARRIO ANDRÉS, «Los delitos cometidos en internet. Marco comparado, internacional y derecho español tras la reforma penal de 2010», *La Ley Penal*, n.º 86, Sección Legislación aplicada a la práctica, Octubre 2011.

(4) Véase mi monografía «Judicial-Tech: El proceso digital y la transformación tecnológica de la justicia», editorial Wolters Kluwer, octubre 2020.

(5) Sobre los problemas de aplicación territorial de la Ley penal en los delitos informáticos, véase el apartado VI de Ricardo M. MATA Y MARTIN, «Criminalidad informática: una introducción al cibercrimen», *Actualidad Penal*, n.º 37, Sección Doctrina, Semana del 6 al 12 de octubre de 2003, Ref. XXXVI, tomo 3, páginas 935 y ss.

pueden desplegar efectos en un Estado sin que el autor se encuentre físicamente presente en el territorio sometido a su jurisdicción y/o encontrándose los datos en servidores localizados en otro país,...

La obtención de una prueba digital en otro Estado no solamente aporta elementos de gran complejidad técnica y jurídica, sino que también puede resultar contraria a los propios intereses nacionales del Estado requerido, ya sean legítimos como la defensa de su soberanía, ya tengan menos legitimidad como ocurre con los paraísos de impunidad tecnológica(6). Por ello, una estrategia que aborde adecuadamente estos problemas ha de establecer mecanismos de mejora de la cooperación judicial y policial internacional.

2.1. Falta de un marco legal adecuado

En primer lugar, a menudo concurre una insuficiencia de los ordenamientos nacionales y diferencias entre los mismos; así como un diferente tratamiento legal de la retención y acceso a los datos en los diferentes países, o incluso una falta de legislación nacional que lo regule.

En segundo lugar, la ausencia de instrumentos normativos internacionales adecuados contribuye a dificultar la utilización de los datos en poder de proveedores para la investigación y prueba de los delitos; sin perjuicio de los avances que se han dado últimamente: Segundo Protocolo del Convenio de Budapest; y Reglamento E-evidence. En este sentido, el apartado 8 del Preámbulo del Reglamento E-evidence afirma que «...*no existe un marco armonizado para la cooperación con los prestadores de servicios, mientras que algunos prestadores de terceros países aceptan solicitudes directas de datos que no sean datos de contenido si lo permite su Derecho nacional aplicable. Por ello, los Estados miembros dependen cada vez más de los canales de cooperación voluntaria y directa con los prestadores de servicios cuando se disponga de ellos, y aplican diferentes instrumentos, condiciones y procedimientos nacionales. Para los datos de contenido, algunos Estados miembros han adoptado medidas unilaterales, mientras que otros siguen confiando en la cooperación judicial*». Y su apartado 9 añade que «*la fragmentación del marco jurídico supone una dificultad para las autoridades policiales y las autoridades judiciales, así como para los prestadores de servicios que desean cumplir los requerimientos judiciales de pruebas electrónicas, ya que se*

(6) Nicolás CABEZUDO RODRÍGUEZ, «Ciberdelincuencia e investigación criminal. Las nuevas medidas de investigación tecnológica en la Ley de Enjuiciamiento Criminal», *Boletín del Ministerio de Justicia*, monográfico sobre «Las reformas de proceso penal», febrero 2016, página 19.

enfrentan cada vez más a una inseguridad jurídica y, potencialmente, a conflictos de leyes».

En este marco resulta especialmente relevante la utilización de las estructuras de colaboración entre autoridades judiciales y policiales de diferentes países, es decir, los instrumentos de cooperación policial y judicial internacional, tanto a nivel regulatorio (normas de cooperación o asistencia internacional) como institucional (instituciones, redes y otros foros de asistencia e intercambio de información y experiencias).

2.2. Dificultades en la obtención de datos en poder de los proveedores de servicios

El acceso a los datos en poder de los proveedores o prestadores de servicios constituye actualmente un **elemento esencial para la investigación de todo tipo de delitos**, y también para **asegurar el cumplimiento del ordenamiento jurídico en el ciberespacio**(7). Alexander SEGER considera que «*la obtención de pruebas electrónicas para su uso en procesos penales es esencial para el Estado de Derecho*»; y añade que «*la capacidad de los gobiernos para garantizar el estado de derecho en el ciberespacio seguirá siendo limitada, a menos que se puedan superar los impedimentos para acceder a datos y, por lo tanto, a pruebas electrónicas para la justicia penal. La falta de datos significa que no hay prueba, que no hay justicia, y por tanto la falta de estado de derecho*»(8).

Téngase en cuenta que los proveedores de servicios almacenan los datos de los usuarios en uno o varios servidores, que pueden hallarse en distintos países tanto dentro como fuera de la UE. Se calcula que en más del 50% de las investigaciones penales hay que cursar una solicitud de obtención de pruebas electrónicas(9). En estos casos, el acceso a estos datos por los órganos del sistema penal resulta mucho más complejo, deviniendo lento y costoso, e incluso en ocasiones materialmente imposible.

También concurren desafíos de la colaboración público-privada, que se concreta en tres cuestiones: marco legal; definición de la jurisdicción com-

(7) Véase mi trabajo «Prueba digital internacional. El Reglamento E-Evidence», publicado en *Diario LA LEY*, N.º 76, Sección Ciberderecho, 15 de septiembre de 2023.

(8) Alexander SEGER «Evidence in the cloud and the rule of law in cyberspace: avoiding the "jungle"». https://www.friendsofeurope.org/insights/evidence-in-the-cloud-and-the-rule-of-law-in-cyberspace-avoiding-the-jungle/

(9) https://www.consilium.europa.eu/es/policies/e-evidence/

petente; y retos asociados con las tecnologías nuevas y emergentes[10]. La inadecuación de esta colaboración puede tener efectos negativos sobre la investigación y prueba de los ciberdelitos.

II. PREVENCIÓN Y SOLUCIÓN DE CONFLICTOS DE JURISDICCIÓN EN LA CIBERDELINCUENCIA

Los elementos internacionales de numerosos delitos en los que se utilizan dispositivos electrónicos y comunicaciones digitales (por ejemplo, en materia de criminalidad organizada), y específicamente en materia de ciberdelincuencia[11], determinan con frecuencia la concurrencia de diversas jurisdicciones nacionales para su investigación y persecución, produciéndose conflictos de jurisdicción y distorsiones que afectan a la eficacia de la represión de esos delitos. Téngase en cuenta asimismo que, en los delitos cometidos a través de Internet, puede haber problemas para determinar el lugar de comisión de delito, y por tanto, para definir la jurisdicción competente de conformidad con el principio de territorialidad. Esta problemática ha de ser evitada desde una doble dimensión: la prevención de conflictos; y, por otro lado, el establecimiento de mecanismos para su solución.

1. Prevención de conflictos

Se trata de la prevención de los propios conflictos de jurisdicción, a través de la armonización de los criterios que determinan la competencia de los tribunales nacionales en las respectivas legislaciones internas de los Estados[12].

Destaca el art. 22 del Convenio de Budapest, que contempla que cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para afirmar su jurisdicción respecto de cualquier delito previsto con arreglo

(10) EUROJUST-EUROPOL, «Common challenges in combating cybercrime...».

(11) Isabel SÁNCHEZ GARCÍA DE PAZ e Isidoro BLANCO CORDERO recuerdan que *«los delitos cometidos a través de Internet presentan dos características que los hacen especialmente problemáticos a la hora de abordar las cuestiones de competencia penal de cada Estado. Por un lado, son, de modo absolutamente predominante, delitos de los denominados "a distancia". Esto es, delitos en los cuales la acción y el resultado tienen lugar en diferentes Estados. Son frecuentemente además, en segundo término, y como consecuencia de lo anterior, delitos de carácter internacional, en el sentido de que varios Estados aparecen implicados o afectados por la comisión del mismo»*, en «Problemas de derecho penal internacional en la persecución de delitos cometidos a través de Internet», *Actualidad Penal*, n.º 7, Sección Doctrina, 2002.

(12) Ignacio FLORES PRADA, «Prevención y solución de conflictos internacionales de jurisdicción en materia de ciberdelincuencia», *Revista Electrónica de Ciencia Penal y Criminología*, RECPC 17-21 (2015); http://criminet.ugr.es/recpc/17/recpc17-21.pdf, página 22.

a los arts. 2 a 11 del presente Convenio, siempre que se haya cometido: a) en su territorio; o b) a bordo de un buque que enarbole pabellón de dicha Parte; o c) a bordo de una aeronave matriculada según las leyes de dicha Parte; o d) por uno de sus nacionales, si el delito es susceptible de sanción penal en el lugar en el que se cometió o si ningún Estado tiene competencia territorial respecto del mismo.

Por otra parte, el mismo precepto dispone que cualquier Estado podrá reservarse el derecho a no aplicar o a aplicar únicamente en determinados casos o condiciones las normas sobre jurisdicción establecidas en los apartados 1.b) a 1.d) del presente artículo o en cualquier otra parte de los mismos. Asimismo, cada Parte adoptará las medidas que resulten necesarias para afirmar su jurisdicción respecto de los delitos mencionados en el apartado 1 del art. 24 del Convenio, cuando el presunto autor del delito se encuentre en su territorio y no pueda ser extraditado a otra Parte por razón de su nacionalidad, previa solicitud de extradición.

El apartado 4 del art. 22 contiene una cláusula según la cual el presente Convenio no excluye ninguna jurisdicción penal ejercida por una Parte de conformidad con su derecho interno.

2. Solución de los conflictos de jurisdicción

El art. 22.5 del Convenio de Budapest no fija un mecanismo de resolución vinculante de conflictos de jurisdicción, sino que se limita a establecer que *«cuando varias Partes reivindiquen su jurisdicción respecto de un presunto delito contemplado en el presente Convenio, las Partes interesadas celebrarán consultas, siempre que sea oportuno, con miras a determinar cuál es la jurisdicción más adecuada para las actuaciones penales»*.

En el ámbito de la UE se regula un sistema de solución de este tipo de conflictos con la participación de Eurojust, que se contiene Reglamento (UE) 2018/1727. En el ordenamiento interno español, debemos acudir a la Ley 29/2022, de 21 de diciembre, por la que se adapta el ordenamiento nacional al Reglamento (UE) 2018/1727 del Parlamento Europeo y del Consejo, de 14 de noviembre de 2018, sobre Eurojust, y se regulan los conflictos de jurisdicción, las redes de cooperación jurídica internacional y el personal dependiente del Ministerio de Justicia en el exterior. La tramitación puede resumirse de la siguiente forma:

A.- Una vez entablado **contacto directo** con la autoridad competente de otro Estado miembro y confirmada la tramitación paralela de dos procedi-

mientos penales contra la misma persona y respecto de los mismos hechos, el órgano judicial **oirá al Ministerio Fiscal y demás partes personadas** y, siempre y cuando no se haya declarado el secreto de las actuaciones, a las demás partes personadas por plazo común de diez días, sobre si procede la sustanciación de ambos procedimientos penales en un mismo Estado miembro y sobre los criterios que concurren para que la autoridad judicial española transfiera o no el procedimiento a otro Estado miembro (artículo 26.1 Ley 29/22).

B.- Tras esta audiencia, el juez o tribunal **promoverá el consenso** con la autoridad competente del otro Estado miembro, para lo que podrá solicitar la asistencia del miembro nacional de Eurojust:

C.- Conseguido el consenso entre las autoridades nacionales o, en su defecto, recibida la recomendación emitida por el miembro nacional o, en su caso, el dictamen del Colegio de Eurojust se oirá de nuevo al Ministerio Fiscal y, en su caso, a las demás partes personadas, en un plazo de cinco días. Tras ello **el juez o tribunal resolverá**, por auto motivado, dictado en el plazo de cinco días, sobre la procedencia de transferir o aceptar la transferencia del procedimiento a o del otro Estado. Este auto será notificado a la autoridad competente del otro Estado miembro y se pondrá en conocimiento de Eurojust a fin de que pueda facilitar su ejecución. Contra el mismo podrán interponerse los recursos ordinarios previstos en la Ley de Enjuiciamiento Criminal, que se tramitarán con carácter preferente y no tendrán efectos suspensivos (artículo 26.3 Ley 29/22).

D.- **Para la resolución del conflicto de jurisdicción el juez o tribunal tendrá en cuenta los siguientes criterios** (artículo 26.5 Ley 29/22):

a) Residencia habitual y nacionalidad de la persona investigada, acusada o procesada.

b) Lugar en el que se ha cometido la mayor parte de la infracción penal o su parte más sustancial.

c) Jurisdicción conforme a cuyas reglas se han obtenido las pruebas o lugar donde es más probable que estas se obtengan.

d) Interés de la víctima.

e) Lugar donde se encuentren los productos o efectos del delito y jurisdicción a instancia de la cual han sido asegurados para el proceso penal.

f) Fase en la que se encuentran los procedimientos penales sustanciados en cada Estado miembro.

III. LA PRUEBA DIGITAL INTERNACIONAL

En este apartado vamos a analizar los instrumentos de cooperación judicial para la obtención de evidencias digitales contra la ciberdelincuencia en dos ámbitos diferenciados: la cooperación judicial clásica (Comisión Rogatoria Internacional); y los mecanismos introducidos por la Unión Europea para mejorar la asistencia judicial entre sus Estados miembros.

1. Cooperación judicial Clásica

1.1. Normativa

La cooperación judicial internacional clásica gira en torno a los siguientes principios: el tribunal de un Estado no puede ejercitar su jurisdicción en el territorio de otro; un Estado, en uso de su soberanía, puede cooperar con otro realizando en su territorio y por sus propios órganos un acto procesal solicitado por el tribunal de ese otro Estado; si existe convenio internacional aplicable entre ambos Estados (bilateral o multilateral), nace la obligación jurídica de practicar el acto procesal solicitado por el otro Estado con pleno sometimiento a las condiciones del Tratado; y, a falta de Tratado, no existe obligación jurídica de practicar el acto procesal solicitado, pero el Estado requerido puede realizarlo esperando que el requirente se comporte de igual manera en el caso opuesto (principio de reciprocidad).

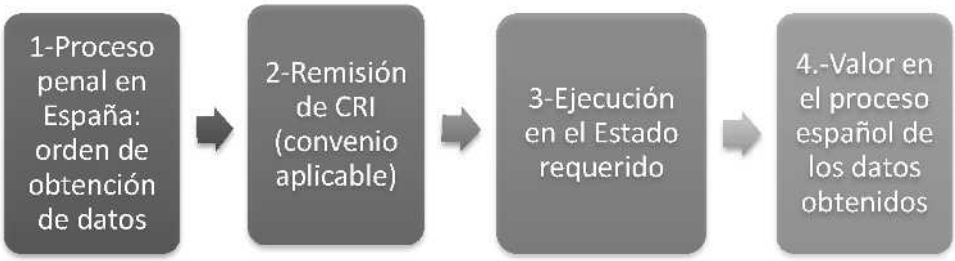
El art. 276 LOPJ, tras la reforma operada por la Ley Orgánica 7/2015, de 21 de julio, recoge las fuentes de la cooperación judicial internacional: *«las peticiones de cooperación internacional se tramitarán de conformidad con lo previsto en los tratados internacionales, las normas de la Unión Europea y las leyes españolas que resulten de aplicación»*.

En materia penal, la cooperación entre los distintos Estados va a girar en torno a dos elementos principales propios de la idea de cooperación antes analizada: las comisiones rogatorias internacionales (CRI), para la realización en otro Estado de un acto procesal de prueba, de notificación o de investigación, y la extradición, para conseguir la entrega de una persona para ser juzgada o para el cumplimiento de una pena.

El principal instrumento internacional en el ámbito de la investigación tecnológica y prueba digital es el Convenio de Budapest, sin perjuicio de los instrumentos de asistencia judicial y de reconocimiento mutuo existentes en el ámbito de la Unión Europea.

1.2. Fases de la cooperación judicial internacional

Cuando, en el seno de un proceso penal abierto en España resulta imprescindible la obtención (acceso) a datos (información en formato digital) que se encuentran fuera del territorio nacional, cabe distinguir cuatro fases:



Una primera fase radica en la existencia de una investigación penal en España, en la que se necesita la obtención de determinados datos en formato digital contenidos en dispositivos electrónicos, almacenados por prestadores de la sociedad de la información y/o transmitidos por redes (interceptación de comunicaciones en tiempo real) que estén sometidos a la jurisdicción de otro Estado. En el proceso judicial tramitado en nuestro país se ha de dictar la correspondiente resolución que ordene la obtención de dichos datos, lo que ha de tramitarse al amparo de la normativa procesal española, sin perjuicio del ulterior sometimiento a la normativa internacional aplicable.

Una segunda fase consiste en la remisión de la solicitud correspondiente, que ha de fundamentarse en el convenio internacional aplicable, bilateral o multilateral.

La tercera fase tiene como objeto la propia obtención de los datos, que tiene lugar en el Estado requerido. La regla general consiste en la *locus regit actum*, es decir, la ley aplicable a la ejecución es la interna del Estado requerido. Sin embargo, la normativa de la Orden Europea de Investigación posibilita la regla del *forum regit actum*, esto es, la aplicación de la normativa del Estado requirente, siempre que éste lo solicite de forma expresa y ello resulte compatible con los principios fundamentales del Estado requerido.

La cuarta fase consiste en la recepción en España del resultado de la actuación solicitada por Comisión Rogatoria Internacional (CRI), que se unirá

al proceso penal tramitado por el órgano judicial requirente y que despliega plenos efectos jurídicos en el procedimiento, sin perjuicio del valor en España de la prueba obtenida.

2. El convenio de Budapest

De forma subsidiaria a otro tratado más específico que resulte de aplicación, el Convenio sobre la Ciberdelincuencia, hecho en Budapest el 23 de noviembre de 2011, que ha sido ratificado por España (BOE 17 de septiembre de 2010), puede servir de base para peticiones de asistencia mutua.

Este convenio es muy relevante para fijar las bases de la lucha contra la ciberdelincuencia y para la obtención de prueba digital de todos los delitos, por dos razones: a) por las obligaciones penales y procesales asumidas por los Estados, que han sido desarrolladas en sus normativas internas; y b) por la introducción de instrumentos de cooperación internacional porque, a falta de tratado más específico, este Convenio puede servir de base para peticiones de asistencia mutua y para solicitudes de extradición.

En el momento de redacción de este trabajo, el Convenio de Budapest contra la Cibercriminalidad ha sido ratificado por 70 Estados de todos los continentes, de tal forma que se ha convertido en la **referencia mundial contra la cibercriminalidad.** Regula las siguientes cuestiones:

SISTEMA DEL CONVENIO DE BUDAPEST
A. Medidas provisionales
B. Remisión de datos
C. Acceso transfronterizo a datos
D. Otras formas: obtención en tiempo real

2.1. Asistencia mutua para medidas provisionales

Este instrumento internacional regula, dentro de la asistencia mutua para medidas provisionales, la llamada **conservación rápida de datos informáticos almacenados**.

El artículo 29.1 del Convenio establece que una Parte podrá solicitar a otra Parte que ordene o asegure de otra forma la conservación rápida de datos almacenados por medio de un sistema informático que se encuentre en el

territorio de esa otra Parte, respecto de los cuales la Parte requirente tenga la intención de presentar una solicitud de asistencia mutua con vistas al registro o al acceso de forma similar, la confiscación o la obtención de forma similar, o la revelación de los datos.

En las solicitudes de conservación que se formulen en virtud del apartado 1 se indicará (artículo 29.2):

a) La autoridad que solicita dicha conservación;

b) el delito objeto de investigación o de procedimiento penal y un breve resumen de los hechos relacionados con el mismo;

c) los datos informáticos almacenados que deben conservarse y su relación con el delito;

d) cualquier información disponible que permita identificar a la persona encargada de la custodia de los datos informáticos almacenados o la ubicación del sistema informático;

e) la necesidad de la conservación; y

f) que la Parte tiene la intención de presentar una solicitud de asistencia mutua para el registro o el acceso de forma similar, la confiscación o la obtención de forma similar o la revelación de los datos informáticos almacenados.

Una vez recibida la solicitud, la Parte requerida tomará las medidas adecuadas para conservar rápidamente los datos especificados de conformidad con su derecho interno. Las medidas de conservación tendrán una duración mínima de **sesenta días**, con objeto de permitir a la Parte requirente presentar una solicitud de registro o de acceso de forma similar, confiscación u obtención de forma similar, o de revelación de los datos. Cuando se reciba dicha solicitud, seguirán conservándose los datos hasta que se adopte una decisión sobre la misma (artículo 29.7).

Cabe la **denegación** en los siguientes supuestos (artículo 29.5): a) la solicitud hace referencia a un delito que la Parte requerida considera delito político o delito relacionado con un delito político; o b) la Parte requerida considera que la ejecución de la solicitud podría atentar contra su soberanía, seguridad, orden público u otros intereses esenciales.

A los efectos de responder a una solicitud, no se requerirá la **doble tipificación penal** como condición para proceder a la conservación (artículo 29.3); aunque cuando una Parte exija la doble tipificación penal como condición para atender una solicitud de asistencia mutua para el registro o el

En atención a los informes y balances oficiales de criminalidad, la ciberdelincuencia constituye un problema criminal en continua expansión, por lo que es preciso que se realicen esfuerzos concertados en prevención, en detección y represión de tales delitos.

La presente monografía ofrece un análisis profundo y transversal sobre los principales problemas que presentan estos ilícitos. Desde la perspectiva penal se abordan, entre otras cuestiones, las estafas informáticas, la IA en la prevención y represión del blanqueo, el discurso de odio en las redes sociales, la IA y los ciberdelitos contra la propiedad intelectual o las sociedades pantalla y la responsabilidad penal de las personas jurídicas.

En el ámbito procesal, el carácter transnacional y la ausencia de fronteras en la Red plantean enormes desafíos para la persecución de la cibercriminalidad. Varios capítulos se enfocan en su estudio, abordando temas que van desde la jurisdicción y competencia de los tribunales españoles hasta las diligencias de investigación útiles frente al fenómeno delictivo online. Además, se subraya el alcance transnacional de la ciberdelincuencia a través de la cooperación judicial internacional y se pone en valor un instrumento de gran potencial para enfrentar los ciberdelitos que operan en múltiples países: los equipos conjuntos de investigación.

ISBN: 978-84-10292-54-3

LA LEY