ARI 4/2021
14 de enero de 2021

El acceso a pruebas electrónicas y el cifrado, dos puntos clave de la agenda de seguridad europea

Javier Alonso Lecuit | Investigador sénior asociado del Real Instituto Elcano y miembro del Grupo de Trabajo sobre Ciberpolítica.

Tema

La agenda de seguridad de la Comisión Europea incluye iniciativas no exentas de complejidad y polémica para abordar la detección y acceso eficaz a información, habitualmente cifrada, en el curso de investigaciones criminales transnacionales.

Resumen

Los grandes proveedores de Internet, cuyo poder de mercado se apalanca en una ingente base de usuarios, marcan el ritmo de la transformación tecnológica de la red y las reglas de uso mundiales de las aplicaciones. En el plano técnico, algunas características (cifrado, arquitecturas de información virtualizadas y distribuidas, etc.) dificultan o en ocasiones impiden el curso de las investigaciones criminales.

El encaje de este escenario con los diversos marcos legales nacionales y regionales plantea serias dificultades en la lucha internacional contra un número creciente de delitos que utilizan el ámbito digital para su consecución. Los medios técnicos y legislativos y las capacidades con que cuentan los cuerpos policiales y operadores judiciales requieren de una continua adaptación pareja al rápido proceso de digitalización de la sociedad.

El ARI analiza el acceso a información cifrada en el curso de investigaciones criminales, como las relacionadas con casos de abuso de menores en la red, y la evolución del marco legal para el acceso transnacional a datos en el curso de investigaciones criminales.

Análisis

La aproximación europea al cifrado: "La seguridad mediante cifrado y a pesar del cifrado"

El uso de cifrado en las aplicaciones de Internet se ha implantado por defecto para reforzar la protección de la privacidad y confidencialidad de las comunicaciones, en particular en la transferencia internacional de datos. Concebido para estos fines legítimos, también lo usa habitualmente la delincuencia, lo que dificulta significativamente la labor de las investigaciones policiales y judiciales en el acceso legal

a pruebas en plataformas de comunicación *online* –el impacto varía entre el 25% y el 100% de los casos, dependiendo del tipo de investigación[1]–.

La regulación europea es diversa[2] y también lo es la extracomunitaria. Algunos países, como Australia, Estados Unidos o India, han implementado o estudian soluciones legales. Australia, Canadá, Nueva Zelanda, el Reino Unido y los Estados Unidos emitieron una declaración conjunta en 2019 en la que solicitaban a las compañías tecnológicas que estudiaran incorporar en el diseño de sus productos y servicios la posibilidad de que los Gobiernos pudieran acceder, con autorización judicial, a la información cifrada en un formato legible y utilizable. También pidieron a la industria la búsqueda conjunta de fórmulas legales compatibles con el criterio de proporcionalidad. Las autoridades judiciales de los Estados Unidos han realizado duras declaraciones públicas sobre el elevado coste que implica el uso "indiscriminado" e "irresponsable" del cifrado respecto al crimen organizado y, en particular, el número de víctimas, acciones criminales y delitos que podrían haberse evitado. Abogan por establecer una legislación efectiva que proteja el acceso legal a las comunicaciones, cuestionando si el riesgo residual derivado de incorporar mecanismos legales para el acceso a comunicaciones cifradas es significativamente superior a las vulnerabilidades con que actualmente ya cuentan las aplicaciones de Internet[3]. Asimismo, llama la atención el diferente tratamiento regulatorio y obligaciones de colaboración de los operadores de telecomunicaciones en relación con la capacidad de los proveedores de Internet de impedir el acceso a pruebas electrónicas y establecer contramedidas de cifrado[4].

En octubre de 2020, el Departamento de Justicia de los Estados Unidos apeló a la colaboración del sector tecnológico para desarrollar por diseño soluciones técnicas, legales y operativas proporcionales y efectivas que permitan a las autoridades acceder a los contenidos ilegales y a las pruebas en formatos legibles (no cifrados). En una declaración sobre las implicaciones del cifrado de extremo a extremo (E2E) para la seguridad pública y el acceso a pruebas electrónicas en las aplicaciones de Internet, terminales móviles y servidores, el Departamento de Justicia subrayó que, "siendo el cifrado de vital importancia para la protección de la privacidad y la ciberseguridad, esto no debería ser a costa de obstaculizar por completo la actuación de las fuerzas de seguridad en la lucha contra la actividad ilegal en la red".

El Mando de Comunicaciones del Reino Unido (Government Communications Headquarters, GCHQ) estudia soluciones del tipo protocolo fantasma (*ghost protocol*), basadas en incorporar de forma oculta a agentes con autorización judicial a foros y grupos privados en redes sociales cifradas que estén siendo investigadas, solución que

[1] Nota de la Comisión 10730/20, sobre encriptación de extremo a extremo en las investigaciones criminales y judiciales, 18/09/2020, p. 3.

[2] El informe conjunto de Europol y EuroJust "Second observatory report on encryption", publicado el 18 de febrero de 2020, detalla el marco legal con el que cuentan algunos Estados miembros.

[3] Discurso del fiscal general de los EE. UU. William P. Barr en la International Conference on Cyber Security, Nueva York, 23/07/2019.

[4] Communications Assistance for Law Enforcement Act (CALEA Act): la ley establece para los operadores de telecomunicaciones de Estados Unidos la obligación de proporcionar acceso legal a las infraestructuras de comunicaciones a las autoridades judiciales y agencias de seguridad, teniendo que asumir los costes.

vulnera los mecanismos de autenticación de los usuarios para el acceso a las plataformas. Esta solución, si bien mantiene inalterado el mecanismo de cifrado, anula la confianza de los usuarios al vulnerar la confidencialidad y privacidad de la comunicación, por lo que ha sido criticado por las grandes plataformas de Internet en una carta abierta.

El Consejo de Europa[5] abordó en diciembre de 2016 en la cumbre de Justicia e Interior una línea de trabajo sobre los retos del cifrado en el ámbito de las investigaciones criminales y en junio de 2017 adoptó unas primeras conclusiones que otorgan a la industria la corresponsabilidad en la lucha contra el terrorismo y el cibercrimen, haciendo un llamamiento para solucionar situaciones en las que el cifrado E2E impide a las autoridades acceder a pruebas digitales.

En octubre de 2017, la Comisión Europea propuso medidas en apoyo de las autoridades policiales y judiciales para acceder a las pruebas electrónicas durante investigaciones transfronterizas junto al desarrollo de capacidades técnicas con el apoyo de Europol-EC3 para acceder a información cifrada en terminales y dispositivos de almacenamiento y a comunicaciones cifradas de extremo a extremo (E2E). Como resultado de la colaboración entre las autoridades policiales y judiciales y representantes del sector privado, la Comisión publicó sus conclusiones en la mencionada Nota 10730/20.

Según las conclusiones, no serían válidas las soluciones técnicas que debiliten o prohíban directa o indirectamente el uso de cifrado, porque el debilitamiento de una parte de un sistema cifrado podría debilitar el sistema en su conjunto, con efectos perjudiciales sobre los derechos a la privacidad y la protección de datos personales. Las órdenes de acceso a comunicaciones cifradas se dirigirán a un individuo o grupo en el marco de una investigación –quedan excluidos accesos masivos– y deben ser proporcionales y emitidas o estar sujetas a validación previa por una autoridad judicial. La transmisión de datos a las autoridades se hará con las medidas de seguridad más avanzadas en el cumplimiento de la protección de datos. Las técnicas que permitan el acceso a información cifrada han de utilizarse solo si no se cuenta con alternativas menos intrusivas *(encryption workarounds*). Dado el amplio espectro de soluciones de cifrado que pueden desplegarse simultáneamente en dispositivos o sistemas para proporcionar múltiples capas de protección, no debería haber una única solución técnica destinada a proporcionar acceso a los datos (principio de neutralidad tecnológica). Las empresas que incorporen el cifrado de productos deben contribuir a identificar las mejores soluciones en cada caso, ya que es indispensable contar con su colaboración y la del resto de la comunidad europea de la ciberseguridad.

La resolución del Consejo posterior de 2020 desarrolla esas conclusiones. Apoya plenamente el desarrollo, la aplicación y el uso del cifrado fuerte como medio necesario para la protección de los derechos fundamentales, la seguridad digital de los Gobiernos,

[5] El Consejo de Europa es una organización internacional con sede en Estrasburgo que tiene por objetivo principal la defensa, protección y promoción de los derechos humanos, en particular los civiles y políticos, la democracia y el Estado de Derecho. La institución engloba las 47 naciones europeas, con la sola excepción de Bielorrusia.

la industria y la sociedad[6]. Al mismo tiempo, el Consejo señala la necesidad de que la UE vele por que las autoridades en el ámbito de la seguridad y la Justicia penal puedan ejercer sus facultades garantizando el acceso a los datos. La resolución establece como punto de partida el principio de "la seguridad mediante el cifrado y a pesar del cifrado", principio que habrá de respetarse en su totalidad, es decir, aunar la protección de los derechos fundamentales, proteger la privacidad y la seguridad de las comunicaciones mediante el desarrollo de técnicas de cifrado robustas, con ofrecer la posibilidad de que las autoridades competentes en el ámbito de la seguridad y la Justicia penal accedan a datos y metadatos de forma legítima y selectiva –esto es, no masiva o indiscriminada–, preservando la ciberseguridad en la lucha contra la delincuencia organizada y el terrorismo mediante la aplicación de soluciones técnicas por definir.

El Consejo hace un llamamiento a la cooperación estrecha y la transparencia entre todos los actores implicados para plantear soluciones técnicas equilibradas y mejorar las capacidades técnicas y operativas de las autoridades policiales y judiciales[7]. Finalmente, es importante señalar que el Consejo no descarta evaluar próximamente la necesidad de un marco reglamentario común en la UE para la implantación de estos objetivos, con lo que deja abierto el debate sobre la regulación del cifrado.

El cifrado de aplicaciones en línea y la lucha contra el abuso de menores en la red

El COVID-19 ha provocado un significativo aumento del volumen de material de abuso sexual infantil intercambiado en la red, tal como informó Europol en junio de 2020, una realidad que se hallaba en niveles elevados antes de la pandemia –Europol calcula un aumento del 25% en algunos Estados miembros–. La intensa actividad mantenida en la *darknet*[8] con estos fines durante el confinamiento evidencia la existencia de organizaciones criminales con modelos de negocio en permanente evolución que constituyen una significativa amenaza para la infancia.

Las redes sociales y las aplicaciones de mensajería electrónica de uso común en Internet (por ejemplo, WhatsApp) incorporan por defecto mecanismos de cifrado E2E, entre los extremos de la comunicación, lo que las convierte en un medio de ocultación muy accesible y efectivo, habitualmente utilizado para el intercambio de material de abuso sexual infantil[9]. La función de autodestrucción de algunas de estas aplicaciones

[6] Resolución 13084/1/20, de 24 de noviembre, sobre seguridad mediante cifrado y a pesar del cifrado.

[7] Para fomentar esas capacidades, el Consejo acordó que parte de los fondos del Mecanismo de Recuperación y Resiliencia se utilizarán para garantizar el acceso policial y judicial y proporcionar un entorno de comunicación seguro, especialmente mediante cifrado cuántico. Conclusiones EUCO 13/20, de 2 de octubre, p. 4.

[8] Por *darknet* ('red oscura') se entiende las redes que se superponen al Internet público y que requieren de *software* específico y configuraciones o autorización para acceder y compartir información u otros contenidos digitales. Utilizan protocolos y puertos "no estándares" establecidos sobre la red subyacente (Internet). La *darknet* recurre a navegadores específicos para el acceso a contenidos no indexados por los motores de búsqueda habituales, como Bing o Google. La más conocida es TOR (The Onion Routing); existen otras de tipo *peer-to-peer* ('entre iguales') tales como Freenet, i2p, GNUnet, Entropy y ANts P2P.

[9] A finales de 2019, Facebook anunció la intención de implementar por defecto el cifrado de extremo a extremo en su servicio de mensajería instantánea. En ausencia de nuevas medidas técnicas (cont.)

de uso habitual hace que las investigaciones sean particularmente complicadas. Igualmente, aumenta el número de foros especializados creados en plataformas de la *darknet* que cuentan con unas reglas y jerarquía *ad hoc* orientadas a maximizar la ocultación de usuarios y contenidos. El material autogenerado se intercambia directamente con otros usuarios en comunidades o grupos, tras lo cual se distribuye a través de las redes sociales y, finalmente, termina en plataformas de contenidos de pornografía infantil en la *darknet*.

Vista la gravedad de la situación, la Comisión elaboró en julio de 2020 la Comunicación COM(2020)607, que establece la estrategia para 2020-2025 para abordar esta situación en línea y en el mundo físico reforzando los instrumentos jurídicos y operativos disponibles en la actualidad. En ella se afirma que "el uso de tecnología de cifrado con fines delictivos debe abordarse de inmediato mediante posibles soluciones que permitan a las empresas detectar y denunciar el abuso sexual infantil en las comunicaciones electrónicas cifradas de extremo a extremo". La estrategia para garantizar tanto la privacidad de las comunicaciones electrónicas como la protección de los niños contra el abuso y la explotación sexual se articula en cuatro puntos: mejorar la coordinación[10], reforzar la regulación disponible (Directiva 2011/93), potenciar la prevención y aumentar la respuesta policial.

En este sentido, la Comisión ha emplazado a un grupo de expertos de la industria bajo el paraguas del Foro de Internet de la UE con el objetivo de haber identificado y evaluado hacia finales de 2020 soluciones técnicas que permitan detectar e informar sobre contenidos y actividades de abuso sexual que utilicen canales de comunicación cifrados de extremo a extremo y señalar retos regulatorios y operacionales junto con oportunidades que surjan en la lucha contra estos delitos. La prensa ha tenido acceso a alguno de los borradores del estudio del Foro de Internet, el cual propone soluciones técnicas que facilitarían a los proveedores de aplicaciones y comunicaciones electrónicas la detección proactiva y denuncia de imágenes y vídeos[11]. Según la información conocida, las soluciones técnicas deben ser eficaces en la detección de contenidos; viables en términos de coste, tiempo y escalabilidad; respetuosas con la privacidad de las comunicaciones y la seguridad de otros usuarios distintos a los que intercambian contenidos de este tipo, y transparentes respecto a las medidas adoptadas.

El estudio apunta tres familias de soluciones técnicas –centradas en el terminal del usuario, el servidor del servicio y el cifrado (técnicas homomórficas)– y ofrece

complementarias, se calcula que esto podría reducir el número total de denuncias de abuso sexual infantil en la UE y en todo el mundo entre el 50% y el 67%, ya que las herramientas de detección utilizadas actualmente no serían válidas en comunicaciones cifradas de extremo a extremo.

[10] El Foro de Internet de la UE reúne desde 2015 a los ministros de Interior de los Estados miembros junto a representantes de alto nivel de las principales empresas de Internet, el Parlamento Europeo y Europol. Es un foro de colaboración intersectorial público-privada creado para la lucha contra contenidos de carácter terrorista en Internet cuyo alcance se ha ampliado en la actualidad a contenidos de abuso sexual de menores, aunque la identificación de esos contenidos exige una metodología distinta y es el único tipo de contenidos cuya sola posesión es ilegal *per se*.

[11] Danny O'Brien, "Orders from the Top: The EU's Timetable for Dismantling End-to-End Encryption", *Electronic Frontier Foundation (E3FF)*, 06/10/2020.

recomendaciones que son de aplicación inmediata, así como otras que requieren investigación e inversión a largo plazo, además de consideraciones técnicas tales como la necesidad de actualizar las tecnología PhotoDNA, la mejora de la calidad e integridad de las bases de datos de identificadores *hash*, la necesidad de desarrollar estándares para la detección de contenidos de abuso sexual infantil en la red o la conveniencia de utilizar soluciones abiertas sin que por ello se ofrezca una posibilidad de manipulación que reduzca su efectividad en los terminales. De hecho, las soluciones implantadas total o parcialmente en el terminal han de recurrir al principio de "seguridad por oscuridad" (*security by obscurity*), de forma que el usuario desconozca los pormenores de la implementación técnica para evitar su neutralización. Este tipo de soluciones basadas en el escaneo de contenidos en el dispositivo del usuario no está exento de polémica, ya que puede considerarse una puerta trasera que puede utilizarse para localizar conversaciones políticas mediante aplicaciones como WeChat en China.

Instrumentos políticos y normativos para el acceso transnacional a datos en procesos criminales

La delincuencia, el crimen organizado y las organizaciones terroristas hacen cada vez un mayor uso de la tecnología e Internet para planear y cometer delitos. Como consecuencia de ello, las autoridades necesitan recurrir en tiempo y forma a pruebas electrónicas. Actualmente se utilizan datos electrónicos en el 85% de las investigaciones penales; el 65% del total de las solicitudes se dirigen a proveedores con sede en otra jurisdicción.

Las pruebas electrónicas son informaciones en formato electrónico que se utilizan para investigar y enjuiciar delitos; algunos ejemplos son los contenidos y metadatos de las comunicaciones electrónicas, mensajes de correo electrónico, mensajes de texto, contenidos procedentes de aplicaciones de mensajería, contenidos audiovisuales, información sobre la actividad en línea del usuario, etc. Esta información puede utilizarse para identificar a una persona, anticipar la comisión de un delito u obtener más información sobre sus actividades. En particular, es de la máxima importancia establecer normas claras para el acceso transfronterizo a pruebas electrónicas en las investigaciones penales.

La Estrategia de la Unión de Seguridad para 2020-2025 constituye el marco estratégico en el que se integran todas las iniciativas políticas y las medidas normativas para la lucha contra la ciberdelincuencia. Incluye un sistema de alerta rápida y propone medidas para proteger a las víctimas del uso indebido de los datos o cualquier forma de usurpación de la identidad (Identidad Digital Europea[12]), regular la conservación de datos de acuerdo con el Tribunal de Justicia de la Unión Europea, crear instrumentos procesales innovadores y formar adecuadamente a los servidores de la ley. En el aspecto técnico se aborda el acceso a datos y retención de pruebas –incluidos los datos que circulen a través de las redes 5G–, la interoperabilidad de las nuevas tecnologías y el uso del cifrado respetando el equilibrio entre privacidad y seguridad. También se fomenta la colaboración entre órganos como la Unidad Conjunta de Intervención, el Foro de la UE sobre Internet, el Protocolo de crisis de la UE sobre terrorismo y extremismo

[12] Comunicación de 19 de febrero de 2020 "Configurar el futuro digital de Europa", COM(2020)67.

violento y el Grupo de Acción Conjunta contra la Ciberdelincuencia de Europol, entre muchos otros.

En el ámbito de la UE, la cooperación judicial cuenta con la Orden Europea de Investigación (EIO). Es una decisión judicial emitida o validada por la autoridad de un país de la UE en el curso de una investigación con el propósito de recopilar o utilizar pruebas en asuntos penales transfronterizos entre Estados miembros de la UE. Permite mantener una relación más directa, sencilla y rápida entre autoridades judiciales y está regulada por la Directiva relativa a la Orden Europea de Investigación en materia penal, aprobada en abril de 2014 y recogida en la Ley 3/2018, de 11 de junio. La colaboración judicial con terceros países cuenta con otros instrumentos, como el Acuerdo de Asistencia Judicial entre los Estados Unidos y la Unión Europea[13], que facilita la cooperación entre el sistema estadounidense y el europeo[14].

En el ámbito internacional, se está actualizando el Segundo Protocolo Adicional al Convenio de Budapest sobre la Ciberdelincuencia[15]. En septiembre de 2017, el Consejo de Europa inició la preparación de este protocolo adicional con el objetivo de mejorar el acceso transfronterizo a las pruebas electrónicas en las investigaciones penales. El Segundo Protocolo Adicional incorpora disposiciones para un régimen de asistencia judicial más eficiente, para la cooperación directa con los proveedores de servicios de terceros países que son partes en el Convenio y para el acceso remoto por las autoridades a servidores u ordenadores; un marco y salvaguardias multilaterales para ampliar las búsquedas a través de las fronteras, y garantías y requisitos exigentes en materia de protección de datos. Los Estados miembros acordaron en junio de 2019 otorgar a la Comisión el mandato para entablar negociaciones internacionales con vistas a haber acordado el Segundo Protocolo Adicional antes del término de 2020.

Propuesta legislativa e-Evidence

Más de la mitad de las investigaciones penales incluyen una solicitud transfronteriza para la obtención de pruebas electrónicas que obran en poder de prestadores de servicios con sede en otro Estado miembro o fuera de la UE; casi dos terceras partes de los delitos cuyas pruebas electrónicas se encuentran en otro país no pueden ser debidamente investigados o enjuiciados debido al tiempo necesario para recabar tales pruebas o a la fragmentación del marco jurídico. La cooperación público-privada entre

[13] Instrumento sobre la aplicación del Tratado de Asistencia Jurídica Mutua de 1990, de 26 de enero de 2010.

[14] Una ley de 2018 (Clarifying Lawful Overseas Use of Data Act, Cloud Act) obliga a los proveedores de EE. UU. a proporcionar acceso a los datos y metadatos en su posesión, custodia o control si son solicitados por las autoridades judiciales. Excluye el acceso a datos de ciudadanos estadounidenses en el país, a los cuales aplica los tratados de asistencia legal mutua.

[15] El Convenio de Budapest sobre Ciberdelincuencia es un acuerdo internacional destinado a combatir los ciberdelitos y delitos cometidos por medio de Internet. Aprobado en noviembre de 2001 y ratificado en el BOE el 17 de septiembre de 2010, busca establecer una legislación penal y procedimientos comunes entre los 65 países miembros del Consejo de Europa —no confundir con el Consejo Europeo— y los invitados a participar en él. El Primer Protocolo Adicional al convenio se dedicó a la penalización de actos de índole racista y xenófoba cometidos en la red y data de enero de 2003.

proveedores y autoridades resulta habitualmente ineficiente al no existir un marco legal para la cooperación voluntaria trasfronteriza.

El acceso a pruebas electrónicas en investigaciones transfronterizas en la UE llega a ser un proceso largo y complicado, dado que los proveedores de servicios en línea almacenan los datos de los usuarios en servidores que pueden hallarse en distintos países, tanto dentro como fuera de la UE. Por este motivo, la Comisión propuso en abril de 2018 dos nuevas normas:

- Un borrador de Reglamento sobre las órdenes europeas de entrega y conservación[16] de pruebas electrónicas a efectos de enjuiciamiento penal.

- Un borrador de Directiva por la que se establecen normas armonizadas para la designación de representantes legales a efectos de recabar pruebas para procesos penales, que obliga a los proveedores de servicios que no tengan sede o representación en la UE pero presten servicios en ella a nombrar a un representante legal responsable de la recepción y ejecución de las órdenes. El objetivo es garantizar que todos los proveedores de servicios que operen en la UE tengan las mismas obligaciones de acceso a las pruebas electrónicas[17].

Las propuestas obligarán a proveedores de servicios cuyo elemento definitorio sea el almacenamiento de datos, como proveedores de comunicaciones electrónicas, de comunicaciones por voz (VoIP), de *hosting* y similares (en la nube, CDN, etc.), de infraestructuras de Internet (registros de dominio y direcciones IP o servicios *proxy*), redes sociales y mercados digitales.

Las propuestas presentadas por la Comisión permitirán a las autoridades judiciales de un país de la UE solicitar directamente el acceso a pruebas electrónicas a cualquier proveedor que preste servicios y tenga sede o representación en otro Estado miembro. Esto agilizaría las solicitudes de acceso, ya que no sería necesario pasar por las autoridades del otro Estado miembro –la Comisión calcula que los plazos actuales son de 120 días con una orden de investigación europea y diez meses mediante un acuerdo de asistencia legal recíproca, que se reducirían a diez días o a seis horas en situaciones excepcionales–.

[16] Propuesta de Reglamento COM(2018)225, de 17 de abril, sobre las órdenes de entrega y preservación de pruebas electrónicas en materia penal. La orden de entrega permitirá que la autoridad judicial de un Estado miembro solicite acceso a pruebas electrónicas directamente a un proveedor de servicios con sede o representación en otro Estado miembro. El proveedor de servicios habrá de responder en un plazo de diez días, o de seis horas en caso de urgencia. La orden de conservación impedirá que el proveedor de servicios suprima pruebas electrónicas cuando todavía se esté tramitando la orden de entrega.

[17] Propuesta de Directiva COM(2018)226, de 17 de abril, para establecer normas armonizadas para la designación de representantes legales de los proveedores de servicios a efectos de recabar pruebas para procesos penales. El Consejo adoptó su posición el diciembre de 2018 en relación con la designación de representantes legales; propone hacer pública una lista completa de representantes legales para garantizar el acceso por parte de las autoridades policiales y judiciales a través de la Red Judicial Europea en materia penal. Los cuerpos policiales y autoridades judiciales tendrán la posibilidad de recurrir a los representantes legales designados en virtud de esta Directiva en procedimientos nacionales.

Las infografías de más abajo reflejan gráficamente la duración de los procedimientos actuales y su simplificación según el paquete e-Evidence, es decir, el Reglamento sobre las órdenes europeas de entrega y conservación y la Directiva para la designación de representantes legales:

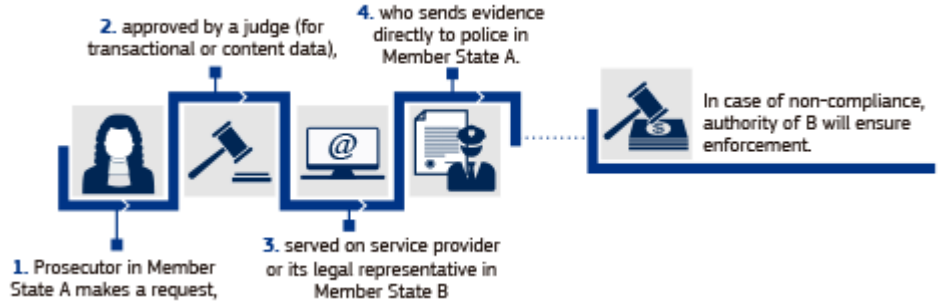
Situación actual: orden de investigación europea a un Estado miembro (arriba), solicitud a un tercer Estado con el que se ha suscrito un acuerdo de asistencia mutua (abajo)

Situación planteada por la propuesta legislativa e-Evidence: fases de una orden de producción europea.

Fuente: FAQ on New EU rules to obtain electronic evidence.

Fases actuales en una investigación que recurre al procedimiento de asistencia mutua (MLA) ante un ataque terrorista en el que el proveedor se encuentra en un país no comunitario.

Fases en aplicación de la propuesta e-Evidence al ejemplo anterior; también aplicarían si las pruebas electrónicas estuvieran almacenadas en un país no comunitario.



Fuente: EC Factsheet e-Evidence.

Actualmente, el borrador del reglamento y de la directiva se encuentran en discusión parlamentaria. A pesar de la urgencia demandada por las autoridades policiales y judiciales de los Estados para su aprobación, existe una fuerte polémica que cuestiona, entre otros aspectos, la necesidad de fijar unos plazos tan ajustados, la ausencia de autoridad judicial en el país al que se destina la orden –podría provocar la incertidumbre jurídica de los proveedores o la indefensión de los acusados– o dificultades de interoperabilidad jurídica en la fase de ejecución de las órdenes de producción entre países en razón de los diferentes marcos jurídicos nacionales.

Conclusiones

El acceso a pruebas digitales cifradas en el curso de investigaciones criminales constituye un punto de la Estrategia de la Unión de Seguridad para 2020-2025 de notable relevancia en virtud del creciente aumento de delitos que utilizan el ámbito digital de la red para su consecución.

En este sentido, es inevitable concluir, en breve, el debate sobre el acceso a pruebas electrónicas cifradas con la adopción de soluciones transnacionales técnicas y jurídicas que cuenten con la colaboración de la industria desde las fases iniciales del diseño de aplicaciones y productos. El uso de cifrado robusto para la protección de la privacidad y del secreto de las comunicaciones no debería impedir la actuación de las fuerzas de seguridad y operadores judiciales en la lucha contra la actividad ilegal en la red, en particular la detección de contenidos de abuso sexual infantil o de carácter terrorista en Internet. Es imprescindible potenciar un marco de colaboración público-privada de ámbito internacional que facilite a las fuerzas de seguridad y operadores judiciales el conocimiento técnico y la participación en la implantación de soluciones a corto plazo.

Las propuestas del paquete de medidas e-Evidence y el Segundo Protocolo Adicional al Convenio de Budapest sobre la Ciberdelincuencia son dos líneas de trabajo de la UE representativas del esfuerzo por adaptar a las exigencias de estos próximos años los actuales instrumentos legales para el acceso transnacional a pruebas electrónicas en la resolución de procesos criminales, un complejo reto jurídico y operativo.