SABER Y JUSTICIA
ESCUELA NACIONAL DE LA JUDICATURA
República Dominicana

LA COOPERACIÓN INTERNACIONAL EN MATERIA DE CIBERCRIMEN Y EVIDENCIA DIGITAL

International Cooperation on Cybercrime and Digital Evidence

Fernando A. Abreu Valencia
Poder Judicial de la República Dominicana
eabreu@poderjudicial.gob.do
linkedin.com/in/fernando-a-abreu-valencia-60077858/

Artículo de investigación
Recibido: 24 de marzo de 2022
Aprobado: 18 de mayo de 2022

Vol. 1, núm. 21, junio 2022
ISSN (impreso): 2305-2589
ISSN (en línea): 2676-0827
saberyjusticia@enj.org

RESUMEN

El ciberespacio se encuentra en constante amenaza y con este todo el sistema estatal y privado. El panorama se muestra mucho más complejo si le agregamos las características propias de este espacio virtual, dentro de los que se incluyen el anonimato de los infractores, la indeterminación geográfica de la comisión del delito, el tiempo y un sinnúmero de factores que además incluyen temas de soberanía y jurisdicción. En ausencia de una cooperación activa entre los Estados y la adopción de nuevas estrategias, el sistema de protección se encuentra destinado al fracaso. El cibercrimen ha desafiado la capacidad de su persecución de formas sin precedentes, lo cual demanda del aumento y la simplificación de la cooperación entre los Estados y particularmente del apoyo del sector privado, constituido especialmente por los proveedores de servicios.

PALABRAS CLAVES

Cibercrimen; cooperación internacional; evidencia digital; procedimiento.

ABSTRACT

Cyberspace is in constant threat and with it the entire state and private system. The problem is much more complex if we add the characteristics of this virtual space, which includes the anonymity of the offenders, the geographical indeterminacy of the commission of the crime, and a number of factors that also include topics involving sovereignty and jurisdiction. In the absence of active cooperation between States and the adoption of new strategies, the protection system is doomed to failure. Cybercrime has challenged the ability to prosecute it in unprecedented ways, which demands an increase and simplification of the cooperation system between States and the particular support of the private sector, especially the service providers.

KEYWORDS

Cybercrime; digital evidence; international cooperation; procedures.

Abreu Valencia, F. A. (2022). La cooperación internacional en materia de cibercrimen y evidencia digital. *Revista Saber y Justicia,* 1(21), 30-53. https://saberyjusticia.enj.org

INTRODUCCIÓN

Las interacciones humanas se han trasladado en gran medida a la esfera virtual, convirtiendo al ciberespacio en un medio imprescindible para llevar a cabo gran parte de nuestras actividades cotidianas (transacciones bancarias y comerciales, estudios, consultas médicas, etc.) ampliando y facilitando estas tareas que tradicionalmente realizábamos de manera presencial, pero como casi todo en la vida, lo positivo trae un costado negativo.

La enorme dependencia de las sociedades occidentales respecto a los sistemas informáticos y electrónicos está haciendo que estas sean más vulnerables a los posibles ataques cibernéticos y al fraude en la red. Internet es un medio de fácil acceso, donde cualquier persona, guardando su anonimato, puede realizar una acción difícil de asociar, virtualmente indetectable. Con esto, la red se está convirtiendo en ese lugar ideal para que los delincuentes y los terroristas lleven a cabo sus acciones y actividades (Sánchez Mederos, 2012).

En otras palabras, los delincuentes y terroristas también han trasladado sus actividades a la esfera virtual, lo que, sin dudas, ha cambiado las reglas del juego en cuanto a la persecución y judicialización de estas acciones se refiere. Las instituciones estatales, diseñadas para proteger la seguridad nacional, limitadas por naturaleza al marco de su propia jurisdicción, se enfrentan al enorme reto de proveer respuestas eficaces a una industria del crimen que crece de manera exponencial, en un escenario predominantemente transnacional, que esencialmente requiere de una cooperación internacional activa, tanto a nivel de los Estados como del sector privado, constituido principalmente por las empresas proveedoras de servicios de internet, en aras de alcanzar los objetivos de prevención, persecución y sanción efectiva de este tipo de delitos.

La transformación digital abre enormes oportunidades al desarrollo socioeconómico, pero al mismo tiempo incorpora amenazas y riesgos nuevos y desconocidos para los que debemos prepararnos. El cibercrimen no tiene fronteras físicas y en este entorno cobra cada día más importancia la cooperación internacional para la prevención de las amenazas y la persecución de los ciberdelincuentes (Artigas, 2022).

LA COOPERACIÓN INTERNACIONAL EN MATERIA DE CIBERCRIMEN – HACIA UN CAMBIO DE PARADIGMA

El concepto que tradicionalmente se ha manejado en torno a la cooperación internacional se fundamenta, de manera esencial, en la necesidad de abolir los hechos criminales y actos fraudulentos que se suscitan a raíz de las interacciones sociales y económicas entre los miembros de una comunidad internacional, formada por grupos humanos y personas morales localizadas en diferentes territorios, enmarcados en soberanías legislativas y judiciales diferentes, claramente determinadas, así como en la necesidad de combatir la impunidad de quienes cometen o realizan tales hechos o actos.

La cooperación internacional es absolutamente imprescindible y se halla materializada en un conjunto de normas reguladoras de origen preferentemente convencional. El derecho interno tiende a facilitar la asistencia, de forma discrecional, atendiendo a principios de cortesía internacional o, más propiamente, de cooperación, utilizando con cierta frecuencia criterios de reciprocidad (Fernández y Sánchez, 2012).

Una de las características principales que enmarcan este concepto tradicional de cooperación internacional es el hecho de que, al menos en la mayoría de los casos, los elementos que conforman o derivan de tales hechos o actos se encuentran básicamente identificados en todo o en gran parte, especialmente a través de evidencias tangibles como es el caso de las armas, huellas, documentos físicos, así como de la relativa facilidad con que pueden obtenerse declaraciones testimoniales sobre algún hecho en concreto, cuestiones que históricamente han permitido identificar con bastante precisión el lugar de la ocurrencia del hecho, la identidad y la correspondiente nacionalidad o domicilio de quien o quienes lo hayan perpetrado.

Si bien, desde la óptica del cibercrimen, la esencia de la cooperación internacional ha mantenido su fundamento primigenio, es notorio que en términos materiales el asunto es mucho más complejo, pues además de enfrentarnos a los tradicionales obstáculos legislativos y judiciales que conlleva toda relación transfronteriza, nos estamos enfrentando a otras dificultades de carácter material, dentro de las que se encuentran la propia vinculación o asimilación de la prueba a uno o varios territorios y a una o varias personas determinadas, así como dificultades de carácter técnico como son la volatilidad, la fragilidad, el volumen y la segmentación de la evidencia, entre muchas otras de diversa naturaleza, y todo esto dentro de este espacio intangible

al que llamamos ciberespacio, cuestiones que de no ser por la colaboración internacional entre los Estados y las que resultan de las interacciones entre los Estados y el sector privado, especialmente con los llamados proveedores de servicios, fueran prácticamente imposible de resolver.

Es en este mismo sentido, que la Organización de las Naciones Unidas, a través de su oficina contra las drogas y el delito (UNODC) ha señalado que son varios los problemas que se plantean en relación con la reunión y utilización de pruebas electrónicas (también conocidas como pruebas o evidencias digitales) en las actuaciones penales:

> Antes de que se puedan presentar como pruebas ante un tribunal de justicia, hay que determinar su autenticidad e integridad examinando los procesos, los métodos y las herramientas utilizadas en la reunión, la adquisición, la conservación y el análisis de las pruebas electrónicas. El volumen, la volatilidad, la velocidad y la fragilidad de los datos son obstáculos para presentar los datos como pruebas en los tribunales. Además, dada la naturaleza transfronteriza de la ciberdelincuencia organizada y los diferentes ordenamientos jurídicos en todo el mundo, las reglas de prueba varían según los países. Esta variación supone un obstáculo para la reunión, la solicitud y la utilización de estas pruebas electrónicas en los tribunales nacionales. También varían entre los países las condiciones y las garantías para la obtención y el uso de pruebas electrónicas en los tribunales de justicia, de manera que se respeten el Estado de derecho y los derechos humanos (UNODC, 2022).

Es importante señalar también, que acorde a datos estadísticos recientes presentados por esta misma organización, el uso de internet está creciendo de manera exponencial, con más de 3.8 billones de usuarios en todo el mundo, lo que representa casi el 47% de la población mundial. Se estima que los usuarios pasarán cinco años de su vida en las redes sociales, que el costo del delito cibernético podría alcanzar los 2.1 billones de dólares a nivel mundial en los próximos años, que más del 80% de los actos delictivos cibernéticos se originan de alguna forma en relación con mercados negros en línea, infección de computadoras y recolección de datos personales y financieros. “Los terroristas utilizan las redes sociales, entre otras cosas, para difundir propaganda, recaudar fondos, reclutar y compartir información. Esta evidencia electrónica puede ser importante para mostrar dónde se encuentra un sospechoso, con quién se está asociando y qué está comunicando” (UNODC, 2018).

La Unión Europea, a través de una encuesta reciente, nos ha arrojado también la información de que más de la mitad de las investigaciones incluyen una solicitud de acceso transfronterizo a pruebas electrónicas, las pruebas electrónicas son relevantes en aproximadamente el 85% del total de investigaciones criminales y que, en casi dos tercios (65%) de las investigaciones en las que las pruebas electrónicas son relevantes, se necesita realizar una solicitud a entidades oficiales o privadas con base en otra jurisdicción. Igualmente, ha revelado este estudio, que el sistema actual de cooperación internacional o asistencia legal mutua (MLA, por sus siglas en inglés) ha resultado ser complejo y en algunos Estados burocrático, a menudo resultando en largas demoras en la obtención de pruebas electrónicas, lo cual colide con la naturaleza rápida de la delincuencia cibernética (Consejo de Europa, 2022).

En base a lo anterior, es imprescindible estar conscientes de que la idea tradicional de la cooperación internacional, basada en la colaboración de los distintos Estados con respecto a la realización de diligencias procesales y de campo tendentes a procurar la obtención de algún medio de prueba material, testimonial o inmovilizar algún bien determinado relacionado con un hecho criminal, llevado a cabo parcialmente en algún espacio físico de su territorio o por alguno de sus nacionales, con efecto en otro u otros países, en la actualidad ha adquirido un nuevo matiz, mucho más complejo e indeterminado, lo cual amerita, de manera urgente, que todos los actores que interactúan con el sistema de justicia posean un conocimiento práctico sobre las diferentes opciones de cooperación internacional que se encuentran actualmente vigentes en materia de cibercrimen y evidencia digital, así como de los proyectos encaminados a su actualización y armonización, en procura de proveer y recibir el auxilio requerido de una manera más eficaz y eficiente.

LA COOPERACIÓN ENTRE ESTADOS DENTRO DEL MARCO DEL CONVENIO DE BUDAPEST

El Convenio sobre Ciberdelincuencia (2001) mejor conocido como Convenio de Budapest (STE 185) constituye el primer y único instrumento internacional en la referida materia, elaborado por el Consejo de Europa, con la participación de Canadá, Estados Unidos, Japón y Sudáfrica, abierto en Budapest, Hungría, en noviembre de 2001, y del cual la República Dominicana es actualmente signataria, conjuntamente con otros 64 Estados parte y 12 Estados observadores.

Este tratado internacional es de naturaleza vinculante, esencialmente penal, cuyo objetivo esencial ha sido armonizar las distintas legislaciones de los Estados parte, en procura de aplicar una política criminal común que permita facilitar y agilizar la persecución de los delitos cometidos en contra de sistemas o medios informáticos, o mediante el uso de los mismos, así como facilitar la cooperación internacional entre estos Estados miembros con la finalidad de proteger a la sociedad frente a la ciberdelincuencia.

El Convenio de Budapest, en esencia, tiene como propósito principal armonizar los derechos, que los sistemas sean los más similares posibles, que tengan todos los regímenes un mínimo que sea compartido por todos, para así facilitar la comprensión y agilidad de los procesos (Verdhello, 2020).

De lo anterior, puede deducirse claramente que el Convenio de Budapest no es simplemente un convenio de cooperación internacional en materia de cibercrimen, su contenido abarca mucho más; pues como hemos señalado, se incluyen aspectos tendentes al establecimiento de una "política penal común" la cual, en menor o mayor medida, toca aspectos relacionados con el derecho interno de cada uno de los Estados parte, tanto en lo referente al derecho penal objetivo (ius poenale) como al derecho penal subjetivo (ius puniendi) el primero relacionado con la definición de determinadas acciones como crímenes o delitos y la determinación de su correspondiente pena y el segundo relacionado con la facultad punitiva del Estado para imponer estas penas a todo aquél que cometa la referida acción, siendo algunos de estos aspectos objeto de más de una controversia por temas ligados a soberanía, orden público interno e internacional, derechos humanos y costumbres, entre otros aspectos, independientemente de la relativa "flexibilidad" de sus textos para ajustarse a las características del sistema normativo de cada Estado en particular.

El convenio sobre cibercriminalidad reserva su capítulo III al tema de la cooperación internacional, señalando en su artículo 23 lo siguiente:

> Los Estados firmantes cooperarán con arreglo a lo dispuesto en el presente capítulo, aplicando para ello los instrumentos internacionales relativos a la cooperación internacional en materia penal, acuerdos basados en la legislación uniforme o recíproca y en su propio derecho nacional, de la forma más amplia posible, con la finalidad de investigar los procedimientos concernientes a infracciones penales vinculadas a sistemas y datos informáticos o para recoger pruebas electrónicas de una infracción penal (Budapest, 2001).

De manera general, los artículos del 25 al 28 del referido texto normativo son los que establecen las pautas para la cooperación y asistencia mutua entre los Estados para llevar a cabo las investigaciones y recolección de evidencias. En esencia, como aspectos más relevantes de estos artículos, se establece que los Estados firmantes deberán ofrecer su colaboración, en la forma más amplia posible, con el objeto de facilitar la investigación de los hechos penales vinculados a sistemas y datos informáticos, así como con respecto a la recolección de las pruebas electrónicas vinculadas a tales hechos.

Se establece que, en caso de emergencia, los Estados firmantes podrán formular su solicitud de colaboración a través de medios de comunicación electrónicos, siempre que ofrezcan las condiciones suficientes de seguridad y autenticidad, pudiendo el Estado requerido responder a través de los mismos medios. Mientras que los artículos del 29 al 34, pertenecientes a la sección 2 del referido capítulo III, establecen las pautas especiales para la asistencia mutua en materia de medidas provisionales, como son la conservación rápida de datos informáticos almacenados y la rápida revelación de estos, así como la asistencia para la obtención en tiempo real de datos relativos al tráfico de comunicaciones específicas e interceptación de datos relativos al contenido de estas comunicaciones transmitidas a través de un medio informático.

De manera particular, quisiéramos referirnos a lo dispuesto por el numeral 4 del artículo 25 el cual señala que “salvo disposición en contrario expresamente prevista en el presente capítulo, la colaboración estará sometida a las condiciones fijadas en el derecho interno del Estado requerido o en los tratados de colaboración aplicables y (el Estado requirente) comprenderá los motivos por los que el Estado requerido puede negarse a colaborar” (Budapest, 2001).

De una lectura rápida e irreflexiva de la referida disposición, muy probablemente nos llegaría a la mente que el convenio se ha colocado en el plano de una textura peligrosamente abierta, situando en aparente desequilibrio la condición de reciprocidad que debe primar entre los Estados signatarios de la misma, lo cual de alguna manera no deja de tener algo de cierto, sin embargo, esto encuentra su razón de ser en la naturaleza primigenia de la cooperación internacional, pues si bien esta figura se ajusta regularmente a los criterios de reciprocidad, en esencia mantiene su carácter de cortesía y discrecionalidad, sobre todo en los puntos en que no existe un compromiso concreto, expresamente plasmado en un texto vinculante, especialmente cuando lo solicitado pudiere afectar directa o indirectamente al orden público interno de este Estado requerido.

Por otra parte, y con la finalidad implícita de reducir los conflictos por las negativas de colaboración de un Estado ante algún requerimiento en particular, especialmente en ausencia de un compromiso concreto y vinculante, el propio convenio nos remite en el numeral 5 del referido artículo 25 a la verificación de la llamada doble incriminación, autorizando al Estado requerido a supeditar su colaboración a los casos en que el hecho constitutivo de la infracción, sobre el cual se requiera la colaboración, sea también considerado en su derecho interno como infracción penal, poco importa que no se encuadre en la misma categoría o que sea designado con la misma terminología.

Es en este mismo sentido que resulta esencial la cuestión de conocer no solamente el sistema normativo del Estado al cual se realiza el requerimiento sino también su cultura jurídica y hasta sus costumbres, pues lo que es legal y generalmente aceptado en el Estado requirente puede ser totalmente inaceptable y contrario a las normas y al orden público interno del Estado requerido y viceversa, en ocasiones pudiera incluso resultar contrario al orden público internacional. En otras palabras, no basta simplemente con verificar la existencia o no de un tratado, o si el mismo ha sido ratificado o no, se hace imperativo también verificar que la solicitud sea compatible con las normas internas y el orden público del Estado requerido, así como el orden público internacional.

Hay situaciones que se presentan en la cooperación que tienen que ver con la penalización o no de tal o cual delito en un país determinado, tenemos por ejemplo que la pornografía infantil es considerada como delito por una gran cantidad de países, sin embargo, en Cuba, por ejemplo, no es considerada como tal, entonces tenemos que si un país le pide a Cuba cooperación internacional con relación a un delito de pornografía infantil es posible que este le conteste que no puede ayudarlo porque eso no es un delito en su legislación interna (Verdhello, 2020).

Dentro de los compromisos que el Convenio de Budapest establece como vinculantes, sobre los cuales el Estado requerido no podrá rehusar su colaboración, so pena de comprometer su responsabilidad internacional, se encuentran los establecidos en los artículos del 2 al 11 del referido texto normativo, cuyo contenido se refieren a infracciones relacionadas con acceso ilícito, interceptación ilícita, ataques a la integridad de los datos, ataques a la integridad del sistema, abuso de los dispositivos, falsificación informática, fraude informático, pornografía infantil, infracciones de la propiedad intelectual y derechos afines, así como las tentativas de cometer estos delitos.

Es importante agregar que, independientemente de las consideraciones anteriores, el convenio ha establecido en su artículo 27.o algunas reservas especiales, ante cuya solicitud los Estados requeridos pueden denegar su asistencia, dentro de estas se enmarcan los requerimientos vinculados con asuntos políticos y aquellos que puedan poner igualmente en riesgo su soberanía y seguridad.

Ha sido igualmente prevista la posibilidad de aplazamiento de la prestación de la asistencia en los casos en que esta pueda perjudicar investigaciones o procedimientos que se encuentren en curso por las autoridades nacionales, evidentemente que haciendo constar los motivos y no sin antes verificar con el Estado requirente si la colaboración puede ser otorgada de manera parcial o bajo ciertas reservas. Se establece igualmente, de manera especial, la posibilidad de que el Estado requirente pueda solicitar al Estado requerido que la propia existencia y objeto de la demanda sea mantenida en total o parcial confidencialidad.

En lo que se refiere a los procedimientos de tramitación de las solicitudes de cooperación, el Convenio de Budapest remite a los protocolos y canales tradicionales de cooperación internacional, es decir, a través de las autoridades centrales de política exterior, como son los ministerios de relaciones exteriores, conocidos en algunos países como cancillería, o cualquier otra entidad equivalente. No obstante, y en vista de la propia naturaleza de los delitos vinculados a sistemas y datos informáticos, así como la vulnerabilidad de las pruebas electrónicas vinculadas a tales hechos, el convenio ha establecido ciertos protocolos para los casos considerados de urgencia.

En los casos considerados de urgencia, el Estado requirente podrá dirigir directamente a las autoridades homólogas del Estado requerido las solicitudes de asistencia, con el compromiso de remitir simultáneamente una copia de tal solicitud a la autoridad central del Estado requerido con el visado de la autoridad central del Estado requirente, estableciendo de manera especial que todas las demandas o comunicaciones formuladas al amparo de estas disposiciones podrán ser tramitadas a través de la Organización Internacional de la Policía Criminal (INTERPOL).

En adición a lo anterior, el artículo 35 del convenio insta a los Estados a establecer un punto de contacto disponible las veinticuatro horas del día, los siete días de la semana, la llamada Red 24/7, con el objeto de garantizar la

asistencia inmediata con relación a las investigaciones o procedimientos relacionados con el cibercrimen.

PROTOCOLO ADICIONAL AL CONVENIO SOBRE LA CIBERDELINCUENCIA RELATIVO A LA PENALIZACIÓN DE ACTOS DE ÍNDOLE RACISTA Y XENÓFOBA COMETIDOS POR MEDIO DE SISTEMAS INFORMÁTICOS

El 28 de enero de 2003 fue adoptado en Estrasburgo el Protocolo adicional al convenio sobre la ciberdelincuencia relativo a la penalización de actos de índole racista y xenófoba cometidos por medio de sistemas informáticos (STE 189) (Consejo de Europa, 2003) este viene a complementar el Convenio sobre la Ciberdelincuencia (Budapest, 2001) especialmente en los aspectos de cooperación internacional y asistencia mutua en la persecución y penalización de la propaganda de índole racista y xenófoba difundida a través de sistemas informáticos. El artículo 2 de este protocolo adicional define como material racista y xenófobo lo siguiente:

> Todo material escrito, toda imagen o cualquier otra representación de ideas o teorías, que propugne, promueva o incite al odio, la discriminación o la violencia, contra cualquier persona o grupo de personas, por razón de la raza, el color, la ascendencia o el origen nacional o étnico, así como de la religión, en la medida en que ésta se utilice como pretexto para cualquiera de esos factores" (Consejo de Europa, 2003).

En lo que se refiere a los aspectos de armonización legislativa y cooperación internacional de este protocolo adicional, básicamente podemos observar que el mismo hace extensiva la aplicación de las medidas y procesos establecidos en el convenio base, pues en su capítulo III, artículo 8, numerales 1 y 2, expresa textualmente que los artículos 1, 12, 13, 22, 41, 44, 45 y 46 del convenio se aplicarán, mutatis mutandis, al presente Protocolo. Las partes harán extensivo el ámbito de aplicación de las medidas definidas en los artículos 14 al 21 y en los artículos 23 al 35 del convenio a los artículos 2.o al 7.o del presente protocolo, razón por la cual no resulta necesario detenernos a analizar estos aspectos con relación a este protocolo adicional.

SEGUNDO PROTOCOLO DEL CONVENIO DE BUDAPEST

El Convenio de Budapest finalmente ha abierto a la firma su segundo protocolo de actualización y reforzamiento en materia de cibercrimen y evidencia digital. Este protocolo, preparado por el Comité de la Convención sobre Ciberdelincuencia (T-CY, por sus siglas en inglés) se encontraba en etapa de redacción y discusión desde el mes de septiembre de 2017 y tenía prevista

su apertura para la firma el mes de diciembre de 2020, lamentablemente, por efectos de la pandemia del COVID 19, se retrasó un poco su apertura, viendo la luz recientemente en este mes de mayo del presente año 2022 en un acto realizado en la sede del Consejo de Europa en Estrasburgo en cuya ceremonia suscribieron el documento 22 países miembros.

La razón de ser de este segundo protocolo se fundamenta en el aumento vertiginoso de la cantidad de delitos cibernéticos, de la cantidad de dispositivos con tecnologías mucho más avanzadas a las existentes en el momento en que fue puesto en funcionamiento el convenio base y con esto el aumento exponencial de usuarios y víctimas, enfrentándonos hoy día a nuevos sistemas, como es el caso de la computación en la nube, lo cual acarrea nuevos retos en materia de territorialidad y jurisdicción. Cuestiones como ¿Dónde está siendo cometido el delito?, ¿dónde están las pruebas?, ¿Quién tiene la evidencia?, ¿Qué régimen legal es aplicable para solicitar o divulgar datos?, toman todavía matices más intrincados.

Este nuevo protocolo pretende aportar soluciones más eficientes en lo que se refiere a la obtención de información sobre suscriptores, las cuales se sitúan actualmente en más de 170,000 solicitudes al año, procurando una cooperación más directa en la relación Estado / proveedores de servicios para facilitar las informaciones de registro de nombres de dominio, obtener datos almacenados y contenido relevante en una situación de emergencia, así como hacer frente a situaciones como la obligatoriedad de los proveedores de responder a las solicitudes legales y el manejo de la confidencialidad de estas, entre otras cuestiones relevantes, lo anterior con el objetivo de que la asistencia mutua sea más eficaz, conciliando estas medidas eficientes y efectivas con el Estado de derecho y los requisitos de protección de datos, dentro del marco de normas más claras y estables (Seger, 2020).

En lo referente a la obtención de información o evidencias, el segundo protocolo intenta sentar las bases y proveer procedimientos para una cooperación directa entre las autoridades de un Estado y un proveedor de servicios ubicado en el territorio de otro Estado, exclusivamente dentro del marco de una investigación criminal o procedimiento y solo respecto a información almacenada que sea relevante para la referida investigación o procedimiento (Albani, 2020).

En este sentido, se plantea dotar de poderes especiales a las autoridades competentes de un Estado a los fines de emitir una orden o solicitud a un proveedor

de servicio localizado en otro Estado, obligar a los Estados parte a adoptar todas las medidas necesarias para que estos proveedores de servicio puedan responder de manera eficaz y eficiente a estos requerimientos, estableciendo un límite de tiempo para responder a tales solicitudes, estandarizar el formato de los requerimientos y los mecanismos de trámite, así como establecer las pautas para la denegación de estas, entre otros aspectos relevantes.

De manera especial, en situaciones de emergencia, el segundo protocolo tiene dentro de sus propósitos proveer un procedimiento expedito, limitado a las solicitudes de emergencia en las cuales exista un riesgo significativo e inminente hacia la vida o la integridad de cualquier persona física, esto requiere que la parte solicitante describa detalladamente los hechos que demuestran o le hacen suponer que la emergencia es real y cómo la asistencia solicitada se relaciona con tal emergencia, quedando igualmente la parte solicitante en la obligación de presentar evidencias adicionales en caso de que le sea requerida. A estos fines, el segundo protocolo procura reforzar la red 24/7, dotándole de mayor flexibilidad respecto a los canales de transmisión y los protocolos de respuesta.

Como novedad de este protocolo se establece la armonización de procedimientos para la utilización de videoconferencias a los fines de recoger las declaraciones de testigos expertos, sospechosos o personas acusadas en el lugar que el Estado requerido permita la audiencia. Igualmente, se plantea el uso de esta tecnología con otros propósitos relacionados, incluyendo la identificación de personas u objetos.

En conclusión, la Convención de Budapest, con su nuevo protocolo, pretende ajustarse a los más altos estándares y necesidades del cibercrimen como un instrumento especializado de justicia criminal internacional con el objetivo de proveer mecanismos operacionales y de asistencia mutua que permitan investigar y asegurar las evidencias electrónicas de manera eficaz y eficiente, dentro de un marco legal que a la vez garantice la protección individual y los derechos en el ciberespacio.

Para alcanzar el consenso internacional respecto a un sistema de cooperación internacional, con el objetivo de hacer que la libertad en internet sea compatible con la necesidad de proveer a la justicia criminal con las herramientas adecuadas para la persecución del cibercrimen y la recolección de evidencias digitales, en un ambiente de respeto a los derechos humanos, las políticas internacionales a estos fines deben ser consideradas como prioridad (Salt, 2020).

COOPERACIÓN ENTRE LOS ESTADOS Y EL SECTOR PRIVADO

Históricamente, cuando hemos hablado de cooperación internacional, lo hemos hecho enfocados en la interacción entre los diferentes Estados para tratar de perseguir los hechos criminales y actos fraudulentos cometidos por personas, físicas o morales, pertenecientes a diferentes soberanías o cuando sus actos o efectos, de alguna manera u otra, se encontraban relacionados a un territorio extranjero; lo anterior basado en los principios tradicionales de solidaridad, cooperación y reciprocidad entre los Estados que conforman la llamada comunidad internacional.

Hoy la historia toma un rumbo diferente, incluso cuestionando en ocasiones la intervención excesiva del aparato Estatal en ciertas diligencias con carácter transfronterizo, especialmente las que requieren de acciones expeditas, como es el caso de los hechos penales vinculados a sistemas y datos informáticos, a los que hemos denominado cibercrimen. Es en este punto donde se plantea la integración directa de una tercera fuerza, a la que llamaremos el sector privado, conformado de manera especial por los “prestadores de servicios” tal como han sido denominados en el Convenio de Budapest.

Desde esta óptica, no ha de sorprender que se formulen una serie de cuestionamientos de resistencia en torno a la participación de estos actores no estatales y la legalidad de sus actuaciones, incluso respecto a la legalidad misma de la evidencia digital obtenida mediante la cooperación directa de estos prestadores de servicio, pues no debemos olvidar que hemos sido tradicionalmente parte de un sistema controlado, en principio, por los actores estatales y su recalcitrante concepto de supremacía de las instituciones.

Para poder asimilar estos cambios y validar cada vez más la importantísima colaboración del sector privado en los temas de cooperación en materia de cibercrimen, hay que situarse en la propia perspectiva de la evolución social y su proyección globalizada, especialmente mediante el uso de las tecnologías de información y comunicación.

Hace veinte años, por ejemplo, en el ambiente jurídico casi nadie hablaba de delitos informáticos o cibercrimen y de repente estos conceptos son mencionados a diario por todos los estamentos, a nivel estatal o privado, prácticamente como si se tratara de una tendencia de moda. La necesidad imperiosa de interactuar con el sector que maneja precisamente estas tecnologías, a los fines de prevenir, perseguir y obtener las evidencias de un hecho criminal realizado en esta esfera

virtual, es hoy día una realidad innegable, lo que nos obliga a reconocer su importancia y a valorar su colaboración.

Tal como los terroristas y el crimen organizado han aumentado sus actividades en el internet, medios sociales y aplicaciones con mensajes encriptados para ejecutar sus planes criminales, asegurar la evidencia desde los proveedores de estos servicios es vital. La evidencia electrónica (e-evidence) almacenada por estos proveedores de servicio pueden probar donde ha sido cometido tal crimen, mostrar las comunicaciones incriminatorias y determinar la ubicación de los agresores. Obtener estas evidencias digitales pueden asegurar que la persona indicada sea efectivamente perseguida, procesada y aquellos que perpetraron tales hechos criminales sean llevados a la justicia (UNODC, 2022).

Hoy día confluyen en la investigación del delito informático tanto los propios Estados a través de sus órganos judiciales y de seguridad como los actores privados que prestan servicios relacionados con internet y que, por sus características, trascienden fronteras y jurisdicciones. En suma, circundando a la asistencia judicial clásica, se van sucediendo colaboraciones y entrecruzamiento de información para la investigación criminal provista a los órganos judiciales, sin distinción de nacionalidad, por parte de las prestadoras de servicios en internet (ESP) y de las prestadoras del servicio de internet (ISP). (Deluca y del Carril, 2017).

En cuanto al marco legal en que se desarrollan las interacciones de cooperación entre los Estados requirentes y estos prestadores de servicios, nos siguen ilustrando estos autores cuando señalan que:

> Esta virtual asistencia internacional no se rige, como es obvio, por los convenios internacionales, sino que se va construyendo a partir de manuales de buenas prácticas, guías de acción para fuerzas de la ley (Law Enforcement Guidelines) propuestas por las compañías de internet a partir de la propia interpretación de las normas locales que las obligan e, incluso, por relaciones interpersonales que generan vínculos de confianza entre las empresas y las instituciones (Deluca y del Carril, 2017).

Esta cooperación, calificada por los autores recién citados como “caótica” y llevada a cabo dentro del marco de buena voluntad no deja de tener sus obstáculos:

> La información de estos proveedores está en todas partes del mundo, puede ser que una información se encuentre almacenada en México o en Guatemala

> o en Estados Unidos. Puede que una persona llame a Estados Unidos a pedir información y le digan que la información está en Suecia o que esta persona llame a Suecia y le informen que la clave para acceder a esa información la tienen en los Estados Unidos (Verdhello, 2020).

Incluso pudiera ser que esta información se encuentra segmentada, por ejemplo, que sea requerida a una empresa prestadora de servicios con sede central en los Estados Unidos y las evidencias se encuentren almacenadas una parte en un servidor de Francia y la otra en China, solo para dar un ejemplo.

Normalmente, cuando se realizaba alguna búsqueda de información relacionada a un delito pues simplemente se buscaba en los archivos de la computadora; ya con la evolución, la mayor parte de esta información puede que se encuentre en archivos fuera de la computadora, en la llamada nube, que básicamente consiste en alojar datos remotamente, en diversos servidores que se encuentran en varias partes del mundo y se mueven aleatoriamente, en la mayoría de los casos las personas e incluso los proveedores de servicio ni siquiera saben en qué país puede estar alojado el servidor que contiene sus datos (Azzolin, 2020).

Entonces se presentan cuestiones de difícil solución, tanto a nivel técnico como de jurisdicción competente, lo que a menudo culmina con el fracaso de la investigación, es en este sentido que se requiere de un inmediato reforzamiento y armonización en las normativas que regulen estos procesos, pues el propio concepto de "el lugar donde esté alojada la evidencia" carece ya de sentido.

Azzolin sugiere un cambio de paradigma, cambiar el concepto del "lugar de la evidencia" por el de "quién tiene el control de los datos", cuestiones que son ya tomadas en cuenta en el contenido del segundo protocolo de Budapest, mientras tanto podíamos ir observando una muestra de este cambio de paradigma a través de la promulgación en los Estados Unidos de la ley denominada *"cloud back"* que en una de sus disposiciones establece que "a partir de ahora, las órdenes judiciales de los jueces americanos dirigidos a las empresas norteamericanas sirven para la información que estas empresas tienen almacenadas tanto en los Estados Unidos como en territorios extranjeros", es en este sentido que Azzolin nos sigue diciendo: "No importa donde Google mande su información (a Finlandia, a Suecia o al espacio) lo importante es saber dónde está Google a los fines de solicitarle al juez competente de donde se encuentre Google para obtener esta información".

LA COOPERACIÓN INTERNACIONAL DESDE LA PLATAFORMA DEL GRUPO META

Acorde a Rick Cavalieros, Law Enforcement Outreach Manager (trad. Gerente de enlace con las autoridades de la ley) del grupo META, anteriormente conocido como grupo Facebook, la empresa META y sus empresas filiales como Instagram y WhatsApp, cuentan con herramientas para que las autoridades policiales e investigativas puedan solicitar información sobre los perfiles y datos contenidos en las páginas de Facebook o cuentas de Instagram, o en el caso de WhatsApp, datos relativos a sus suscriptores, expresando que la empresa tiene dos portales separados, uno para solicitar información de las cuentas de Facebook e Instagram y otro portal para WhatsApp.

Preservar una cuenta, por lo menos a través de Facebook o de WhatsApp, puede hacerse en unos treinta segundos, como mucho. Anteriormente había que hacerlo a través de una solicitud, por lo menos en los Estados Unidos, al departamento de justicia, esto pasaba a una unidad de análisis y posteriormente enviaban la orden de preservación; todo eso llevaba bastante tiempo y el tiempo en estos procesos es muy importante porque en cuestión de segundos se puede perder toda información, especialmente si la persona o personas que están siendo investigadas sospechan que están siendo investigados (Cavalieros, 2020).

La empresa META, como hemos referido antes, cuenta con dos portales de solicitud, identificados como "Online Record Request System" que traducido al español sería algo como Portal En Línea de Solicitud de Registros, además de contar con un personal humano, que en propias palabras de Cavalieros, puede ir orientando y ayudando a los solicitantes con sus dudas. Dentro de estos analistas, hay un equipo llamado ERT que son los que reciben 24/7 las solicitudes de emergencia, los cuales, acorde a las leyes de los Estados Unidos, pueden ofrecer estas informaciones de manera urgente a los oficiales de la ley en los casos en que se verifica una inminente amenaza a la vida o daños corporales graves, en tal caso se puede enviar esa información sin necesidad de orden judicial.

A pesar de que los portales son exactamente los mismos para todos los países, el procedimiento de solicitud y respuesta dependerá de la legislación de cada país, de cuál autoridad y cómo esa autoridad está facultada por su norma interna para solicitar esa información. Por ejemplo, en algunos países los fiscales deben proveerse de una orden judicial para solicitar esta información mientras que en otros están facultados para realizar estas solicitudes directamente a los proveedores de servicio.

LA COOPERACIÓN INTERNACIONAL DESDE LA PLATAFORMA DEL GRUPO MICROSOFT

En cuanto a la empresa Microsoft, Bethular (2020) nos explica que este gigante de la tecnología también ha adecuado su procedimiento de requerimientos judiciales de información de una manera sustancial en los últimos días, pues desde el mes de noviembre de 2020 estos trámites se realizan a través de un servicio online, dentro del cual se incluye también una asistencia especial en casos de emergencia. Dentro de los servicios más populares de Microsoft se encuentran los correos de Outlook y Hotmail, One Drive, Xbox Live, Skype, LinkedIn, Teams y Office 365, entre muchos otros.

Es importante señalar que Microsoft es una empresa de los Estados Unidos y sus procedimientos siempre estarán ajustados a la legislación de este país, aunque tenga diferentes oficinas operativas alrededor del mundo. Sus procedimientos de otorgamiento de información varían dependiendo de si el trámite es simple o urgente. Para el trámite simple u ordinario puede realizarse a través del Law Enforcement Request Portal y el tiempo aproximado de respuesta es de 10 días hábiles desde la remisión de la solicitud, la información se ofrece únicamente dentro del contexto de una investigación penal y comprende datos registrales y logs de conexión de los servicios online de Microsoft. En el caso específico de LinkedIn, el requerimiento debe realizarse a través de la vía tradicional de la comisión rogatoria, la cual implica que una autoridad judicial de un país realice una solicitud formal para obtener asistencia en un caso específico.

El trámite urgente solo tiene aplicación en casos de real emergencia, es decir, bajo el típico supuesto en que se verifique una situación de peligro inminente de muerte o lesiones físicas graves a una o varias personas determinadas, directamente relacionadas con la investigación y la información que se solicita. Estas solicitudes se realizan a través del correo electrónico lealert@microsoft.com y el tiempo aproximado de respuesta es de 6 horas.

CONCLUSIONES

Internet ha redefinido los paradigmas del comportamiento criminal, permitiendo a los delincuentes que residen en una jurisdicción perpetrar los delitos en otra u otras de manera simultánea y bajo el manto de un anonimato casi absoluto. A través de la tecnología, los delincuentes y grupos criminales realizan una variedad de actos que incluyen la explotación sexual de niños, el tráfico de drogas y armas, el robo de identidad, los fraudes financieros y un sinnúmero de acciones dolosas que sobrepasan la capacidad de comprensión de un ciudadano común.

Estas innovaciones criminales han cambiado las reglas del juego en cuanto a la persecución criminal y aplicación de la ley se refiere. Las instituciones diseñadas para proteger la seguridad nacional, limitadas por naturaleza al marco de su propia jurisdicción, han tenido que rediseñarse para poder proveer de una respuesta eficaz a una industria del cibercrimen que crece de manera exponencial. Es en este sentido que resulta impostergable que todos los Estados del mundo colaboren de manera activa en la prevención y persecución de estos delitos y armonicen, en la medida de lo posible, sus normas sustantivas y adjetivas para facilitar la cooperación internacional en la lucha contra el cibercrimen.

Es necesario también entender, y aquí radica parte de la dificultad de su implementación, que estos procesos deben mantenerse siempre apegados al ideal de protección del Estado democrático y el orden público interno e internacional. Se trata pues de equilibrar los conceptos de soberanía y seguridad con un proceso que también garantice rapidez, previsibilidad, eficiencia y seguridad jurídica, tal como lo demanda el escenario actual.

Los tratados, convenios y codificaciones internacionales son sistemas correctos en el sentido de que, al menos en principio, tratan de armonizar la solución de eventuales conflictos, normativos o procesales, que pudieran surgir de tal o cual relación. Parecería ser que este es el sistema ideal, pues estos instrumentos intentan garantizar los elementos de previsibilidad, de orden público, debido proceso, seguridad, etc., y estamos seguros de que así sería, si no existieran los infinitos criterios interpretativos sobre lo que significan cada uno de estos conceptos en los diferentes ordenamientos jurídicos.

En base a esta disparidad conceptual generalizada entre los diferentes elementos que concurren al momento de dar respuesta a una solicitud de cooperación internacional, se hace necesario realizar reformas con miras a

enmarcar dentro de un concepto concreto y claro las nociones fundamentales que concurren en el proceso. En otras palabras, unificar criterios entre los diferentes ordenamientos jurídicos mediante una clara definición del significado y alcance de cada uno de estos elementos de conflicto, que es lo que en cierta medida ha sido el espíritu del Convenio de Budapest desde el momento de su creación y que ahora pretende reforzar con la entrada en vigor de su segundo protocolo.

En principio, si se contara con un texto que preventivamente eliminara cuestiones interpretativas y utilizara categorías muy delimitadas, se evitarían problemas *a posteriori*. No obstante, esta labor aparenta ser un tanto titánica cuando intervienen los factores de cultura jurídica y de orden público de un Estado en particular.

La solución más simple a cuestiones como las señaladas vendría dada por la existencia, junto al texto del convenio, de la atribución de competencia interpretativa a una jurisdicción internacional que se pronunciase en caso de existir desavenencia en torno a los términos del convenio. Es decir, abrir expresamente la vía a un recurso en una jurisdicción internacional o acudir a una organización especializada en la materia objeto del texto internacional que asegure una interpretación objetiva y autónoma, lógicamente mediante un sistema también expedito, pero en lo que esto llega debemos conformarnos con la buena voluntad y el ánimo de cooperación y asistencia mutua entre los Estados parte.

Otro de los temas que no podemos dejar de lado es la creciente y extremadamente necesaria colaboración del sector privado, los llamados proveedores de servicio, con las autoridades estatales de los diversos países en los procesos que envuelven las persecuciones e investigaciones sobre hechos criminales cometidos en el ciberespacio y desde sus plataformas de servicio. Y es que no podía ser de otra manera, pues estos constituyen la fuente primaria, la plataforma que sirve de instrumento para que los criminales del ciberespacio realicen sus actos dolosos. Es por esto que nos atrevemos a afirmar que hoy día resulta prácticamente imposible pensar que la persecución e investigación de los actos criminales llevados en esta esfera virtual pueda ser una actividad exclusiva de los aparatos estatales sin la colaboración activa del sector privado.

Podemos estar plenamente seguros, al menos en la mayoría de los casos, que estas plataformas virtuales no han sido creadas con el objetivo de realizar actos contrarios a la seguridad y a la integridad de sus usuarios o de sus bienes, cuestión por la cual la cooperación de este sector privado reviste un interés

mutuo, pues a la vez que cumplen con el deber ciudadano o institucional de colaborar con las autoridades en los temas de investigación y persecución de actos criminales, coadyuvan en el mantenimiento de un ciberespacio seguro a la vez que protegen también su reputación frente a sus usuarios y patrocinadores.

El propio Convenio de Budapest, aunque de manera un poco tímida, se refiere en su preámbulo a la importancia de reconocer la necesidad de una cooperación entre los Estados y la industria privada en la lucha contra la cibercriminalidad, esto por la necesidad de proteger los intereses legítimos vinculados al desarrollo de las tecnologías de la información, lo anterior a pesar de que en el contenido de sus textos se sigue delegando en el "Estado requerido" las funciones operativas o de gestión, con carácter de intermediación, entre el Estado requirente y el prestador de servicios localizado en su territorio, supeditando la asistencia solicitada a una acción de mandato, orden u obligación de este "Estado requerido" sobre el prestador de servicios.

En principio, digamos, este mecanismo es hasta cierto punto comprensible, pues evidentemente que el convenio debe mantener su esencia de instrumento de compromiso entre Estados. Sin embargo, seguimos apostando a que este segundo protocolo, que ha sido recientemente abierto a su firma, realmente ayude a dinamizar estos aspectos mediante una interacción más directa entre Estado requirente y el sector privado proveedor del servicio, tal como ha sido planteado.

Es importante tener muy claro que la intención no es que la intervención estatal sea totalmente desplazada y suprimida por la interacción directa del Estado requirente con el sector privado, sino más bien crear la conciencia de que se hace impostergable el establecimiento de mecanismos más fluidos, con una intervención Estatal mínima en los aspectos operativos de "intermediación", quizás tratando de reforzar la parte regulatoria, mediante instrumentos que garanticen el control estatal, pero que a la vez simplifiquen, dinamicen, fortalezcan y complementen sus actuaciones, pues está claro que dada la propia naturaleza de la colaboración requerida, una excesiva "intermediación" operativa del aparato estatal, con sus consecuentes entramados burocráticos, pudieran afectar seriamente el desarrollo y feliz término de una investigación de esta naturaleza.

En sentido general, debemos estar conscientes de que la efectividad y celeridad con que deben manejarse estos procesos también forman parte del escenario actual y con ella la permanente necesidad de transformación y

adecuación del régimen legal que está llamado a regularlos. Las normas de hoy serán obsoletas mañana, el proceso que hoy es efectivo posiblemente mañana deje de serlo pues las disposiciones normativas deben estar siempre un paso adelante o al menos caminar paralelamente a los procesos que regulan.

Es en este sentido que entendemos que la revisión y actualización de las normas que regulan la cooperación internacional en materia de cibercrimen no debe enmarcarse dentro de la realización de nuevos cambios estáticos que otorguen solución a un conflicto existente o claramente previsible, se trata pues de crear normativas y procedimientos capaces de adaptarse a las diferentes situaciones que se presentan en el día a día, de fluir con la misma rapidez que caracteriza a las tecnologías del mundo actual, e incluso con mecanismos de auto revisión periódica y órganos supranacionales de unificación de criterios, pero sobre todo con la participación de todos los actores que intervienen en los referidos procesos, pues solo así estaríamos alcanzando el verdadero propósito de una cooperación internacional eficiente y segura, acorde a las necesidades actuales.

REFERENCIAS

Albani, I. (2020). *Effective Access to electronic evidence: towards a new Protocol to the Budapest Convention.* International Association of Prosecutors and the Council of Europe. Webinar.

Artigas, C. & Rodríguez, A. L. (2022). *II Jornada STIC - Colombia: La cooperación internacional, fórmula contra el cibercrimen.* TrendTIC. https://www.trendtic.cl/2022/03/ii-jornada-stic-colombia-la-cooperacion-internacional-formula-contra-el-cibercrimen/

Azzolin, H. (2020). *Acceso Fronterizo.* Diplomado de Posgrado Iberoamericano en Cibercrimen. Universidad Hartmann de México e Instituto Argentino de Reconstrucción Forense Especializada.

Bethular, G. (2020). *Cooperación entre Estados y el Sector Privado.* Diplomado de Posgrado Iberoamericano en Cibercrimen. Universidad Hartmann de México e Instituto Argentino de Reconstrucción Forense Especializada.

Cavalieros, R. (2020). *Cooperación entre Estados y el Sector Privado.* Diplomado de Posgrado Iberoamericano en Cibercrimen. Universidad Hartmann de México e Instituto Argentino de Reconstrucción Forense Especializada.

Consejo de Europa (2001). *Convenio sobre la Ciberdelincuencia.* Budapest.

Consejo de Europa (2003). *Protocolo adicional al Convenio sobre la ciberdelincuencia relativo a la penalización de actos de índole racista y xenófoba cometidos por medio de sistemas informáticos.* Estrasburgo.

Consejo de Europa (2022). *Mejor acceso a las pruebas electrónicas para combatir la delincuencia.* (s/f). Europa.eu, de https://www.consilium.europa.eu/es/policies/e-evidence/

Deluca, S. & del Carril, E. (2017). *Cooperación Internacional en Materia Penal en el Mercosur: El Cibercrimen.*

Fernández, J. & Sánchez, S. (2012). *Diplomado en Derecho de los Negocios Internacionales.* Fundación Global, Democracia y Desarrollo (Funglode) y Universidad Complutense de Madrid.

Oficina de las Naciones Unidas contra la droga y el delito (UNODC) (2022). *Compendio de Ciberdelincuencia organizada,* Naciones Unidas, Viena. p.116

Salt, M. (2020). *Effective Access to electronic evidence: towards a new Protocol to the Budapest Convention.* International Association of Prosecutors and the Council of Europe. Webinar.

Sánchez, G. (2012). *Ciberespacio y el Crimen Organizado.* Los Nuevos Desafíos del Siglo XXI. Universidad Complutense de Madrid.

Seger, A. (2020). *Effective Access to electronic evidence: towards a new Protocol to the Budapest Convention.* International Association of Prosecutors and the Council of Europe. Webinar.

United Nations Office on Drugs and Crime (UNODC) (2018). *Practical Guide for Requesting Electronic Evidence Accross Borders.* https://sherloc.unodc.org/cld/en/publications/practical-guide/practical-guide.html

Verdhelo, P. (2020). *Cooperación Internacional entre Estados y Acceso Fronterizo.* Diplomado de Posgrado Iberoamericano en Cibercrimen. Universidad Hartmann de México e Instituto Argentino de Reconstrucción Forense Especializada.