Universidad Internacional de La Rioja

Facultad de Derecho

Máster Universitario en Ciberdelincuencia

Estado actual de la regulación peruana en el marco del Convenio de Budapest: Análisis desde la cooperación internacional

Trabajo fin de estudio presentado por:	Lizet Nancy Rodriguez Rocha
Tipo de trabajo:	Trabajo de Fin de Máster
Director/a:	D. Daniel Tejada Plana
Fecha:	13-07-2022

Resumen

El Convenio sobre la Ciberdelincuencia nació desde hace más de 20 años; sin embargo, debido a la regulación de los aspectos sustantivos, de índole procesal y de cooperación jurídica internacional, actualmente constituye una herramienta fundamental en la lucha de este tipo de delincuencia. Dicho Convenio cuenta actualmente con 66 Estados Parte, entre los que se encuentra el Perú, país que desde la etapa previa a su adhesión efectuó una serie de modificaciones normativas, logrando entrar en vigor el 1 de diciembre de 2019. Mediante el presente trabajo se analizará el estado actual de la regulación en el Perú a raíz de su incorporación a dicho Convenio y cómo, a pesar de los diversos esfuerzos, existe la necesidad de realizar mayores reformas normativas, suceso que viene trayendo diversas consecuencias desde su aplicación práctica y que repercute en el avance de las investigaciones.

Palabras clave:

Convenio sobre la Ciberdelincuencia

Ciberdelitos

Cooperación jurídica internacional

Abstract

The Convention on Cybercrime was born more than 20 years ago, however, due to the regulation of substantive, procedural and international legal cooperation aspects, it currently constitutes a fundamental tool in the fight against this type of crime. Said Convention currently has 66 States Parties, among which is Peru, a country that from the stage prior to its accession made a series of regulatory modifications, managing to enter into force on December 1, 2019. Through this work, it will be analyzed the current state of regulation in Peru as a result of its incorporation into said Convention and how, despite the various efforts, there is a need for further regulatory reforms, an event that has brought various consequences from its practical application and that has repercussions on progress of investigations.

Keywords:

Convention on Cybercrime

Cybercrime

International legal cooperation

Índice de contenidos

Introducción

1.1. Justificación del tema elegido

En el Perú la regulación de la ciberdelincuencia ha tenido pocos cambios, siendo que en nuestro Código Penal de 1991 se incluyó en el capítulo de delitos contra el patrimonio individual el hurto mediante la transferencia no autorizada de fondos y posteriormente, mediante la Ley N°27309, de fecha 17 de julio de 2000, se incorporaron los delitos informáticos de acceso ilícito y atentado contra sistemas informáticos. Asimismo, mediante la Ley N°30096, del 11 de octubre de 2013, se regularon en una ley especial los delitos informáticos, con la que se produjo la modificación del delito de pornografía infantil y del delito de discriminación para incluir la utilización de medios tecnológicos. También se reguló la figura del agente encubierto en delitos informáticos. Posteriormente, a través de la Ley N°30171, del 10 de marzo de 2014, se efectuó la modificación de la Ley N°30096, referente a la tipificación de los artículos 2, 3, 4, 5, 7, 8 y 10, siendo esta la regulación hasta la actualidad de los delitos informáticos.

Con dichas disposiciones de índole sustantiva y la única de índole procesal, es que en el año 2014 el Perú solicitó suscribir el Convenio de Budapest. El Consejo de Europa aprobó la solicitud del Perú y en el año 2015 fue invitado para su suscripción, siendo que después de que la Presidencia del Consejo de Ministros del Perú recomendara la referida suscripción acogiéndose a las reservas previstas, el Convenio sobre la Ciberdelincuencia fue ratificado mediante Decreto Supremo N°010-2019-RE, de fecha 10 de marzo de 2019 y estableciéndose su entrada en vigor el 1 de diciembre de 2019.

No obstante, para que nuestro país pueda lograr la integración de las disposiciones del Convenio sobre la Ciberdelincuencia, resulta necesario efectuar diversas modificaciones normativas. Al respecto, existen diversos estudios internacionales que resaltan la necesidad de que los países adopten decisiones políticas que permitan mejorar los niveles de coordinación, armonización y actualización normativa, la adopción de recursos necesarios para gestionar una estructura adecuada para la detección, investigación y persecución eficaz de los delitos informáticos (TEMPERINI 2014). Por su parte, VELASCO (2011) realiza un análisis de los instrumentos jurídicos de cooperación bilateral y multilateral, así como los memorándums de entendimiento que utilizan los gobiernos para obtener información

relacionada con la localización de sospechosos y víctimas. En esa misma línea tenemos a DÍAZ (2010), quien resalta la importancia del correcto establecimiento de la cooperación internacional para hacer frente a los ciberdelitos.

Asimismo, en el ámbito peruano se han realizados diversos estudios en los que los autores consideraron necesario la adopción de diferentes medidas procesales con el fin de viabilizar la persecución penal y facilitar la acumulación de pruebas, tal es el caso de GUTIÉRREZ (2018), quien luego de haber realizado un estudio integral sobre las normas penales y en materia de ciberseguridad peruana, resaltó la necesidad de la adopción de obligaciones referente a la conservación de datos informáticos. Así también, PEREYRA Y TURPO (2020) concluyen que es de suma urgencia y necesidad, la revisión y actualización de la ley de delitos informáticos con el fin de adecuarlos al marco legal del Convenio de Budapest para que los mecanismos de cooperación internacional resulten más eficaces.

Es por ello que, mediante el presente trabajo, se abordará la situación actual peruana, demostrándose que, a pesar de que el Perú es Estado Parte del Convenio desde hace más de dos años, hasta la fecha no ha logrado adaptar sus disposiciones al ámbito procesal, especialmente en lo relativo a (i) las relacionadas con las medidas de conservación rápida de datos informáticos, conservación y revelación parcial rápida de los datos relativos al tráfico (artículos 16 y 17 del Convenio) y (ii) al marco de la cooperación internacional, referente a las regulaciones de asistencia mutua en medidas provisionales (artículos 29 y 30 del Convenio).

1.2. Problema y finalidad del trabajo

El presente trabajo se realiza debido a la problemática advertida en el marco de la tramitación de los pedidos cooperación jurídica internacional y de las solicitudes efectuadas al amparo de la Red 24/7 del Convenio sobre Ciberdelincuencia relacionadas con la conservación de datos informáticos, de cuyos trámites se verificó la existencia de diversas regulaciones de la retención de datos que abarcan desde normas administrativas hasta penales, tal y como lo hallamos en el artículo 16 de la Ley N°27336, Ley de Desarrollo de las Funciones y Facultades del Organismo Supervisor de Inversión Privada en Telecomunicaciones – OSIPTEL. En este artículo se establece que las entidades se encuentran obligadas a guardar información relacionada con la tasación, los registros fuentes del detalle de las llamadas y facturación de los servicios que explota por un periodo de 3 años, pero el periodo cambia si lo que se requiere

es solicitar información sobre los registros de asignaciones de direcciones IP públicas y privadas asociadas al servicio de acceso a internet del usuario, de forma estática o dinámica. Esto es así ya que en el artículo 11 de la Resolución de Consejo Directivo de OSIPTEL N°123-2014-CD-OSIPTEL se establece una obligación a las empresas proveedoras de almacenar por un periodo mínimo de 3 meses, tiempo que difiere cuando el pedido se encuentra relacionado con la medida de geolocalización de equipos de comunicación en la lucha contra la delincuencia y el crimen organizado, en el que a través del Decreto Legislativo N°1182 se estableció que los concesionarios de servicios públicos de telecomunicaciones y las entidades públicas deban conservar los datos derivados de las telecomunicaciones durante los primeros doce (12) meses en sistemas informáticos.

Estas diferentes regulaciones han permitido evidenciar que, para el caso de las informaciones relacionadas con las IP´s -que constituyen la mayor cantidad de pedidos en el marco de investigaciones relacionadas con la ciberdelincuencia-, se presenten serios problemas. Ello es debido al corto periodo de obligación existente para retener los datos, toda vez que al recibir las solicitudes de conservación provenientes de países extranjeros, se han obtenido respuestas negativas por parte de los proveedores que prestan servicios en territorio peruano, quienes indicaron que el periodo de obligación para que almacenarán la información ya se encontraba vencido a la fecha que se les envío el requerimiento.

Asimismo, en el marco de las solicitudes de asistencia judicial internacional pasivas, también relacionadas con la identificación de titularidad de IP´s, se obtuvieron respuestas de los proveedores señalando la imposibilidad técnica de brindar la información debido a que no tenían registrado la titularidad de los clientes, respuestas con las que no se contribuye al avance de las investigaciones penales.

Siendo que, a nivel de derecho comparado, podemos citar los esfuerzos realizados desde el ámbito del derecho europeo, quienes no solo intentaron efectuar una regulación del tratamiento de los Datos Personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas mediante la Directiva 2002/58/CE, la que fue posteriormente modificada por la Directiva 2009/136/CE del Parlamento Europeo y del Consejo. Asimismo, podemos reseñar la reciente jurisprudencia (FJ 129 STJ 5/2022) en la que el Tribunal de Justicia de la Unión Europea declaró que no se oponían a una conservación selectiva de los datos y tráfico y de localización que esté delimitada, para un periodo temporalmente limitado a lo

estrictamente necesario, pero que podrá renovarse; así como a una conservación generalizada e indiferenciada de las direcciones IP atribuidas al origen de una conexión y a una conservación generalizada e indiferenciada de los datos relativos a la identidad civil de los usuario de medios de comunicaciones electrónicas.

1.3. Objetivos

1.3.1. Objetivo general

- Analizar el estado actual de la regulación peruana ante la de vigencia del Convenio de Budapest

1.3.2. Objetivos específicos

- Determinar la regulación normativa peruana a nivel sustantivo, procesal y de cooperación internacional.

- Identificar la problemática actual existente en la tramitación de los pedidos de cooperación internacional pasivos en el marco de la ciberdelincuencia.

- Identificar la problemática actual existente en la tramitación de los pedidos pasivos al amparo de la Red 24/7 del Convenio de Budapest.

2. Marco teórico y desarrollo

2.1. El Convenio de Budapest y su regulación

El Convenio sobre la Ciberdelincuencia es un tratado internacional que fue adoptado en Hungría- Budapest con la finalidad de establecer lineamientos comunes para los Estados en la lucha contra el fenómeno de la ciberdelincuencia. Actualmente se encuentra vigente en 66 Estados Parte, siendo el primer y único instrumento internacional existente hasta la fecha en la materia (DIAZ, 2010, p 195).

Sobre su estructura, cabe señalar que éste consta de 48 artículos y un preámbulo inicial, los que se encuentran recogidos en cuatro capítulos, divididos en secciones y títulos, y cuyo objetivo consiste en intensificar la cooperación entre los Estados Parte, así como aplicar una política penal común para proteger a la sociedad frente a la ciberdelincuencia, términos en los que hemos puesto énfasis, toda vez que constituyen las líneas de orientación de los artículos del citado convenio.

- A nivel del derecho sustantivo, el Convenio establece que cada país debe adoptar medidas legislativas para tipificar como delito en su derecho interno los siguientes ilícitos: 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, entre otros.
- A nivel de derecho procesal se establece lo referente a la conservación rápida de datos informáticos almacenados, la orden de presentación, el registro y confiscación de datos informáticos almacenados, obtención en tiempo real de datos relativos al tráfico, interceptación de datos relativos al contenido, así como las medidas legislativas necesarias para que cada Estado Parte afirme su jurisdicción respecto de los delitos regulados en los artículos 2 al 11 del Convenio.
- A nivel de la cooperación internacional se establece regulación de la extradición, los principios generales relativos a la asistencia mutua (los que se aplican en ausencia de acuerdos internacionales); la confidencialidad y restricciones de uso. Así también, en el marco de la asistencia mutua en medida provisionales se regula la conservación rápida de datos informáticos almacenados; la revelación rápida de datos conservados;

la asistencia mutua relacionada con el acceso a datos almacenados; el acceso transfronterizo a datos almacenados con consentimiento o cuando sean accesibles al público; la asistencia mutua para la obtención en tiempo real de datos relativos al tráfico y la regulación sobre el funcionamiento de la Red 24/7.

2.1.1. Evolución de la legislación peruana en el marco de la ciberdelincuencia

La evolución de la regulación de la ciberdelincuencia el Perú nos lleva a revisar nuestro Código Penal de 1991, en especial el capítulo de delitos contra el patrimonio individual, en cuyo numeral 3 del artículo 186 se tipificó el **delito de hurto mediante la utilización de sistemas de transferencia electrónica de fondos y de telemática en general.** Al respecto, BRAMONT-ARIAS TORRES (1997, p. 301), sostuvo que la transferencia electrónica de fondos es aquel procedimiento que se realiza a través de un terminal electrónico, instrumento telefónico o un ordenador, por el cual se autoriza un crédito o débito. Asimismo, ROJAS VARGAS (2000, p. 282) señaló que las modalidades comisivas de la agravante podían darse mediante el apoderamiento, cargando a la cuenta del acreedor los fondos derivados de la cuenta o de la tarjeta de crédito del deudor, incursiones a las cuentas bancarias del agraviado para desviar fondos a cuenta de terceras personas, adulteración de saldo de una cuenta en base a transferencias ficticias.

Por su parte, SALINAS (2008, p. 893), sostuvo que esta era una de las formas más frecuentes de sustracción y apoderamiento de dinero y que muchas veces no se denunciaba para evitar la desconfianza de los usuarios en el sistema financiero, situación que originó el alto índice de la cifra negra de la criminalidad informática.

No pasó mucho tiempo para que el legislador peruano advirtiera que lo previsto en dicho articulado solo servía para sancionar un número reducido de conductas patrimoniales, pero no para reprimir la manipulación de los ordenadores, destrucción de programas o datos, ni el acceso o utilización indebida de información (SALINAS 2008).

Es por ello, que en 17 de julio de 2000 se promulgó la Ley N°27309, mediante la que se incorporaron los delitos informáticos al Código Penal peruano, normativa por la que se tipificó en el artículo 207-A el **delito de acceso ilícito o hacking lesivo**, a través del cual se reguló la sanción de quien utilizaba o ingresaba indebidamente una base de datos, sistema o red de computadoras para interferir, interceptar, acceder o copiar información en tránsito o

contenida en una base de datos, y atentado contra sistemas informáticos. Por otro lado, en el artículo 207-B se reguló el **delito de sabotaje informático,** por medio del cual se estableció la sanción para el que utilizaba, ingresaba o interfería indebidamente una base de datos, sistema, red de computadoras con el fin de alterarlos, dañarlos o destruirlos, cada una de las figuras contaban con su **modalidad agravante**, la que se encontraba tipificada en el artículo 207-C.

En el año 2011, la Comisión de Justicia y Derechos Humanos del Congreso (Dic, CJDH, de 14 de febrero de 2014), luego de analizar la aplicación de los tipos penales regulados en la Ley N°27309 y de advertir que se no registraban estadísticas oficiales por más de 11 años, concluyó la necesidad de sistematizar los tipos penales que afectan a los sistemas informáticos y en los que su uso lesione bienes jurídicos tales como la indemnidad sexual, patrimonio, fe pública y propiedad intelectual en una ley especial, con la finalidad de contribuir a una oportuna persecución y sanción de este tipo de delitos.

Es a raíz de ello que el 11 de octubre de 2013 se promulgó la Ley N°30096, denominada Ley de delitos informáticos, normativa mediante la cual se derogaron los artículos 207-A, 207-B y 207-C del Código Penal y que estableció como objeto el prevenir y sancionar las conductas ilícitas que afectan los sistemas y datos informáticos y otros bienes jurídicos de relevancia penal cometidos mediante la utilización de tecnologías de la información o de la comunicación. Dicha norma regula los siguientes delitos:

- Capítulo II: Los delitos contra datos y sistemas informáticos, lo que se encuentran conformados por el delito de acceso ilícito, atentado contra la integridad de datos informáticos y atentado contra la integridad de sistemas informáticos;
- Capítulo III: Los delitos contra la indemnidad y libertad sexual, conformado por el delito de proposiciones a niños, niñas y adolescentes con fines sexuales por medios tecnológicos;
- Capítulo IV: Los delitos contra la intimidad y el secreto de las comunicaciones, conformados por el delito de tráfico ilegal de datos y el de interceptación de datos informáticos;
- Capítulo V, los delitos contra el patrimonio, conformados por el delito de fraude informático; capítulo VI los delitos contra la fe pública, en el que se encuentra el delito de suplantación de identidad

- Capítulo VII: El delito de abuso de mecanismos y dispositivos informáticos, las circunstancias agravantes, así como la exención de responsabilidad.

No obstante, no pasaron muchos meses para que, el 10 de marzo de 2014, se efectuara la modificación de la Ley 30096, la que se produjo mediante la Ley N°30171. Al respecto, VILLAVICENCIO (2014, p. 287) sostiene que su finalidad fue adecuar los estándares del Convenio sobre Ciberdelincuencia referente a la tipificación de los artículos 2, 3, 4, 5, 7, 8 y 10 al adecuar la posibilidad de cometer el delito deliberada e ilegítimamente. Asimismo, se efectuó la modificación de la tercera, cuarta y undécima disposiciones complementarias finales de la Ley 30096, siendo importante resaltar la regulación e imposiciones de multas por el organismo Supervisor de Inversión Privada en telecomunicaciones, en el que se estableció la aplicación de multas en escala a las empresas que incumplan con la obligación prevista en la diligencia de intervención, grabación o registro de las comunicaciones y telecomunicaciones, las que debían ser impuestas en atención a las características, complejidad y circunstancias de los casos aplicables.

Referente a las modificaciones efectuadas en el ámbito procesal, debemos señalar que de la revisión del Código Procesal Penal, promulgado mediante Decreto Legislativo N°638, del 27 de abril de 1991, ni del Nuevo Código Procesal Penal, Decreto Legislativo N°957, del 29 de julio de 2004- que se encuentra vigente hasta la fecha-, no se advirtieron mayores modificaciones referentes a las técnicas destinadas a combatir la ciberdelincuencia. Por el contrario, sólo podemos hacer mención a la incorporación de la figura del **agente encubierto informático,** la que se produjo en el marco de la Segunda Disposición Complementaria final de la Ley N°30096, y que estableció como facultad del fiscal el autorizar estas actuaciones para los delitos previstos en el marco de la ley de delitos informáticos y en todo delito que se cometa mediante tecnologías de las información o comunicación.

Un punto importante que resaltar de esta regulación es que para su aplicación no se exige que el delito informático se realice en el marco de una organización criminal, a diferencia de la regulación existente en el artículo 342 de nuestro Código Procesal Penal, siendo esta la única modificación a nivel procesal, por cuanto actualmente para la realización de diligencias de interceptación de comunicaciones, así como otras técnicas de investigación se continúan aplicando las disposiciones generales contenidas en nuestro Código Procesal Penal.

2.1.2. Proceso para la adhesión del Perú al Convenio de Budapest

Para que los países puedan efectuar su adhesión a una Convención internacional, de manera previa deben efectuar una serie de acciones a nivel interno con el fin de realizar las modificaciones normativas necesarias para brindar mayor operatividad a las disposiciones, de modo que estas no contravengan el contenido del Convenio internacional.

En el caso de la Convención sobre la Ciberdelincuencia, los Estados que participaron en la negociación, esto es, los miembros del Consejo de Europa, Canadá, Japón, Sudáfrica y Estados Unidos de América, se encontraban habilitados para firmar y ratificar el Tratado. No obstante, de conformidad con lo establecido en el artículo 37, cualquier Estado que no sea miembro del Consejo de Europa también se encontraba facultado para convertirse en Parte mediante un procedimiento de adhesión, el que se realiza si el Estado se encuentra preparado para implementar el tratado.

En el caso del Perú, en el año 2014 solicitó adherirse al Convenio de Budapest, lo que implicó que a nivel interno se efectuaran diversas coordinaciones con las entidades que estarían involucradas con su implementación, a raíz de lo cual se recibió diversas opiniones, entre las que resaltan la emitida por la Oficina Nacional del Gobierno Electrónico e Informática de la Presidencia del Consejo de Ministros, entidad que hizo referencia a que la adhesión al Convenio formaba parte de la vigente Política Nacional de Gobierno Electrónico y la Agenda Digital Peruana 2.0, destinadas al combate de la ciberdelincuencia.

En el año 2015, después de los trámites oportunos realizados por parte de la Oficina de Tratados de la Dirección de Asesoría Jurídica y de Derecho Internacional Público del Consejo de Europa, el Perú fue invitado para su adhesión. No obstante, el proceso a nivel interno no resultó célere, por cuanto recién en mayo del 2018, esto es, casi 3 años después, el Ministro de Relaciones Exteriores puso a consideración del Congreso de la República el Proyecto de Resolución Legislativa que aprobaba el Convenio sobre Ciberdelincuencia, la que fue aprobada mediante Resolución Legislativa N°30912, de fecha 13 de febrero de 2019 y ratificada mediante el Decreto Supremo N°010-2019-RE, de fecha 10 de marzo de 2019, en el que se efectuaron las siguientes **declaraciones**:

- En el delito de acceso ilícito, en el que se indicó que nuestro país exige que éste se cometa infringiendo medidas de seguridad;

- En el delito de interceptación ilícita se declaró que la legislación exige que se cometa con intención delictiva y que pueda cometerse con relación con un sistema informático conectado a otro;
- En el delito de falsificación informática, nuestro país declaró que podrá exigir que exista una intención fraudulenta o delictiva similar para que dichas conductas generen responsabilidad penal.
- En el marco de la cooperación internacional declaró que, en aras de la eficacia del trámite de las solicitudes de asistencia mutua en ausencia de acuerdos internacionales aplicables, estas deben dirigirse a nuestra Autoridad Central.

En cuanto a las **reservas** se realizaron las siguientes:

- La no aplicación de disposiciones relativas al delito de abuso de dispositivos;
- Respecto al delito de pornografía infantil, se establecieron reservas sobre las conductas que no involucraban la participación de un menor de edad;
- El derecho de denegar una solicitud de conservación en el caso que se tengan motivos para creer que al momento su revelación no se cumplirá con la condición de la doble incriminación.

Con fecha 18 de marzo de 2019, a solicitud de la Presidencia del Consejo de Ministros, se llevó a cabo una reunión de trabajo multisectorial entre los representantes del Ministerio del Interior, Ministerio de Justicia y Derechos Humanos, Policía Nacional del Perú, Academia de la Magistratura, Poder Judicial, Tribunal Constitucional y el Ministerio Público -*siendo que en el caso de esta última institución participaron fiscales de la Oficina de Cooperación Judicial Internacional y Extradiciones de la Fiscalía de la Nación*- con la finalidad de definir las acciones correspondientes y pasos a seguir para la implementación del citado Convenio. A raíz de lo anterior se efectuó el compromiso de solicitar a cada autoridad involucrada para analizar los tipos penales regulados en el Convenio de Budapest con el fin de lograr su armonización con el derecho interno. Sin embargo, luego de dicha reunión no se efectuaron mayores avances.

Pese a esta falta de avances, el 22 de setiembre de 2019 se efectuó la publicación en el Diario Oficial El Peruano del Convenio sobre la Ciberdelincuencia, estableciendo como fecha de su entrada en vigencia el 1 de diciembre de 2019.

Asimismo, la Oficina de Cooperación Judicial Internacional y Extradiciones elevó un informe a la Fiscalía de la Nación (UCJIE 2019) en el que se efectuó el análisis de la data estadística existente de los delitos informáticos regulados desde el año 2014 y de su evolución, se expuso la experiencia de los países de la región tales como de la República de Argentina, Paraguay y Brasil, los que desde hace varios años atrás ya contaban con Unidades Fiscales Especializadas en Delitos Informáticos, así como se presentaron las contribuciones de dichas oficinas en el avance de las investigaciones por lo que se sugirió la conversión de fiscalías que conocían delitos comunes con el fin de que se avoquen al conocimiento de los delitos informáticos. No obstante, las mismas no fueron implementadas antes de que entrara en vigor el citado Convenio.

2.2. La Cooperación Internacional y el Convenio de Budapest

Actualmente, diversos aspectos tales como la aparición de las nuevas tecnologías de la comunicación y el ciberespacio, la extraterritorialidad de las conductas -que se originan debido al uso del internet y la ausencia de barreras geográficas- y la globalización han propiciado la comisión de diversos ilícitos a una distancia y velocidad impensadas (RIQUET 2008). Ante ello, la cooperación judicial internacional se erige como una herramienta de vital importancia, ya que permite llevar a cabo un acto en una jurisdicción extranjera (GOICOCHEA 2016). Existen para ello dos formas distintas de colaboración, por un lado la que brinda y ejecuta una autoridad nacional para brindar apoyo a un Estado extranjero y suele denominarse como cooperación pasiva; y, por otro lado, la que se efectúa ante un requerimiento formulado por las autoridades nacionales hacia el extranjero, la que se denomina cooperación activa (CASTELLO 1983).

En ese sentido, (VILLALTA 2013, p. 51), define a la cooperación judicial internacional en materia penal como un conjunto de actos de naturaleza jurisdiccional, diplomática o administrativa que involucra a dos o más Estados y que tiene por finalidad la persecución y la solución de un hecho delictivo ocurrido en territorio cuando menos, de uno de tales Estados, por lo que sostiene que se ha convertido en la actualidad en uno de los instrumentos más eficaces y necesarios para el combate de la delincuencia.

Esta herramienta tiene como fundamento jurídico los tratados bilaterales o multilaterales y de manera residual en el Principio de Reciprocidad, así como la legislación procesal penal

interna de los países y su utilización permite el intercambio de información, practicar actuaciones judiciales, localizar e identificar a personas y bienes, recibir testimonios, interrogatorios de imputados, testigos o peritos, embargos, secuestro, decomiso de bienes, entre otros, y que posteriormente dicha prueba pueda ser incorporada válidamente en el marco de las investigaciones y procesos penales.

Al respecto existen diversos estudios internacionales entre los que se resalta la necesidad de que los países adopten decisiones políticas que permitan mejorar los niveles de coordinación, armonización y actualización normativa, la adopción de recursos necesarios para gestionar una estructura adecuada para la detección, investigación y persecución eficaz de los delitos informáticos (TEMPERINI 2014). Por su parte, VELASCO (2011), en su tesis doctoral «El derecho y la jurisdicción aplicable en materia de conductas delictivas cometidas en internet a la luz del convenio sobre ciberdelincuencia del Consejo de Europa con un particular enfoque en México y países de Latinoamérica», realiza un análisis de los instrumentos jurídicos de cooperación bilateral y multilateral, así como los memorándums de entendimiento que utilizan los gobiernos para obtener información relacionada con la localización de sospechosos y víctimas. En esa misma línea tenemos a la tesis doctoral «El Delito informático, su problemática y la cooperación internacional como paradigma de su solución: El Convenio de Budapest», mediante la cual se resalta la importancia del correcto establecimiento de la cooperación internacional para hacer frente a los ciberdelitos (DIAZ 2010).

Asimismo, en el ámbito peruano se han realizados diversos estudios en los que los autores han considerado necesario la adopción de diferentes medidas procesales con el fin de viabilizar la persecución penal y facilitar la acumulación de pruebas, tal es el caso de GUTIERREZ (2018) quien luego de haber realizado un estudio integral sobe las normas penales y en materia de ciberseguridad peruana resaltó la necesidad de la adopción de obligaciones referente a la conservación de datos informáticos. Así también, PEREYRA Y TURPO (2020), en su trabajo de investigación denominado «Instrumentos normativos que se deben adecuar en nuestra legislación según el marco del Convenio de Budapest como mecanismo legal de protección a la intimidad personal frente a las TICS», concluyen que resulta de suma urgencia y necesidad la revisión y actualización de la ley de delitos informáticos con el fin de adecuarlos al marco legal del Convenio de Budapest para que los mecanismos de cooperación internacional resulten más eficaces.

En el marco de la regulación del Convenio sobre la Ciberdelincuencia este aspecto se encuentra reconocido en su capítulo III, denominado cooperación internacional, en el que se destaca el ***alcance general de la obligación de cooperar*** y se establece en su artículo 23 que la cooperación se realizará respecto de todos los delitos penales relacionados con sistemas y datos informáticos, así como para la obtención de pruebas en formatos electrónicos de los delitos. Por ejemplo, se puede citar dicho Convenio como instrumento jurídico cuando se deba requerir una solicitud de asistencia judicial internacional en el marco de una investigación por un delito de acceso ilícito o cuando se encuentre investigando un delito de chantaje sexual en el que se esté usando el Facebook o Instagram para su comisión.

Con relación a la ***transmisión espontánea de información***, esta herramienta se encuentra regulada en el artículo 26 del citado Convenio y su importancia radica en que en la posesión de información valiosa que posee un Estado Parte y que puede ayudar a otro en una investigación o procedimiento penal, su fundamento se encuentra en la mayor colaboración de los Estados, resaltando su utilidad puesto que el envío de información se efectúa sin necesidad de que exista petición previa del otro Estado, y sólo en el caso de que se envíe información de carácter sensible se puede requerir que ésta se mantenga confidencial, o que la misma se utilice bajo ciertas condiciones (Consejo de Europa, 2003).

Con relación a los ***actos de asistencia mutua en materia de medidas provisionales***, nos centraremos en especial en la asistencia mutua regulada en el artículo 25 del citado Convenio, la que en atención a la volatilidad de los datos informáticos y el correspondiente riesgo de eliminación, ante la demora en la obtención de información, otorga la facultad a los Estados Parte para formular solicitudes de cooperación y remitirlas por medios expeditivos, tales como el uso de correos electrónicos, fax, siendo esta una de las principales ventajas, a diferencia de las formas de cooperación tradicional cuyo trámite era realizado por intermedio de valijas diplomáticas, lo que implicaba mayor trámite e inversión de tiempo y costos, medida también reconocida para obtener respuestas rápidas.

Con relación a la ***conservación rápida de datos informáticos almacenados***, constituye un mecanismo que se encuentra regulado en el artículo 29 y mediante el cual se establece la autorización a un Estado Parte para requerir la conservación rápida de los datos que se encuentran en algún sistema informático de un territorio extranjero. Esta tiene carácter provisional y su finalidad esencial está relacionada con el impedimento de que la información

sea alterada o eliminada, ya que el resguardo se produce para ayudar a la autoridad extranjera mientras elabora su solicitud de asistencia judicial internacional con la finalidad de obtener la revelación de la información. Ya en el Informe Explicativo de la Convención (Consejo de Europa, 2003, p. 83) se señala que esta medida -debido a su naturaleza- requiere que su atención en la práctica convencional sea menor a la que demora una solicitud de asistencia mutua, con la única finalidad de evitar que los datos se pierdan de manera irreparable.

La ***revelación rápida de datos conservados relativos al tráfico***, medida regulada en el artículo 30, en el que se establece que la Parte requerida puede descubrir que los datos relativos al tráfico encontrados en su territorio revelan que la transmisión había sido encaminada desde un proveedor de servicios situado en un tercer Estado, o desde un proveedor de servicios que se encuentra en el mismo Estado requirente. En tales casos, la Parte requerida debe proporcionar sin demora a la Parte requirente una cantidad suficiente de datos relativos al tráfico que permita la identificación del proveedor de servicios y el trayecto de la comunicación desde el otro Estado. Asimismo, se señala que, si la transmisión pasó por un tercer Estado, la información proporcionada debe permitir a la parte requirente hacer una solicitud rápida de conservación y asistencia mutua a ese otro Estado con el fin de rastrear la transmisión hasta su origen (Consejo de Europa 2003, p. 85).

Respecto a la ***Red 24/7,*** esta resulta una novedad, por cuanto de la revisión de las Convenciones de Naciones Unidas contra el Tráfico Ilícito de Estupefacientes y Sustancias Psicotrópicas, contra la Corrupción y contra el Crimen Organizado Transnacional, no se advierte un mecanismo de dicha naturaleza regulado por un instrumento jurídico de carácter internacional. Asimismo, es importante hacer mención que en el Informe Explicativo se hace referencia que para su creación se tomó como base la experiencia de la Red creada con el auspicio de las naciones del G8 (Consejo de Europa, 2003, p. 88).

El funcionamiento de la red se encuentra regulado en el artículo 35 y establece la obligación de cada Estado Parte para designar a un punto de contacto que esté disponible las 24 horas del día, los 7 días de la semana, con el fin de asegurar la asistencia inmediata en las investigaciones. Asimismo, se hace referencia a que los puntos de contacto deben efectuar labores de asesoramiento técnico, apoyo en la conservación de datos, obtención de pruebas, localización de sospechosos y suministro de información de carácter jurídico, esta última a manera de ejemplo se grafica con la asesoría que se brindan a las autoridades para el

conocimiento de los requisitos necesarios para prestar la cooperación, ya sea de manera formal o informal, así como se resalta la necesidad de dotar al personal que participa como parte del equipo de la red, tanto de la logística adecuada, como de una formación adecuada con relación a los delitos informáticos. Es por ello por lo que los expertos señalan que el establecimiento de dicha red es uno de los más importantes medios previstos para responder eficazmente a los desafíos que plantea la aplicación de las leyes respecto de los delitos informáticos o los delitos relacionados con la informática (Consejo de Europa 2003, p.89).

Como se ha podido apreciar, el establecimiento de estas herramientas de la cooperación internacional en el marco de la ciberdelincuencia no resultan nuevas, ya que se encuentran vigentes desde el año 2001 y si bien con el paso de los años el desarrollo de la tecnología ha ido evolucionando y con ello las nuevas técnicas y modalidades de la comisión de delitos, también lo es que el citado Convenio se encuentra en constante revisión y su actualización se viene realizando a través de su Protocolos Adicionales.

El *Primer Protocolo Adicional que penaliza la criminalización de actos de naturaleza racista y xenófoba cometidos a través de sistemas informáticos*, se abrió a la firma el 28 de enero de 2003, habiéndose establecido su entrada en vigor el 01 de marzo de 2006. Este instrumento internacional establece que su finalidad es completar las disposiciones del Convenio sobre la Ciberdelincuencia y regula como medidas que debe tomarse a nivel nacional que cada Estado parte deba adoptar las medidas legislativas para tipificar en su derecho interno la difusión de material racista y xenófobo mediante sistemas informáticos, amenazas con motivación racista y xenófoba, insultos con motivación racista y xenófoba y negación, minimización burda, aprobación o justificación del genocidio o de crímenes contra la humanidad. A la fecha cuenta con 33 países que se han adherido, siendo que, en el caso de América Latina, Paraguay es el único país que se adhirió, habiendo entrado en vigor en el año 2018.

El *Segundo Protocolo Adicional relativo al refuerzo de la cooperación y divulgación de pruebas electrónicas*, instrumento jurídico que fue abierto a la firma este 13 de mayo de 2022 y hasta la fecha cuenta con 24 países firmantes. Este contempla las siguientes herramientas, tales como las solicitudes directas a registradores en otras jurisdicciones para obtener información de registro de nombres de dominio, cooperación directa con proveedores de servicios en otras jurisdicciones para obtener información de suscriptor, medios efectivos para obtener información de suscriptores y datos de tráfico de gobierno a gobierno, la cooperación expedita

en situaciones de emergencia, los equipos conjuntos de investigación y la regulación de la videoconferencia como medio válido para practicar tomas de declaraciones.

2.2.1. La Autoridad Central peruana y sus funciones

Antes de hablar de la cooperación jurídica internacional en el Perú, resulta necesario efectuar una explicación sobre lo que es una Autoridad Central y qué rol viene desempeñando actualmente.

MORÁN (2015, p. 4), señala que el nacimiento de la idea de Autoridad Central se realizó en el marco de la cooperación civil en el Convenio de La Haya de 1965 relativo a la citación y notificación en el extranjero de actos judiciales y extrajudiciales en materia civil y comercial y cuyo objetivo consistió en contar con un mecanismo rápido de transmisión, así como eliminar las vías diplomáticas. En ese sentido, refiere que la Autoridad Central se constituye como un órgano técnico especializado encargado de la interlocución en materia de cooperación judicial en los aspectos tanto civiles como penales y cuya creación constituyó el primer paso en el proceso de agilización de comunicaciones entre dos o más Estados y que viene jugando un papel importante en la mejora de la cooperación internacional desde el siglo XX.

Del mismo modo, hace referencia a los resultados del informe emitido por la Comisión Europea sobre cooperación internacional en materia de drogas entre Europa y los países de Latinoamérica y Caribe, en el que luego de advertir que ciertos países contaban con más de 4 diferentes autoridades centrales -las que incluso se localizaron en organismos administrativos sin vinculación con la administración de justicia- recomendaron que la designación de las Autoridades Centrales sea una sola en cada país, destacando las ventajas de que las Fiscalías ejerzan dicha tarea. Para dicha autora, el situar a las fiscalías como autoridades centrales favorece la agilidad y la comunicación, siendo que los países latinoamericanos vienen optando en los últimos años por designar como autoridades centrales a los Ministerio Públicos.

Con relación a la formación de la Autoridad Central peruana debemos indicar que en un inicio las labores fueron ejercidas por el Ministerio de Justicia y Derechos Humanos. No obstante, desde 1993 ya existía el Proyecto de Ley sobre Asistencia Mutua en Materia Penal y Traslado de Condenado, en cuyo artículo 2 se establecía que correspondería a la Fiscalía de la Nación el asumir el rol de autoridad central para la coordinación, recepción o envío, por intermedio

del Ministerio de Relaciones Exteriores, de las solicitudes sobre asistencia judicial y traslados de condenados.

Posteriormente, en julio del año 2004 se dio la promulgación del Decreto Legislativo N°957- Nuevo Código Procesal Penal, cuerpo normativo que en el Libro VIII reguló la Cooperación Judicial Internacional y en cuyo artículo 512 se estableció que la Fiscalía de la Nación es la Autoridad Central en materia de cooperación jurídica internacional, habiéndose regulado como funciones la coordinación y realización de consultas con la autoridad extranjera para instar los actos de cooperación judicial internacional y el celebrar con las autoridades centrales del extranjero actos dirigidos al intercambio de tecnología, experiencia, coordinación de la cooperación judicial, capacitación o cualquier otro acto que tenga similares propósitos.

No obstante, dichas regulaciones no solo no resultaban suficientes, sino que tampoco entraron de vigencia de manera inmediata, toda vez que en la Primera Disposición Complementaria- Disposición Final del Decreto Legislativo N°957 se estableció que entraría de manera progresiva en los diversos territorios del país, habiéndose fijado el 1 de febrero de 2006 como fecha de entrada vigencia en todo el país del Libro Séptimo del Código Procesal Penal.

Asimismo, y con la finalidad de que la Fiscalía de la Nación-Ministerio Público pueda realizar las funciones detalladas en el artículo 512 del Código Procesal Penal, con fecha 3 de febrero de 2006, mediante Resolución N°124-2006-MP-FN, se dispuso la creación de la Unidad de Cooperación Judicial Internacional y Extradiciones como unidad orgánica. Y, en el el artículo 106 del Reglamento de Organización y Funciones del Ministerio Público**,** se estableció que dicha Unidad es el órgano encargado de gestionar y realizar el seguimiento de los actos de cooperación jurídica internacional en materia penal y recuperación de activos, otorgándosele las siguientes funciones:

Función Normativa y Reguladora:

- Coadyuvar en la ejecución e implementación de la política internacional del Ministerio Público frente a los demás estados, con la finalidad de garantizar la operatividad de la cooperación jurídica internacional.

Función Administrativa y Ejecutora:

- Centralizar la coordinación y ejecución de todas las acciones reguladas por el Libro Séptimo del Código Procesal Penal.
- Coadyuvar en la ejecución e implementación de los mecanismos relativos al intercambio de pruebas e información, requeridos en virtud de los actos de cooperación jurídica internacional.
- Facilitar información a los organismos internacionales que tengan por finalidad la elaboración de instrumentos internacionales en materia de cooperación jurídica internacional penal y recuperación de activos.
- Gestionar las solicitudes de asistencia judicial en materia de cooperación jurídica internacional penal y recuperación de activos.
- Orientar a los operadores jurídicos en el libramiento de solicitudes de cooperación jurídica internacional penal y recuperación de activos.
- Coadyuvar en la recuperación de activos a nivel internacional, participando activamente en sus diferentes etapas.
- Coordinar con las autoridades competentes de otros estados en materia de cooperación jurídica internacional y recuperación de activos.
- Participar activamente en Mesas de Trabajo Interinstitucionales, que tengan por finalidad desarrollar temas sobre cooperación jurídica internacional en materia penal y recuperación de activos, la elaboración de iniciativas legislativas, Tratados Bilaterales, Memorándums Interinstitucionales, entre otras relacionadas a la materia.

No obstante, al advertirse que dichas funciones sólo se encontraban reguladas en un documento normativo interno del Ministerio Público, con fecha 29 de diciembre de 2016, se promulgó el Decreto Legislativo N°1281, en el que se efectuaron diversas modificaciones al Libro VII del Código Procesal Penal, así como se dotaron de mayores funciones a la Autoridad Central, estableciéndose:

- La comunicación directa con las Autoridades Centrales extranjeras
- La gestión y el seguimiento de las solicitudes de cooperación jurídica internacional.
- El cautelar los plazos y absolver consultas formuladas por las autoridades extranjeras y nacionales.
- La recepción y verificación de la presentación y el otorgamiento de las garantías diplomáticas solicitadas por el Poder Judicial y el Poder Ejecutivo.

- El realizar el seguimiento del cumplimiento de las garantías ofrecidas por el Estado peruano o el Estado requirente.
- El coadyuvar con las autoridades nacionales competentes para verificar el cumplimiento del ordenamiento jurídico internacional y el derecho nacional, en materia de cooperación jurídica internacional.

Es en mérito a dicha designación que la Unidad de Cooperación Judicial Internacional y Extradiciones desde el año 2006 viene encargándose de tramitar los siguientes actos de cooperación internacional: Extradiciones, solicitudes de asistencia judicial internacional, traslado de condenados, entregas vigiladas de bienes delictivos en el exterior, transmisión espontánea de información y denuncias internacionales, los cuales son cursados por los operadores jurídicos (jueces y fiscales) a nivel nacional[1], dentro del marco de sus competencias, así como los requerimientos que provienen de los Estados extranjeros[2].

Como se podrá apreciar, para el establecimiento de la Autoridad Central peruana se tomaron en consideración las recomendaciones de que esta recaiga en una sola entidad, siendo esta el Ministerio Público, por lo que la Fiscalía de la Nación es la que se encarga de efectuar el trámite de los actos de cooperación en el marco de las Convenciones Multilaterales; en el ámbito interamericano, para la Convención sobre Asistencia Mutua en Materia Penal (Convención de Nassau), Convención Interamericana contra la Corrupción; en el marco de las Naciones Unidas, para la Convención de las Naciones Unidas contra el Tráfico Ilícito de Estupefacientes y Sustancias Psicotrópicas (Convención de Viena), Convención de las Naciones Unidas contra la Corrupción (Convención de Mérida) y la Convención de las Naciones Unidas contra el Crimen Organizado Transnacional (Convención de Palermo); mientras que en el marco del Consejo de Europa, para el Convenio sobre Ciberdelincuencia (Convenio de Budapest).

Así como para las Convenciones bilaterales y cuando en ausencia de tratado se invoca el Principio de Reciprocidad.

---

[1] La Asistencia Judicial internacional
Artículo 536 del NCPP: *Corresponde a los jueces y fiscales, en el ámbito de sus respectivas atribuciones, cursar la carta rogatoria a las autoridades extranjeras. Ésta se tramitará por intermedio de la Fiscalía de la Nación*.

[2] Artículo 532 del NCPP: *La Fiscalía de la Nación cursará las solicitudes de asistencia de las autoridades extranjeras al juez de la investigación preparatoria del lugar donde deba realizarse la diligencia, que, en el plazo de dos días, decidirá acerca de la procedencia de la referida solicitud.*

2.2.1.1. Los actos de cooperación internacional

En el artículo 511 del Código Procesal Penal peruano (CPP) se encuentran detallados los actos de cooperación jurídica internacional, entre los cuales se encuentran la extradición, la asistencia judicial internacional, el traslado de condenados y la entrega vigilada de bienes delictivos.

En los artículos 513 al 527 del CPP se encuentra la regulación de la extradición, estableciéndose que la persona procesada, acusada o condenada como autor o participe que se encuentra en otro Estado, puede ser extraditada a fin de ser juzgada o de cumplir la sanción penal que le haya sido impuesta como acusada presente.

En los artículos 528 al 537 del CPP se encuentra la regulación de la asistencia judicial internacional, estableciéndose que sólo procederá cuando la pena privativa de libertad para el delito investigado o juzgado no sea menor de un año y siempre que no se trate de un delito sujeto exclusivamente a la legislación militar. Del mismo modo, en el artículo 511 CPP se efectúa un desarrollo de los tipos de requerimientos que pueden solicitarse mediante la asistencia judicial internacional, siendo los siguientes:

- Notificación de resoluciones y sentencias, así como de testigos y peritos
- Exhibición y remisión de documentos judiciales o copia de ellos
- Remisión de documentos e informes
- Realización de indagaciones o de inspecciones
- Examen de objetos y lugares
- Práctica de bloqueos de cuentas, embargos, incautaciones o secuestro de bienes delictivos, inmovilización de activos, registros domiciliarios, allanamientos, control de comunicaciones, identificación o ubicación del producto de los bienes o los instrumentos de la comisión de un delito, y de las demás medidas limitativas de derechos.
- Facilitar información y elementos de prueba

Y en los artículos 540 al 544-A del CPP, se encuentra la regulación del traslado de condenado.

Es en el marco de las funciones que ha venido realizando la Unidad de Cooperación Judicial Internacional y Extradiciones desde su entrada en funcionamiento hasta la fecha que se advirtió que la solicitud de asistencia judicial internacional es el acto que posee mayor cantidad de requerimientos (a diferencia de los demás actos de cooperación internacional conforme se verifica de la información estadística obtenida del sistema informático denominado SUCJIE perteneciente a dicha entidad y en el que se presenta el consolidado total de los pedidos activos y pasivos librados durante el año 2019 al 2021).

AÑOS	**ASISTENCIA JUDICIAL**	**EXTRADICIONES**	**TRASLADO DE CONDENADO**
2019	2388	370	151
2020	1251	217	99
2021	1560	263	34

Tabla 1. DATA ESTADÍSTICA DE CANTIDAD DE ACTOS DE COOPERACIÓN ATENDIDOS.

FUENTE: SISTEMA SUCJIE.

Siendo que el hecho de que las solicitudes de asistencia judicial internacional presenten mayor demanda se encuentra directamente vinculado con el tipo de información que puede obtenerse al utilizar dicho acto de cooperación.

Del mismo modo se puede apreciar que las solicitudes activas que libran las autoridades peruanas son las que más se requieren a diferencia de los pedidos pasivos, constante que se ha mantenido desde el 2019 hasta la fecha.

	2019	**2020**	**2021**
Asistencias judiciales activas	2188	1097	1401
Asistencias judiciales pasivas	200	154	159
Totales	2388	1251	1560

Tabla 2. DATA ESTADÍSTICA DE ASISTENCIAS JUDICIALES ACTIVAS Y PASIVAS. ELABORACIÓN PROPIA. FUENTE: SISTEMA SUCJIE.

Asimismo, es importante mencionar que, antes de la entrada en vigencia del Convenio de Budapest en el Perú, los diversos requerimientos de asistencias judiciales internacionales cursados con la finalidad de obtener información en el marco de investigaciones relativas a delitos informáticos se amparaban en su mayoría en los tratados bilaterales[3] y el caso de los pedidos librados a los Estados Unidos de América, país que concentra la mayor cantidad de proveedores de servicios, los requerimientos de asistencia judicial han sido realizados al amparo de la Convención Interamericana sobre Asistencia Mutua en Materia Penal, también conocida como Convención de Nassau, instrumento jurídico multilateral de la que tanto Estados Unidos de América y Perú son Estados Parte. Lo anteriormente señalado se aprecia de la información que se detalla a continuación y que se encuentra conformada por pedidos en trámite ante la Unidad de Cooperación Judicial Internacional, registrados a julio de 2020.

FECHA DE INGRESO	TRATADO INVOCADO	ACTO DE COOPERACIÓN SOLICITADO	ESTADO REQUERIDO
6/02/2018		Información sobre existencia de cuentas Facebook	
18/06/2018		Solicita información sobre cuentas Facebook	
23/07/2018		Solicita información y documentación sobre ciudadano norteamericano	
19/12/2018		Información de correos electrónicos Hotmail	
11/01/2019		Nombres de titulares cuentas Facebook	
14/01/2019		Solicita información sobre cuenta Facebook	

[3] Los países con los que el Perú cuenta con un Tratado Bilateral sobre asistencia jurídica en materia penal son: Argentina, Bolivia, Brasil, Canadá, China Colombia, Corea, Cuba, Ecuador, El Salvador, España, Francia, Guatemala, Italia, México, Paraguay, Panamá, República Dominicana, Confederación Suiza, Tailandia.

16/01/2019	Convenio de Nassau	Solicita información sobre cuentas Gmail	Estados Unidos de América
10/04/2019		Solicitud de información sobre cuentas Facebook	
27/05/2019		Solicita información sobre cuentas Facebook	
4/07/2019		Solicita información sobre cuentas Facebook	
17/09/2019		Solicita información sobre cuentas Facebook	
7/10/2019		Solicita información sobre cuentas Facebook	
4/11/2019		Solicita información sobre cuentas Facebook	
24/10/2019		Solicita información sobre cuentas Facebook	
9/12/2019		Solicita información sobre cuentas Facebook	

Tabla 3. SOLICITUDES DE ASISTENCIA JUDICIAL INTERNACIONAL EN TRÁMITE. FUENTE: SUCJIE.

Asimismo, del análisis de las solicitudes que fueron cursadas al Departamento de Justicia de los Estados Unidos, Autoridad Central estadounidense, se advierte que las solicitudes se encuentran conformados por entrega de información de suscriptor, tráfico y contenido de los proveedores Facebook, Microsoft y Google, los cuales en su mayoría han sido cursados en el marco de investigaciones por delitos comunes, conforme se aprecia de la información que se detalla a continuación:

NÚMERO DE ASISTENCIA	**DELITO**	**INFORMACIÓN REQUERIDA**
008-2013	Cohecho	Contenido de cuenta Hotmail (Microsoft)
119-2013	Extorsión	Suscriptor, tráfico y contenido de cuentas Hotmail (Microsoft)
603-2013	Extorsión	Suscriptor Facebook y tráfico (Google)
651-2013	Cohecho	Contenido de cuenta Hotmail (Microsoft)
566-2014	Suplantación de identidad	Suscriptor
590-2014	Acceso Ilícito	Suscriptor y Contenido

912-2014	Pornografía Infantil	Suscriptor y Tráfico
698-2014	Aborto consentido	Suscriptor (Facebook)
121-2015	Pornografía infantil	Suscriptor y tráfico (Facebook)
323-2015	Colusión	Contenido
1115-2015	Extorsión/AID/Pánico Financiero	Suscriptor, Tráfico y Contenido
03-2016	Colusión	Suscriptor, tráfico y contenido de cuentas (Hotmail, Gmail y 0utlook)
141-2016	Trata de personas	Suscriptor, tráfico y contenido de cuenta Gmail (Google)
646-2016	Trata de personas	Suscriptor, tráfico y contenido de cuenta Gmail (Google)
954-2016	Exhibiciones obscenas y publicaciones	Suscriptor (Facebook)
66-2017	Asociación ilícita	No precisa, genérico tuman.pe y (Hotmail)
111-2017	Proposiciones a niños, niñas y adolescentes	Suscriptor, Tráfico y Contenido
406-2017	Grave perturbación tranquilidad pública	Suscriptor, Tráfico y Contenido
769-2017	Extorsión	Suscriptor, tráfico y contenido de cuenta Facebook
1269-2017	Colusión	Contenido
1112-2018	Cohecho	Suscriptor y Contenido Hotmail y Gmail
637-2018	Estafa	Suscriptor y Tráfico
653-2018	Cohecho Activo	Suscriptor, Tráfico y Contenido
812-2018	Homicidio Calificado	Suscriptor y Contenido
1163-2018	Suplantación de identidad	Suscriptor y Tráfico
1057-2018	Colusión agravada	Contenido de cuenta Hotmail (Microsoft)
42-2019	Proposiciones a niños, niñas y adolescentes	Suscriptor, tráfico y contenido de cuentas Gmail (Google)
43-2019	Afiliación al terrorismo	Suscriptor y Contenido Facebook
381-2019	Patrocinio Ilegal	Tráfico
944-2019	Trata de personas	Suscriptor, tráfico y contenido de cuentas Facebook
1385-2019	Homicidio	Suscriptor, Tráfico y Contenido
1535-2019	Robo Agravado	Suscriptor, Tráfico y Contenido
1866-2019	Clonación o adulteración de terminales	Suscriptor
1968-2019	Trata de personas	Suscriptor, tráfico y contenido de cuenta Facebook
2096-2018	Tráfico ilícito de migrantes	Suscriptor, tráfico y contenido de cuentas Hotmail (Microsoft)
455-2020	Trata de Personas agravada con fines de explotación sexual	Suscriptor, Tráfico y Contenido
970-2020	Acoso	Contenido
1057-2020	Suplantación de identidad	Suscriptor y Tráfico
1065-2020	Cohecho pasivo específico y secuestro	Suscriptor y Contenido
299-2021	Suplantación de identidad	Suscriptor y Tráfico
301-2021	Estafa agravada	Suscriptor y Tráfico
302-2021	Apología al Terrorismo	Suscriptor y Tráfico

424-2021	Suplantación de identidad	Suscriptor
435-2021	Pornografía Infantil	Suscriptor y Tráfico
611-2021	Favorecimiento a la prostitución	Suscriptor, Tráfico y Contenido
612-2021	Favorecimiento a la prostitución	Suscriptor, Tráfico y Contenido
704-2021	Atentado contra la integridad de los sistemas informáticos	Datos de suscriptor

Tabla 4. SOLICITUDES DE ASISTENCIA JUDICIAL INTERNACIONAL POR INFORMACIÓN REQUERIDA. FUENTE: SUCJIE.

2.2.1.2. Los actos de cooperación internacional y el Convenio de Budapest

Luego de que el Convenio sobre Ciberdelincuencia entrara en vigor en el Perú desde el 01 de diciembre de 2019, la Unidad de Cooperación Judicial Internacional y Extradiciones advirtió que este no venía siendo invocado por los operadores jurídicos, por lo que en su calidad de Autoridad Central y de las funciones conferidas en la legislación procesal[4] cursó el oficio N°2170-2020-MP-GN-UCJIE, de fecha 05 de febrero de 2020, solicitando la difusión entre las Presidencias de los Distritos Fiscales a nivel nacional y recomendó su utilización con el fin de solicitar pedidos de asistencia judicial internacional en el marco de los delitos informáticos, así como para la obtención de evidencia digital.

a) Las solicitudes de asistencia judicial internacional

Durante el año 2020 no se recibió ningún pedido de asistencia judicial al amparo de la Convención sobre la Ciberdelincuencia[5]. En el año 2021 se libraron 27 solicitudes de asistencia judicial internacional, en su mayoría dirigidas a Estados Unidos de América y se recibieron 2 pedidos de República Dominicana; mientras que durante el año 2022[6], se libraron 62 solicitudes de asistencia judicial internacional activas, no habiéndose recibido ningún pedido pasivo en este año.

[4] Art. 512 CPP:
(…) 4. La Autoridad Central coadyuva con las autoridades nacionales competentes para verificar el cumplimiento del ordenamiento jurídico internacional y del derecho nacional, en materia de cooperación jurídica internacional.
[5] Difusión del Convenio mediante actividades de capacitación desde febrero a setiembre de 2021, así como la incorporación del Convenio de Budapest en la página web de la Unidad de Cooperación Judicial Internacional y Extradiciones, rubro formatos.
[6] El cierre de la data se efectuó al 30 de junio de 2022.

ASISTENCIAS JUDICIALES INTERNACIONALES- AÑO 2021		
PAIS	**TOTAL**	**INDICADOR**
Estados Unidos de América	23	
Argentina	1	
República Checa	1	
Irlanda	1	
Israel	1	Activa
República Dominicana	2	Pasiva

ASISTENCIAS JUDICIALES INTERNACIONALES- AÑO 2022		
PAIS	**TOTAL**	**INDICADOR**
Estados Unidos de América	54	
Francia	1	
Marruecos	1	
Malta	1	
Argentina	1	
Países Bajos	1	
Australia	1	
Alemania	1	
Polonia	1	Activa

Tabla 5. ASISTENCIAS JUDICIALES INTERNACIONALES. FUENTE: SISTEMA SUCJIE.

De la data presentada se verifica un mayor incremento de pedidos durante el año 2022 al amparo del Convenio sobre Ciberdelincuencia; se mantiene la constante de que los pedidos activos son mayores que los pasivos y que las autoridades peruanas (fiscales y jueces) dirigen la mayoría de sus requerimientos a los Estados Unidos de América. Actualmente las solicitudes de asistencia judicial internacional vienen siendo libradas para obtener información de suscriptor de cuentas de correo Gmail y de Twitter; para obtener información de tráfico y contenido de cuentas Facebook, así como de la plataforma Xvideos.

b) Las transmisiones espontáneas de información

Las autoridades fiscales peruanas han empezado a invocar las nuevas herramientas de la cooperación internacional, entre ellas, la denominada transmisión espontánea de información, técnica que viene permitiendo que nuestros operadores remitan información a las autoridades extranjeras con la finalidad de coadyuvar en sus investigaciones o para permitir que den a una investigación.

Durante el año 2021 se tramitaron 5 pedidos derivando información a los países de Chile, Argentina, Estados Unidos de América, Letonia y Costa Rica y se recibieron 3 pedidos de

Argentina y 1 de Costa Rica. En el año 2022 no existen registros de transmisiones activas ni pasivas.

c) Las Denuncias internacionales

Esta herramienta de cooperación constituye el procedimiento por el que las autoridades de un Estado y que se encuentran encargadas de la persecución penal, remiten las actuaciones que tienen a su cargo, a otro Estado, lo que se realiza con la finalidad de que los hechos ilícitos sean investigados y juzgados de acuerdo a la legislación de ese país[7],

Durante el año 2021 se tramitaron 4 denuncias internacionales a los países de Chile, Argentina, Estados Unidos de América y Letonia y se recibieron 2 denuncias por parte de las autoridades argentinas. En el año 2022 se advirtió un incremento en el uso de esta herramienta de cooperación al haberse tramitado hasta la fecha 8 denuncias internacionales dirigidas a los países de España, Estados Unidos de América, Marruecos, Colombia, Reino Unido y se han recibido 4 denuncias internacionales de los países de Argentina, Canadá y Portugal.

2.2.1.3. Las solicitudes de conservación de datos al amparo de la Red 24/7

Desde el año 2019 y en mérito a lo dispuesto mediante las Resoluciones de Fiscalía de la Nación[8], los puntos de contacto de la Red 24/7 del Convenio sobre la Ciberdelincuencia recaen en funcionarios la Unidad de Cooperación Judicial Internacional y Extradiciones, quienes en virtud de las funciones conferidas en el artículo 35 han tramitado las solicitudes de conservación de datos, medida que se justifica por la alta volatibilidad de los datos

[7] En el caso peruano, esta facultad tiene como base el artículo 1) del Código Penal peruano aborda el Principio de territorialidad, señalando: "*La Ley Penal Peruana se aplica a todo el que comete un hecho punible en el territorio de la República".* Asimismo, de conformidad con el numeral 1 del artículo 21 del Código Procesal Penal, la competencia por razón del territorio se establece en el siguiente orden: Por el lugar donde se cometió el hecho delictuoso o se realizó el último acto en caso de tentativa, o cesó la continuidad o la permanencia del delito.

[8] Resolución de Fiscalía de la Nación N°3492-2019-MP-FN, de fecha 09 de diciembre de 2019, mediante el cual se dispuso designar a Lizet Rodriguez Rocha como punto focal alterno del Ministerio Público ante la RED 24/7 en el marco del Convenio de Ciberdelincuencia.
Resolución N°920-2020-MP-FN, de fecha 25 de agosto de 2020, mediante el cual se dispuso designar a Rocío Gala Gálvez, Fiscal Superior y Jefa de la Oficina de Cooperación Judicial Internacional y Extradiciones, como punto de contacto titular del Ministerio Público para la Red 24/7 en el marco del Convenio sobre la Ciberdelincuencia y a Lizet Rodriguez Rocha, Fiscal Adjunta Provincial de la Oficina de Cooperación Judicial Internacional y Extradiciones, como punto de contacto alterno del Ministerio Público para la Red 24/7 en el marco del Convenio sobre la Ciberdelincuencia.

informáticos y que tiene como finalidad realizar el aseguramiento de información que se encuentran almacenada en un sistema informático y respecto de los cuales, posteriormente se requerirá su revelación[9].

Respecto de los pedidos activos, durante el año 2021 se tramitaron 36 solicitudes de conservación de datos, los que constituyeron requerimientos cursados a los proveedores de servicios tales como Google, Amazon, Apple, Xvideos, Wix, entre otros, para lo cual contó con la cooperación de los países Estados Unidos de América, Malta, Singapur, Finlandia, España, Israel, República Checa, entre otros, quienes atendieron con prontitud este tipo de requerimientos.

Durante el año 2022, se tramitaron 20 pedidos de conservación de datos los cuales han sido dirigidos a los países de la República Francesa, Estados Unidos de América, República de Chipre y la República de Singapur.

Con relación a los pedidos pasivos**,** durante el año 2021 se recibieron 02 solicitudes de conservación de datos provenientes de los países de Argentina y de República Checa, quienes solicitaron la conservación de datos de IPS administradas por las empresas de telefonía.

2.3. Análisis de las respuestas brindadas por los proveedores de servicios peruanos

En el marco del trámite de las asistencias judiciales internacionales pasivas en las que se solicitó **identificar a los titulares de direcciones IP´s,** se pudo advertir diversas respuestas de índole negativa por parte de las empresas concesionarias de servicios de telefonía, las cuales se señalan a continuación:

EMPRESA DE TELEFONÍA	RESPUESTA BRINDADA
Telefónica	Telefónica mediante el oficio TSP-83030000-LMP-723-2018-C-F, informó sobre la imposibilidad de brindar la información por no tener registrado en su sistema la titularidad de los clientes.

[9] La revelación de la información se producirá a través de la solicitud de asistencia judicial internacional.

Telefónica	Telefónica mediante oficio TSP-83030000-EHC-1123-2019-C-F, de fecha 21 de enero de 2020 informó no tener registrado la titularidad de los clientes, por cuanto corresponde a conexiones BAM (Banda Ancha Móvil). Y que no es posible determinar el nombre de usuario en la fecha y horas solicitados, toda vez que estas pertenecen a redes correspondiente a la plataforma de red CGNAT, cuya IP es pública.
Bitel	El Departamento legal de la compañía Bitel informó que no era posible remitir la información requerida toda vez que la dirección IP corresponde a una IP pública.

Asimismo, en el marco del trámite de los pedidos de conservación de datos en mérito a la Red 24/7 del Convenio sobre la Ciberdelincuencia, se recibieron respuestas de índole negativa, las cuales se reseñan a continuación:

EMPRESA DE TELEFONÍA	**RESPUESTA BRINDADA**
Telefónica	La empresa Telefónica informó el 16.09.2020, mediante oficio N°TSP-83030000-OCR_4208_2020_CF que no contaban con el registro de identificación de los titulares a los que se le asignaron las direcciones IP toda vez que correspondían a servidores CGNAT.
Entel	Entel informó mediante carta N°SDI-5153/20, de fecha 23.10.2020 que no contaban con un sistema técnico que pueda brindar reportes de IP´s, por lo que les resultaba técnicamente imposible resguardar y brindar la información relacionada a

	la titularidad de IP´s solicitadas. Asimismo, señalaron que de acuerdo al marco normativo vigente dispuesto mediante Resolución de Consejo Directivo de OSIPTEL N°123-2014-CD-OSIPTEL, a través del cual se aprobó el Reglamento General de Calidad de los Servicios Públicos de Telecomunicaciones, las empresas supervisadas, como en su caso, únicamente se encuentran obligadas a conservación la información por un periodo de al menos tres meses, concluyendo, entre otros, que debido a la antigüedad de la información se encontraban impedidos de cumplir con lo solicitado.
Telefónica	La empresa Telefónica respondió mediante oficio N°TSP-83030000OCR_9827_11409_10753_ 10825_2021_C_F, de fecha 23.11.2021, indicando que la dirección IP tiene como característica ser una dirección con tecnología CGNAT, y que no cuentan con un registro individualizado de conexión de dichos usuarios.

De las respuestas detalladas se puede apreciar que los proveedores de telefonía que prestan servicios en el Perú no vienen cumpliendo con la obligación de almacenar la información de los titulares a quienes brindan servicios de internet, ya que desde hace varios años a tras hasta la fecha, continúan aduciendo problemas de índole técnico para no guardar dicha titularidad, amparándose en que se tratan de IP Públicas[10], conexiones BAM[11], redes CGNAT[12] o el no

[10] En referencia a la que asigna el proveedor de internet y que visualizaremos cuando nos conectemos a la red.
[11] Hace referencia a un servicio de banda ancha móvil, es decir, servicio de internet móvil con elevada capacidad para transportar información.
[12] Por sus siglas Carrier-Grade NAT y hace referencia a la conexión a internet de varios equipos utilizando una dirección IP.

contar con sistema técnico de reporte de IP´, información que brindan después de varios meses de recibido los requerimientos.

Al respecto, debemos hacer hincapié que el Organismo Supervisor de Telecomunicaciones peruano, OSIPTEL, mediante el oficio N°00033-GG/2022, de fecha 10 de enero de 2022, informó que, si bien la norma no hace referencia a una forma específica de conservar y consultar la información sobre los IP, **sí establece la obligación de llevar un registro y conservarlo**. Asimismo, indicaron que las empresas deben disponer de todos los mecanismos y herramientas necesarias con el fin de contar con los registros completos, considerando todos los niveles de jerarquías existentes para las direcciones IP´s tanto privadas como públicas, siendo que de la casuística presentada se verifica que las empresas de telefonía no se encuentran cumpliendo con dicha obligación. Esta situación representa actualmente un verdadero problema, ya que no permite brindar apoyo a las autoridades extranjeras, con lo que el Perú no viene siendo recíproco en la atención de este tipo de pedidos, ya que por parte de las autoridades extranjeras si se recibe respuesta ya sea mediante el trámite de solicitudes de asistencia judicial internacional o a través de los pedidos de conservación de datos por intermedio de la Red 24/7.

Con relación a la demora en la respuesta por parte de los proveedores de servicios, de acuerdo a lo señalado por los representantes de las empresas Telefónica, Claro, Entel y Bitel esto se debe a que no existe una distinción entre los requerimientos que provienen a nivel nacional, relacionados con medidas limitativas de derechos, y los requerimientos que provienen de las autoridades extranjeras (solicitudes de asistencia judicial internacional y pedidos de conservación de datos informáticos), ya que no solo existe una única mesa de partes virtual para el envío de todos los pedidos, sino que tampoco poseen criterios de distinción para establecer su atención prioritaria.

Asimismo, advertimos una problemática adicional y que resulta más perjudicial, ya que las empresas de telefonía se ampararon en la Resolución de Consejo Directivo de OSIPTEL para indicar que únicamente se encuentran obligadas a retener información por un periodo de al menos tres meses, y si bien de la revisión del artículo 11 de la Resolución de Consejo Directivo de OSIPTEL N°123-2014-CD-OSIPTEL, se advierte la obligación de las empresas proveedoras de conservar por un periodo mínimo de 3 meses, los registros de asignaciones de direcciones IP públicas y privadas asociadas al servicio de acceso a internet del usuario, de forma estática o dinámica, también lo es que dicho periodo de retención para los casos provenientes de la

cooperación judicial internacional resulta insuficiente. Ello es así por cuanto en los pedidos que provienen de jurisdicciones extranjeras, muchas veces el trámite interno previo hasta la llegada a nuestro país toma un par de meses[13], por lo que somos de la opinión que resulta necesario efectuar una modificación normativa con la finalidad de ampliar el periodo de retención de este tipo de información, tal y como ocurre con la retención de la información realizada con la tasación, los registros fuentes del detalle de las llamadas y facturación de los servicios de telefonía, en la que se establece un plazo mayor, en dicho caso se establece un periodo de al menos 3 años, conforme se encuentra regulado en el numeral 6 del artículo 16 de la Ley N°27336, Ley de Desarrollo de las Funciones y Facultades del Organismo Supervisor de Inversión Privada en Telecomunicaciones – OSIPTEL.

2.3.1. Propuestas de solución

Una de las principales propuestas de solución para poder cumplir con el compromiso del Perú con relación al Convenio sobre la Ciberdelincuencia **es** realizar modificaciones en nuestra normativa procesal penal con el fin de lograr la incorporación de las medidas reguladas en el Capítulo III del Convenio, entre los que nos centramos principalmente en la regulación de la medida de conservación de datos informáticos, para lo cual proponemos tomar como base el artículo 588 octies de la Ley de Enjuiciamiento Criminal española, proponiendo la siguiente regulación:

Medida de conservación de datos

El Fiscal podrá requerir a cualquier persona física o jurídica la conservación de datos o información incluida en un sistema informático de almacenamiento que se encuentre a su disposición hasta que se realice el procedimiento correspondiente para su cesión.

Los datos se conservarán por un periodo máximo de noventa días, prorrogable hasta un máximo de ciento ochenta días.

El requerido está obligado a prestar su colaboración de manera célere y a guardar secreto del desarrollo de la diligencia, quedando sujeto a responsabilidad.

[13] Al respecto, y debido a que Autoridad Central recibe requerimientos provenientes de países extranjeros, en uno de los casos provenientes de Argentina, se advirtió que desde la comisión de los hechos hasta la remisión de la solicitud al Perú transcurrieron un aproximado de 7 meses.

Con relación a la retención de datos, tomando en consideración que en América Latina se cuenta con la experiencia de los países de Chile[14] y Brasil[15], en cuyos casos se advierten que los periodos de retención de datos son por un plazo no inferior a un año, por lo que se propone una modificación del artículo 11 de la Resolución de Consejo Directivo de OSIPTEL N°123-2014-CD-OSIPTEL, con el fin de lograr su ampliación de 3 meses a 1 año, recordemos que a nivel nacional este periodo de 1 año, ya se encuentra consignado en el marco del Decreto Legislativo N°1182, en el que se estableció que los concesionarios de servicios públicos de telecomunicaciones y las entidades públicas deban retener los datos derivados de las telecomunicaciones durante los primeros doce (12) meses en sistemas informáticos, por ello somos de la opinión que esta propuesta de ampliación también debe aplicarse para las IPs, ya que este nuevo plazo que permitiría que los casos provenientes de cooperación internacional puedan ser atendidos.

Con relación a la falta de registro de titularidades de IP, proponemos que se adopten no solo las medidas sancionatorias administrativas correspondientes, sino que se incorpore en nuestra legislación procesal penal un artículo de deber de colaboración, ello con la finalidad de que las empresas cumplan con su obligación de mantener un registro completo considerando las direcciones IP´s privadas y públicas, por cuanto la no existencia de un registro dificulta el avance de las investigaciones, para ello proponemos tomar como base el artículo 588 ter e de la Ley de Enjuiciamiento Criminal española:

Deber de colaboración

Todos los proveedores de servicios de las telecomunicaciones, de acceso a una red de telecomunicaciones o de servicios de la sociedad de información, así como toda persona

[14] Art. 222 CPP chileno: "(…) Las empresas telefónicas y de comunicaciones deberán dar cumplimiento a esta medida, proporcionando a los funcionarios encargados de la diligencia las facilidades necesarias para que se lleve a cabo con la oportunidad con que se requiera. Con este objetivo los proveedores de tales servicios deberán mantener, en carácter reservado, a disposición del Ministerio Público, un listado actualizado de sus rangos autorizados de direcciones IP y un registro, **no inferior a un año**, de los números IP de las conexiones que realicen sus abonados".

[15] Resolución Nº738, de 21 de diciembre de 2020: Art. 65-J. Para garantizar la inspección y el seguimiento permanente de las obligaciones legales y reglamentarias, los proveedores deben mantener a disposición de ANATEL los datos relacionados con la prestación del servicio, incluidos, en su caso y en cumplimiento de las normas pertinentes:
(…) II - Registros de conexión a Internet por un **período mínimo de 1 (un) año** en servicios que permitan la conexión a Internet.

que de cualquier modo contribuya a facilitar las comunicaciones a través del teléfono o de cualquier otro medio o sistema de comunicación, están obligados a prestar la asistencia y colaboración necesaria a los operadores jurídicos designados para la prácticas de las medidas relativas con la conservación e intervención de las comunicaciones.

Asimismo, se propone que las empresas operadoras de servicios creen un canal exclusivo de atención de los pedidos de asistencia judicial internacional, con la finalidad que estas sean atendidas brindando la prioridad debida, en especial cuando se tratan de solicitudes de conservación de datos informáticos, las que por su naturaleza deben ser atendidas de manera célere, toda vez que la demora en su atención podría traer perjuicios irreparables.

Del mismo modo, se propone efectuar capacitaciones para lograr cambios en la estrategia de investigación fiscal, con el fin de que los operadores jurídicos puedan requerir cooperación internacional en el momento oportuno, apenas adviertan el componente de carácter internacional y no como se viene realizando actualmente, en lo que muchas veces formulan la solicitud de asistencia judicial cuando se encuentran a menos de un mes para el vencimiento del plazo de su investigación.

Así también, se propone efectuar la difusión del empleo de las redes internacionales en materia de ciberdelincuencia: Red 24/7 del Convenio de Budapest, la que por su propia naturaleza actúa de manera célere con el fin de apoyar a los operadores jurídicos en la conservación de datos informáticos, medida de vital importancia ante la alta volatilidad de los datos informáticos.

2.4. Avances y desafíos en el marco de la cooperación internacional y la ciberdelincuencia

En el marco de las labores ejercidas por la Autoridad Central peruana se han venido realizando diversas acciones con la finalidad de coadyuvar en la mejor formulación de los actos de la cooperación jurídica internacional, por lo que siguiendo las plantillas elaboradas por el Consejo de Europa se elaboraron diversos formatos, entre los que se destacan la solicitud de

asistencia judicial internacional en el marco de la ciberdelincuencia[16] y el formato de solicitud de conservación de datos al amparo de la Red 24/7[17].

Asimismo, se elaboraron diversos productos, entre los que destaca la Guía práctica para requerir información a proveedores internacionales de servicios de internet[18], documento difundido en los 34 Distritos Fiscales y mediante el cual se informa sobre los diversos niveles de información en el marco de la ciberdelincuencia (información de suscriptor, de tráfico y de contenido), el procedimiento para requerir información de suscriptor de manera directa a través de las plataformas elaboradas por los proveedores internacionales. Este documento resultó de vital importancia por cuanto se advirtió que los fiscales vienen requiriendo información de suscriptor de manera directa a través de las plataformas LERS[19], lo cual resulta positivo, por cuanto antes de su difusión un aproximado del 85.4% de los pedidos de asistencia judicial dirigidos a Estados Unidos de América se encontraban conformados por requerimientos para obtener información de suscriptor, los cuales tardaban más de seis meses en ser atendidos por dichas autoridades[20], aunado al hecho que implicaba un mayor gasto para el Ministerio Público por cuanto estos pedidos debían ser previamente traducidos al idioma inglés antes de su remisión a la autoridad extranjera[21]. Actualmente, y de acuerdo con la información proporcionada a la Unidad de Cooperación por diversos fiscales a nivel nacional, se tomó conocimiento que se viene obteniendo respuesta en un aproximado de 21 días[22], lo cual no solo coadyuva con el avance de las investigaciones fiscales, sino que también permite la descarga de las solicitudes de asistencia judicial internacional en la Unidad de Cooperación Judicial Internacional.

---

[16] Documento que puede ser hallado en el siguiente link: https://www.gob.pe/institucion/mpfn/informes-publicaciones/2117459-formato-de-solicitud-de-asistencia-judicial-en-el-marco-de-la-ciberdelincuencia

[17] Documento que puede ser hallado en el siguiente link: https://www.gob.pe/institucion/mpfn/informes-publicaciones/1977383-solicitud-de-conservacion-de-datos

[18] Documento que puede ser hallado en el siguiente link: https://cdn.www.gob.pe/uploads/document/file/1707041/GUI%CC%81A%20PRA%CC%81CTICA%20PARA%20REQUERIR%20INFORMACIO%CC%81N%20A%20PROVEEDORES%20INTERNACIONALES%20%20DE%20SERVICIOS%20DE%20INTERNET.pdf.pdf

[19] Dirigidas a las autoridades de cumplimiento de la ley (policiales, fiscales y jueces).

[20] Data obtenida de un universo de 48 pedidos de asistencia judicial internacional librados a Estados Unidos de América y que cuyo análisis fue elevado a la jefatura de la UCJIE mediante el informe N°04-2021-UCJIE-LNRR.

[21] Artículo 509 CPP:

4. Corresponderá a la autoridad central, en coordinación con el Ministerio de Relaciones Exteriores, traducir las solicitudes y la demás documentación que envíen las autoridades peruanas a las extranjeras.

[22] Con referencia a la información de suscriptor proporcionada por Facebook.

También se cuenta con El Boletín Informativo N°01, denominado ""La conservación de datos informáticos, el uso de las Redes Internacionales 24/7 y G7, y la solicitud de asistencia judicial internacional en el marco de la ciberdelincuencia", documento en el que se efectúa un desarrollo sobre las redes internacionales, los rubros que debe contener un pedido de asistencia judicial internacional en el marco de la ciberdelincuencia, así como el tipo de fundamentación que se debe efectuar al momento de redactar una solicitud de asistencia judicial para cumplir con los estándares requeridos por las autoridades de los Estados Unidos de América, toda vez que éste país posee diferentes estándares de acuerdo al tipo de información que se va a requerir.

Todos estos pequeños esfuerzos han venido coadyuvando en la mejora de los trámites de la cooperación internacional activas. No obstante, como parte de los desafíos pendientes se encuentran el efectuar las modificaciones normativas para incluir las regulaciones del Convenio sobre Ciberdelincuencia, entre las que destacamos la conservación de datos y el establecimiento que la información sea conservada por 90 días, así como lo referente a la ampliación del plazo del periodo de retención de datos de 3 meses a 1 año, las cuales permitirían efectuar mejoras en el trámite de las solicitudes pasivas de asistencia judicial internacional y la solicitudes de conservación de datos y que deberían de ir de la mano con el mayor compromiso de los operadores de telefonía para establecer un sistema de registro de los titulares de IP´s.

3. Conclusiones

En ese sentido, del trabajo desarrollado podemos concluir que resulta necesario que el Perú efectúe diversas acciones con el fin de permitir la lucha efectiva y eficaz ante los ciberdelitos, cobrando vital importancia el aspecto de la cooperación internacional, toda vez que, debido a la transnacionalidad de los ciberdelitos, esta medida permite a las autoridades obtener evidencia en territorio extranjero. De manera concreta, podemos llegar a las siguientes conclusiones:

PRIMERA. – En el marco sustantivo se advierte que nuestra normativa de Ley de Delitos Informáticos cumple con la regulación establecida en la Convención sobre la Ciberdelincuencia, ya que contamos con tipos penales que ya se encuentran reconocidos en el citado Convenio.

SEGUNDA. – En el marco procesal se advierte que la legislación procesal peruana no ha tenido muchos cambios, por lo que necesita contar con modificaciones normativas con la finalidad de dotar de mejores técnicas especiales de investigación, entre ellas del agente encubierto informático, así como establecer medidas de acceso remoto, entre otras, que permitan a los operadores jurídicos luchar de manera eficaz contra la ciberdelincuencia.

TERCERA. - En el marco de la cooperación internacional no se han efectuado cambios normativos con la finalidad de incorporar las medidas reguladas en el capítulo III de la Convención sobre Ciberdelincuencia, por lo que se propone incorporar al Código Procesal Penal la medida de conservación de datos informáticos siguiendo la experiencia española.

CUARTA. – El trámite de las solicitudes de asistencia judicial internacional pasivos relacionados con la identificación de IP´s presentan como problemática que la atención no se realiza de manera célere por parte de los proveedores de servicios de telefonía, lo que se encuentra relacionado con la existencia de un mismo canal de recepción de los pedidos de cooperación internacional y de las solicitudes nacionales relacionadas con el trámite de medidas limitativas.

QUINTA.- Otro de los problemas advertidos en cuanto al trámite de las solicitudes de asistencia judicial internacional pasivos relacionados con la identificación de IP´s lo encontramos en el corto plazo establecido para la retención de datos informáticos por parte de las empresas de telefonía, el que al ser de 3 meses no resulta suficiente cuando se tratan de requerimientos provenientes del extranjero.

SEXTA.- Otro de los problemas advertidos en cuanto al trámite de las solicitudes de asistencia judicial internacional pasivos relacionados con la identificación de IP´s lo encontramos en el hecho de que los proveedores de servicios no cumplen con su obligación de establecer un registro de los titulares de IP, lo que origina que se brinden respuestas negativas sin lograr la identificación de la persona a la que se viene prestando servicios y que resulta de interés para las autoridades extranjeras.

SÉPTIMA. - El trámite de las solicitudes de conservación de datos informáticos presentan como problemática que la atención no se realiza de manera célere por parte de los proveedores de servicios de telefonía, lo que se encuentra relacionado con la existencia de un mismo canal de recepción de este tipo de requerimientos y de las solicitudes nacionales relacionadas con el trámite de medidas limitativas, lo que viene impidiendo su atención de manera célere tal y como lo establece la Convención.

OCTAVA. – Existe escasa colaboración por parte de las empresas privadas en nuestro país con el fin de brindar una respuesta ante requerimientos de países extranjeros en el marco de la cooperación jurídica internacional.

NOVENA.- Referente a la actuación de los órganos estatales, se advierte la ausencia de una clara conceptualización clara y diferenciación entre los conceptos de retención y conservación de datos informáticos, puesto que se utiliza el término de conservación para hacer referencia al periodo previo de almacenamiento de información.

DÉCIMA.- Se advierte el desconocimiento por parte de los operadores jurídicos nacionales sobre la importancia del uso de las redes internacionales en materia de ciberdelincuencia, la que posee bondades importantes respecto a la medida de conservación de datos informáticos, así como la posibilidad de obtener información de otros países, siempre que su legislación lo permita.

DÉCIMA PRIMERA- No se advierte una adecuada estrategia fiscal en las investigaciones de ciberdelincuencia por cuanto no se requiere de manera célere la medida de conservación de datos informáticos, así como tampoco se efectúa la formulación de solicitudes de asistencia judicial internacional desde el primer momento que se advierte el componente internacional en una investigación de esa naturaleza, habiéndose advertido que muchas veces los pedidos son librados a pocos días del vencimiento de la investigación.

Referencias bibliográficas

Bibliografía básica

BRAMONT-ARIAS TORRES, L. *El delito informático en el Código Penal peruano*. Lima: Fondo Editorial de la Pontificia Universidad Católica del Perú, 1997.

CASTELLO CRUZ, L. Informe nacional. En: Cooperación Interamericana en los Procedimientos Penales. [en línea]. 1983, p. 81 [Consulta: junio de 2022]. Disponible en: file:///C:/Users/LIZET/Downloads/15425-Texto%20del%20art%C3%ADculo-61225-1-10-20161004%20(2).pdf

DIAZ GOMEZ, A. «El delito informático, su problemática y la cooperación internacional como paradigma de su solución: El Convenio de Budapest». *Revista electrónica de Derecho de la Universidad de La Rioja*, REDUR, 2010, Nº.8, pp. 169-203. [Consulta: abril de 2022]. ISSN-e 1695-078X, Disponible en: https://publicaciones.unirioja.es/ojs/index.php/redur/article/view/4071/3321

GOICOCHEA, I. Nuevos desarrollos en la cooperación jurídica internacional en materia civil y comercial. [en línea]. 2016, pp. 128. [Consulta: junio de 2022]. Disponible en: https://www.corteidh.or.cr/tablas/r36039.pdf

MORÁN MARTINEZ, R. Nuevas tendencias de la cooperación judicial internacional fuera de la UE. [en línea]. 2015. pp. 04. [Consulta: junio de 2022]. Disponible en: https://docplayer.es/18497241-Nuevas-tendencias-de-la-cooperacion-judicial-internacional-fuera-de-la-ue-rosa-ana-moran-martinez-fiscal-de-sala-de-cooperacion-internacional.html

PEREYRA MAITA, L.A y TURPO HINOSTROZA, J.A. Instrumentos normativos que se deben adecuar en nuestra legislación según el marco del Convenio de Budapest como mecanismo legal de protección a la intimidad personal frente a las TICS. Universidad Tecnológica del Perú. Facultad de Derecho y Ciencias Humanas, Lima, 2020. [Consulta: abril de 2022]. Disponible en:https://repositorio.utp.edu.pe/bitstream/handle/20.500.12867/3579/Luz%20Pereyra_Jessy%20Turpo_Trabajo%20de%20Investigacion_Bachiller_2020.pdf?sequence=1&isAllowed=y

RIQUET M. Mercosur: Estado de la legislación contra la delincuencia informática en el Mercosur. [en línea]. 2008. p.2. [Consulta: junio de 2022]. Disponible en: https://perso.unifr.ch/derechopenal/assets/files/articulos/a_20080526_88.pdf

ROJAS VARGAS, F. *Derecho Penal. Parte Especial*. 3° ed. Lima: Grijley, 2000.

SALINAS SICCHA, R. *Curso de Derecho penal peruano. Parte especial III*. 2° ed. Lima: Idemsa, 2006.

TEMPERINI, M. «Delitos Informáticos en Latinoamérica: Un estudio de derecho comparado». Buenos Aires: Simposio Argentino de informática y derecho. 2014. Disponible en: https://43jaiio.sadio.org.ar/proceedings/SID/13.pdf

VELASCO SAN MARTIN, C. «El derecho y la jurisdicción aplicable en materia de conductas delictivas cometidas en internet a la luz del convenio sobre ciberdelincuencia del Consejo de Europa con un particular enfoque en México y países de Latinoamérica». Universidad Carlos III de Madrid. Departamento de Derecho Penal, Procesal e Historia del Derecho, Madrid, 2011. [Consulta: abril de 2022]. Disponible en: https://researchportal.uc3m.es/individual/act374388

Bibliografía complementaria

CONGRESO DE LA REPÚBLICA DEL PERÚ. Diario de los Debates. (2014, febrero). *Comisión permanente- Octava sesión*. Lima, Perú. [Consulta: abril de 2022]. Disponible en: https://www.congreso.gob.pe/diariodebates/diariodebates/

----------*Informe explicativo del Primer Protocolo Adicional a la Convención en Cibercrimen, respecto de la criminalización de actos de naturaleza racista y xenofóbica cometidos a través de sistemas de ordenador.* Consejo de Europa. 2003. Disponible en: https://rm.coe.int/16800d37ae

----------. *Informe explicativo sobre el Segundo Protocolo Adicional al Convenio destinado a mejorar la cooperación y la divulgación de pruebas electrónicas.* Consejo de Europa. 2022. Disponible en: https://rm.coe.int/special-edition-second-protocol-en-2021/1680a69930

GOICOCHEA, C. *Informe jurídico N°01-2019, relativo a la propuesta para la designación de Fiscalías Especializadas en Delitos Informáticos.* (Informe inédito). UCJIE. 2019.

Legislación citada

Convenio (numero 185) relativo al Convenio sobre la Ciberdelincuencia adoptado en Budapest el 23 de noviembre de 2001. Disponible en: https://www.oas.org/juridico/english/cyb_pry_convenio.pdf

Decreto Legislativo N°635 del 08 de abril de 1991. Código Penal peruano. Diario Oficial El Peruano. Disponible en: https://spij.minjus.gob.pe/spij-ext-web/detallenorma/H682692

Decreto Legislativo N°957 del 29 de julio de 2004. Código Procesal Penal peruano. Diario Oficial El Peruano. Disponible en: https://spij.minjus.gob.pe/spij-ext-web/detallenorma/H682695

Decreto Legislativo N°1281. Diario Oficial El Peruano. 28 de diciembre de 2016. Disponible en: https://busquedas.elperuano.pe/normaslegales/decreto-legislativo-que-modifica-el-codigo-procesal-penal-re-decreto-legislativo-n-1281-1468461-2/

Decreto Supremo N°010-2019-RE, relativo a la ratificación del Convenio sobre la Ciberdelincuencia. Diario Oficial El Peruano. 10 de marzo de 2019. Disponible en: https://busquedas.elperuano.pe/download/url/ratifican-el-convenio-sobre-la-ciberdelincuencia-decreto-supremo-n-010-2019-re-1748338-2

Real Decreto de 14 de setiembre de 1982 por el que se aprueba la Ley de Enjuiciamiento Criminal. Boletín Oficial del Estado. 17 de setiembre de 1882, núm 260. Disponible en: https://www.boe.es/buscar/act.php?id=BOE-A-1882-6036

Ley N° 27309 relativo a la modificación del Título V del Libro Segundo del Código Penal, promulgado por Decreto Legislativo Nº635. 17 de julio del 2000. Diario Oficial El Peruano. Disponible en: https://cdn.www.gob.pe/uploads/document/file/356824/NORMA_1887_Ley_27309.pdf

Ley 30096 relativo a la Ley de los Delitos Informáticos. 22 de octubre de 2013. Diario Oficial El Peruano. Disponible en: https://busquedas.elperuano.pe/normaslegales/ley-de-delitos-informaticos-ley-n-30096-1003117-1/

Ley 30171 relativo a la Ley que modifica la Ley 30096, Ley de Delitos Informáticos. Diario Oficial el Peruano. 10 de marzo de 2014. Disponible en: https://www.gob.pe/institucion/minsa/normas-legales/197055-30171

Ley N°27336, Ley de Desarrollo de las Funciones y Facultades del Organismo Supervisor de Inversión Privada en Telecomunicaciones – OSIPTEL. Sistema de Información Jurídica. Disponible en: https://cdn.www.gob.pe/uploads/document/file/971580/Ley_N__27336.PDF

Primer Protocolo Adicional a la Convención en Cibercrimen, respecto de la criminalización de actos de naturaleza racista y xenofóbica cometidos a través de sistemas de ordenador (STE N° 189), adoptado en Estrasburgo el 28 de enero de 2003. Disponible en: https://www.plataformaong.org/conferencia/wp-content/uploads/2014/10/Protocolo_adicional_convencion_cibercrimen.pdf

Resolución de Consejo Directivo de OSIPTEL N°123-2014-CD-OSIPTEL, relativo al reglamento General de Calidad de los Servicios Públicos de Telecomunicaciones. 10 de octubre de 2014. Disponible en: https://cdn.www.gob.pe/uploads/document/file/1530135/N%C2%BA%20123-2014-CD/OSIPTEL%C2%A0.pdf

Segundo Protocolo Adicional al Convenio destinado a mejorar la cooperación y la divulgación de pruebas electrónicas (CETS N° 224), adoptado en Estrasburgo el 12 de mayo de 2022. Disponible en: https://rm.coe.int/1680a49dab

Jurisprudencia

Sentencia del 5 de abril de 2022, Commissioner of the Garda Siochána y otros, C-140/20, EU:C:2022:258, apartado 129. Disponible en: https://curia.europa.eu/juris/document/document_print.jsf?docid=257242&text=&dir=&doclang=ES&part=1&occ=first&mode=lst&pageIndex=0&cid=4540876

.

Listado de abreviaturas

COE	Consejo de Europa
CPP	Código Procesal Penal
LECRIM	Ley de Enjuiciamiento Criminal
IP	Internet protocol
UCJIE	Unidad de Cooperación Judicial Internacional y Extradiciones
OSIPTEL	Organismo Supervisor de Inversión Privada en Telecomunicaciones