Cibercrimen:

DESAFÍOS DE LA ARMONIZACIÓN DE LA CONVENCIÓN DE BUDAPEST EN EL SISTEMA PENAL PARAGUAYO

Maricarmen Sequera
& Marlene Samaniego *

Esta investigación fue producida en el marco del proyecto “Grupo de trabajo sobre Ciberseguridad en América Latina”, gracias al trabajo conjunto de las organizaciones Hiperderecho (Perú), IPANDETEC (Panamá), Fundación Karisma (Colombia), Red en Defensa de los Derechos Digitales (México) y TEDIC (Paraguay),bajo la coordinación de Derechos Digitales, y gracias al apoyo de Ford Foundation.

Grupo de trabajo sobre Ciberseguridad en América Latina
Coordinación: Marianne Díaz, *Derechos Digitales*

Investigación:
Martín Borgioli y Carlos Guerrero, *Hiperderecho*
Sara Frati, Lía Hernández y Diego Morales, *IPANDETEC*
Juan Diego Castañeda y Amalia Toledo, *Karisma*
Danya Centeno, *R3D*
Maricarmen Sequera y Marlene Samaniego, *TEDIC*

Edición: Marianne Díaz
Revisión Paraguay: Luis Pablo Alonzo Fulchi
Portada: Violeta Cereceda
Diagramación: Constanza Figueroa
Junio 2018.

RESUMEN

Uno de los principales desafíos del sistema penal paraguayo en el Siglo XXI es afrontar las conductas delictivas en la era digital. En un primera etapa se han realizado reformas al código penal para incluir sanciones especiales a los delitos vinculados a la tecnología. Por otra parte, en el 2017 se ratifica en Paraguay, el Convenio de Ciberdelincuencia de Budapest: un marco normativo que busca la armonización de la persecución de los delitos cibernéticos de forma transfronteriza.

La presente investigación tiene como objetivo exponer las preocupaciones, los vacíos y los desafíos del marco normativo que presenta el Convenio de Ciberdelincuencia de Budapest, las normas internas vigentes y las autoridades locales para una eficaz persecución de los delitos informáticos en el marco del respeto de los tratados internacionales de los derechos humanos y los más altos estándares de protección de datos personales. Para esto, la investigación aborda un diagnóstico local a partir de un análisis jurídico y entrevistas semi-estructuradas a las autoridades de persecución penal en Paraguay.

Palabras clave: cibercrimen, delitos informáticos, datos de tráfico, Convención de Budapest, derechos humanos.

INTRODUCCIÓN

La tecnología aplicada en el Ciberespacio ha modificado por completo las diversas relaciones sociales y la globalización ha puesto en jaque a los pilares del Estado y las bases de la sociedad tradicional, hasta el punto de crear “una sociedad” paralela a la física. Este punto de inflexión ha generado grandes avances del ser humano como la comunicación y acceso al conocimiento entre millones de personas a nivel mundial. No obstante, este espacio cibernético no está exento de problemas: está habitado también por grupos extremistas, terroristas, delincuentes e individuos sin fines pacíficos.

Esto conlleva nuevos planteamientos de regulación, de forma urgente y necesaria para abordar esta problemática, puesto que si un delito se comete utilizando tecnología y genera impactos en diversos territorios de varios Estados, se requerirán mecanismos de colaboración transfronterizos para la persecución efectiva. Esta a su vez debe ser proporcionada y acorde a los derechos humanos, uno de los principales pilares de los sistemas democráticos actuales.

En consecuencia, es necesario modificar las legislaciones que de cada país de forma armonizada y crear sistemas que permitan la detención, investigación y persecución de los supuestos delitos en el marco que resguarde los derechos de las personas y que a su vez disminuya el riesgo en contra de la confidencialidad, integridad y disponibilidad de los sistemas informáticos.

La presente investigación busca realizar un diagnóstico local a partir de la ratificación del Convenio de Ciberdelincuencia de Budapest y abordar la eventual reforma a la persecución de delitos con componentes u objetivos tecnológicos, asumiendo estás observaciones y cuestionamientos en el marco de los derechos humanos.

¿QUÉ SE ENTIENDE POR CIBERCRIMEN?

En la discusión del Convenio sobre Ciberdelincuencia de Budapest –en adelante Convenio– se manejan los conceptos específicos de la materia.

Por tanto las definiciones de estos conceptos o su ausencia son relevantes para comprender mejor los alcances y desafíos que representa esta temática. A continuación se desarrollan varias de estas definiciones.

1. CIBERDELITO O CIBERCRIMEN

Se entiende por "ciberdelito"[1] o "cibercrimen" cualquier infracción punible, ya sea delito o falta, en el que se involucra un equipo informático o Internet y en el que el ordenador, teléfono, televisión, reproductor de audio o vídeo o dispositivo electrónico, en general, puede ser usado para la comisión del delito o puede ser objeto del mismo delito.

Cómo criterio para la construcción del marco teórico se toma el concepto de delito informático desarrollado por Julio Tellez Valdez. Que lo clasifica a los delitos informáticos en base a dos criterios: como instrumento o medio, o como fin u objetivo:

> "las conductas típicas, antijurídicas y culpables en que se tienen a las computadoras como instrumento o fin" y por las segundas "actitudes ilícitas en que se tienen a las computadoras como instrumento o fin" (Téllez Valdez, Julio, 2003).

Este es un término que carece de una definición universalmente homogénea y aceptada por los especialistas en el área. Si bien muchos investigadores están de acuerdo en que es una actividad ilegal realizada a través del computador, existe un desacuerdo con respecto al lugar en el que se ejecuta (Wingyan Chung, Weiping Chang, & Shihchieh Chou, 2004).

2. EVIDENCIA ELECTRÓNICA

El "e-evidence" se refiere a la evidencia digital o electrónica, como los contenidos de redes sociales, correos electrónicos, servicios de mensajería o datos almacenados en la "nube". El acceso a estos datos a menudo es requerido en investigaciones criminales. Dado que en el entorno digital las fronteras geográficas a menudo son confusas, las investigaciones requieren una cooperación transfronteriza entre las autoridades públicas y entre estas con el sector pri-

1 Sobre la diferencia entre el delito informático (que se vale de elementos informáticos para la perpetración) y el ciberdelito (que se refiere a una posterior generación delictiva vinculada a las TIC en el que interviene la comunicación telemática abierta, cerrada o de uso restringido) puede verse ROMEO CASABONA, Carlos. "De los delitos informáticos al cibercrimen. Una aproximación conceptual y político-criminal" en El cibercrimen nuevos retos jurídico-penales, nuevas respuestas político-criminales. Editorial Comares. Granada 2006, pp. 1-42.

vado («Access to e-evidence», 2017). Ejemplo de esto son el contenido de los mensajes de correo electrónico, registros de actividad digital, datos biométricos, entre otros, suelen estar en servidores y computadoras en diversos puntos del planeta.

3. DATOS PERSONALES

Se refiere a toda información sobre una persona física identificada o identificable (el interesado); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona (Jazmin Acuña, Luis Alonzo Fulchi, & Maricarmen Sequera, 2017).

4. DATOS INFORMÁTICOS

La ley 4439 (Congreso Nacional, 2011) que modifica el código penal paraguayo define a datos informáticos de la siguiente manera:

> "Se entenderán sólo aquellos que sean almacenados o se transmitan electrónica o magnéticamente, o en otra forma no inmediatamente visible".

5. DATOS DE TRÁFICO

El artículo 1 del Convenio define los datos de tráfico como cualquier información de computadora relacionada con una comunicación generado por un sistema informático que forma parte de una cadena de comunicación, indicando el origen, el destino, la ruta, la hora, la fecha, el tamaño, la duración o el origen de la comunicación, tipo de servicio subyacente.

7

TENSIONES Y DESAFÍOS PARA LA ARMONIZACIÓN DEL CONVENIO DE BUDAPEST

Para analizar al Convenio se debe enfatizar que "armonizado" no significa idéntico: lo que se busca es la complementariedad que permitirá que los mecanismos de aplicación trabajen de forma efectiva respetando las diferencias de los países. Por otro lado, es importante recalcar que el Convenio permite la adecuación de otras medidas nortmativas nacionales, regionales o internacionales organismos que abordan estos delitos sustantivos en la medida que no sean inconsistentes con el Convenio.

1. EL CONVENIO SOBRE LA CIBERDELINCUENCIA

El Convenio sobre la ciberdelincuencia, conocido como el Convenio de Budapest fue firmado en dicha ciudad el 23 de noviembre de 2001 y entró en vigencia el 1 de julio de 2004. El mismo busca proteger a la sociedad frente al "nuevo" tipo de delincuencia, adoptando y armonizando una legislación adecuada para cada país y mantener una política de cooperación internacional. En su redacción participaron los 41 países miembros del Consejo de Europa, junto a otros Estados no miembros como Estados Unidos, Canadá, Japón y Sudáfrica. El Convenio se encuentra actualmente vigente en Paraguay a través del decreto N°243 de fecha 20 de diciembre[2] de 2017[3].

Además, en el 2003 se promulgó la firma del Protocolo Adicional al Convenio de Ciberdelincuencia[4] (Council of Europe, 2003) criminalizando los actos de racismo y xenofobia relacionados con las nuevas tecnologías. Este protocolo fue ratificado por Paraguay en el mismo decreto presidencial citado más arriba.

Habiendo pasado más de 15 años de su entrada en vigor, es oportuno reflexionar sobre el papel de la Convención en la armonización de las leyes de cibercrimen y su lugar entre otros esfuerzos internacionales para combatir dicho flagelo.

El convenio cuenta con 4 capítulos, que incluyen una serie de terminologías y establece 3 ejes elementales para la persecución de delitos informáticos. El primer eje son los delitos sustantivos en virtud del Convenio se pueden clasificar en general en "(1) delitos contra la confidencialidad, la integridad y la disponibilidad de datos y sistemas informáticos; (2) delitos relacionados con la informática; (3) delitos relacionados con el contenido; y (4) infracción criminal de derechos de autor " (Clough, 2014).

---

2 Decreto Presidencial N° 243 del 20 de diciembre de 2017. http://www.gacetaoficial.gov.py/index/getDocumento/50005

3 Ver listas de paises que firmaron y ratificaron el Convenio de Budapest. Disponible en: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures

4 Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems. 2003. Disponible en https://rm.coe.int/168008160f

Los delitos que tienen a la tecnología como fin son aquellos que atentan contra la confidencialidad, integridad o disponibilidad de la información. Por ejemplo, el daño informático, el acceso ilícito a un sistema, etc..

Por otra parte, los delitos que tienen a la tecnología como medio son los que se encuentran tipificados en las legislaciones penales: en Paraguay están en el Código Penal, Ley Nº. 1.160/97 y "se trasladan" a Internet para su aplicación. Y son: fraude informático y falsificación de datos digitales.

Los delitos relacionados con el contenido, son los relacionados a varios aspectos de la producción, posesión y distribución digital de la pornografía infantil.

Por último, los delitos sobre infracción criminal de derechos de autor, se refiere a la reproducción y difusión en Internet de contenidos protegidos por el derecho de autor, sin autorización del titular de la obra. Un ejemplo de ello son las infracciones a la "propiedad intelectual".

El segundo eje elemental del Convenio es el establecimiento de los procedimientos para salvaguardar la evidencia digital, así como las herramientas relacionadas con su la manipulación. Por tanto regula el ámbito de aplicación de las disposiciones de procedimiento (artículo 14), las condiciones y salvaguardias previstas en el derecho interno de cada país miembro (artículo 15), la rápida conservación de datos informáticos almacenados, la conservación y revelación parcial de los datos relativos al tráfico, la entrega de facultades a la autoridad para que ordene a personas naturales o proveedores entregar datos informáticos que obren en su poder (artículo 18), el registro y confiscación de datos informáticos almacenados (artículo 19), la obtención en tiempo real de datos relativos al tráfico y la interceptación de datos relativos al contenido (artículos 20 y 21), así como también relativas a la jurisdicción (artículo 22).

Por último el eje que contiene las normas de cooperación internacional, que son reglas de cooperación para investigar cualquier delito que involucre evidencia digital. Allí se incluyen normas especiales en torno a la extradición (artículo 24), la asistencia mutua entre distintas instituciones(artículo 25), la colaboración en entrega de información que pueda resultar útil para una investigación (artículo 26), la utilización de tratados de asistencia mutua (artículos 27 y 28), la conservación, revelación y asistencia mutua en relación a datos informáticos almacenados (artículos 29, 30 y 31), la asistencia mutua para la obtención en tiempo real de datos relativos al tráfico y en relación con la interceptación de datos relativos al contenido. Además se establece una red «24/7», es decir, un punto de contacto localizable las 24 horas del día y 7 días de la semana, que cada parte deberá designar con el fin de garantizar la asistencia inmediata en la persecución de este tipo de delitos (Lara, Martínez, & Viollier, 2014).

Este capítulo busca armonizar un proceso penal ágil y eficiente, con esfuerzo organizado por los países partes. Viendo que la evidencia digital es volátil e intangible, las investigaciones que involucran este tipo de pruebas deben ser rápidas y precisas.

9 —

Actualmente el Convenio se encuentra en etapa de borrador para la elaboración del segundo protocolo adicional de Cibercrimen[5]. El plan de la Comisión Europea es proponer nuevas reglas sobre el intercambio de pruebas y la posibilidad de que las autoridades soliciten pruebas electrónicas directamente de las empresas de tecnología. Una de las opciones propuestas es que la policía pueda acceder a los datos directamente desde los servicios basados en la nube («Access to e-evidence», 2017).

5 Cybercrime Convention Committee (T-CY)(DRAFT) Terms of Reference for the Preparation of a Draft 2nd Additional Protocol to the Budapest Convention on Cybercrime. Marzo 2017. Disponible enhttps://goo.gl/xfQwY7

2. RESERVAS SOBRE EL CONVENIO DE BUDAPEST

El Convenio ha tenido muchas críticas a nivel internacional, acerca de su enfoque de cómo prevenir y luchar contra el delito cibernético de manera efectiva y actualizada. Se describirá algunos puntos más importantes que se deberán tomar con precaución a la hora de pensar su armonización al sistema penal paraguayo.

2.1 UN CONVENIO CERRADO Y DESACTUALIZADO

Durante los años de elaboración del Convenio (1997-2001) muchas amenazas en el campo de la seguridad de la información, incluyendo los delitos, eran desconocidos o tenían un impacto menor o se consideraba insignificante. Desde su promulgación, se han identificado nuevos tipos de crímenes tales como la vigilancia masiva de las comunicaciones, la vigilancia especifica a través de software malicioso –que permite acceder de forma remota a los sistemas informáticos–, el phishing, medidas anti-spam, entre otros.

El Convenio no previó cubrir ni mitigar nuevas formas de cibercrimen, pero pensar modificarlo y/o ampliarlo será una tarea complicada, ya que tiene unos procedimientos de enmiendas muy complejos, que pueden ser introducidas solo después de su ratificación, por voto mayoritario. El informe de Electronic Privacy Information Center (EPIC) lo plantea de la siguiente forma:

> "De un modo muy secreto y antidemocrático, el Comité de Expertos sobre Crimen en el Ciberespacio del Consejo de Europa [...] completó diecinueve borradores de la Convención antes de que el documento fue se comunicado al público. Entre los años 1997 y 2000 ninguno de los borradores fue liberado ni se solicitó aportes al público. La Convención fue redactada por personas y agrupaciones principalmente asociadas a autoridades de cumplimiento de la ley y refleja exclusivamente sus preocupaciones, con el consiguiente menoscabo a la privacidad y las libertades civiles" (EPIC, 2004).

En este sentido, la Unión Internacional de Telecomunicaciones (UIT)[6], criticó las propuestas para adoptar el Convenio como estándar mundial y homogeneizar las legislaciones de los países, porque considera que la misma fue redactada principalmente por y para los estados europeos y a mas de varios años de su vigencia, la convención se encuentra desactualizada[7]. El entonces Secretario General de la ITUs, Hamadoun Touré afirmaba lo siguiente:

> "Los europeos deben ser felicitados porque ya tienen leyes. Lamen-

6 Unión Internacional de Telecomunicación. Pagina oficial – Disponible enhttps://www.itu.int/

7 ITU calls for global cybersecurity measures. Mayo 2009 Disponible enhttp://www.h-online.com/security/news/item/ITU-calls-for-global-cybersecurity-measures-741711.html [Fecha de consulta: 8 de Febrero, 2018].

> tablemente, la convención tampoco es el mejor modelo y ya está un poco polvoriento"[8] [La traducción es propia]

2.2 CONTROVERSIAS EN LA PARTE SUSTANTIVA

Otras de las controversias que ha suscitado el Convenio es la inclusión de delitos ordinarios como por ejemplo: falsificación, fraude y pornografía infantil. Los expertos dicen que los mismos ya se encuentran en los cuerpos legislativos penales de las naciones modernas. A pesar que se presupone que con el uso de la tecnología aumentan los casos en que algunos delitos caerían fuera de la definición ordinaria, esto podría aplicarse también a otros delitos ordinarios como por ejemplo el hurto o la extorsión, y sin embargo no se tipifican de forma especial.

Ni la Convención ni el Reporte Explicativo adjunto a la misma indican: i) ¿por qué solo un subgrupo de delitos fueron incluidos en la Convención?, y ii) ¿por qué este particular conjunto de conductas fue elegida? (Susan Brenner, 2012).

Algunas de las críticas mas especificas acerca del Convenio fueron sobre el Artículo 1, donde se provee la siguiente definición de proveedora de servicio:

> "i. toda entidad pública o privada que ofrezca a los usuarios de sus servicios la posibilidad de comunicar a través de un sistema informático, y ii. Cualquier otra entidad que procese o almacena datos informáticos para dicho servicio de comunicación o para los usuarios del mismo"

Resulta confuso que el concepto de proveedores de servicio comprenda al proveedor a acceso a Internet y al proveedor de contenidos, y esto da lugar a una interpretación amplia.

Sobre el artículo 4, Ataques de la integridad de los datos, que expresa lo siguiente:

> "Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno la comisión deliberada e ilegitima todo acto que dañe, borre, deteriore, altere o suprima datos informáticos".

Y el segundo párrafo dice:

> "Las Partes podrán reservarse el derecho a exigir que los actos definidos en el párrafo 1 comporten daños graves".

En primer lugar, las legislaciones penales no deberán aceptar esta norma tal

8 ITU will IP-Adressen verwalten. Octubre 2009. Disponible en https://www.heise.de/newsticker/meldung/ITU-will-IP-Adressen-verwalten-835928.html?netze=mrw_channel [Fecha de consulta: 8 de Febrero, 2018].

cual como está escrita, porque contradice el principio de intervención mínima del aparato punitivo del Estado, propio de lo que se denomina “derecho penal mínimo o ultima ratio”[9].

Por otro lado, el segundo párrafo no determina la diferenciación de la gravedad de los hechos, y tampoco orienta o describe cuáles actos son graves, dejando abierta a una interpretación ambigua del artículo, incluyendo la ausencia de definición de daño en el contexto de delitos informáticos. Es decir, se hace compleja la armonización de este artículo a legislaciones penales locales porque no se distingue la gravedad entre la destrucción de cualquier sistema informático y los ataques que provocan daños económicos: para el Convenio, cualquier delito es igual de grave.

Sobre el artículo 6 - Abusos de dispositivos, por el cual cada Parte adoptará medidas legislativas para tipificar como delito, la comisión deliberada e ilegítima:

a) la producción, venta, obtención para su utilización, importación, difusión u otra forma de puesta a disposición de : i. cualquier dispositivo.../ ii. Contraseña, código de acceso o datos informáticos similares que permitan acceder a todo o parte de un sistema informático.

Hay expertos que afirman que este artículo pone en riesgo la libertad de expresión y a su vez, penaliza actividades legítimas de profesionales y empresas de seguridad informática.

Otras de las reservas al Convenio es referente al segundo párrafo del artículo 9, sobre Delitos relacionados con la pornografía infantil, los inc b y c dicen: “Una persona que parezca un menor comportándose de una forma sexualmente explícita” y también a las “imágenes realistas que representen a un menor comportándose de una forma sexualmente explícita”.

Según estudiosos de la materia, la persecución de este hecho punible pretende proteger a los niños y adolescentes de la explotación sexual. Es decir que para que se cumpla el presupuesto del tipo penal debe haber una victima menor de edad. El Convenio tiene una falla sustancial de enfoque e intervención mínima del derecho penal. Para ejemplificar, si se aplicara el Convenio, tanto las animaciones japonesas (animé) o pinturas de niños desnudos en la playa caerían en el supuesto penal (Carlos Reusser, 2017).

Por otro lado, Brasil se negó a ratificar el Convenio expresando sus reservas sobre disposiciones en elartículo 10, relativa a la penalización de las infracciones a

9 “Derecho penal mínimo significa la reducción al mínimo de las circunstancias penales y su codificación general mediante la despenalización de todas aquellas conducta que no ofendan bienes fundamentales y que saturan el trabajo judicial con un dispendio inútil e inocuo de aquel recurso escaso y costoso que es la pena y tienen el triple efecto del debilitamiento general de las garantías, de la ineficacia de la maquinaria judicial y de la devaluación de los bienes jurídicos merecedores de tutela penal.” Ferrajoli, Luigi. Crisis del sistema político y jurisdicción: la naturaleza de la crisis italiana y el rol de la magistratura. Revista Pena y Estado año 1 número 1-Argentina 1995: Editores del Puerto s.r.l. p. 113.

la propiedad intelectual[10]. Consideran un punto oscuro porque anula el debate sobre el tipo y gravedad del delito. Además es una forma de control social por descargas de contenidos de Internet que pueden ser consideradas irrisorias o irrelevantes en el sistema de propiedad intelectual, conllevando violaciones al derechos humanos como el acceso a la información y a la cultura.

2.3 DIVERGENCIAS EN LA PARTE PROCESAL

También se encuentran las normas sobre procedimiento de la Convención que han generado polémicas a nivel Internacional. Entre una de ellas se encuentra el artículo 14 – Ámbito de aplicación de las disposiciones de procedimiento que tiene como objetivo la aplicación de los procedimientos establecidos en el Convenio, no sólo a los establecidos en los artículos 2 al 11 del mismo, sino a:

> "cualquier otro tipo de delito cometido por medio de un sistema informático; y a la obtención de pruebas electrónicas de cualquier delito" Inc b del Artículo 14

Esto produce una ampliación de facultades conferidas por el Convenio en las disposiciones sustantivas, ya que en las disposiciones de procedimiento se aplicarán a todas las investigaciones que requieran evidencia digital y que no necesariamente califiquen como delito informático o cibercrimen. Al final, pareciere que la parte sustantiva es insignificante o innecesaria (Susan Brenner, 2012).

Los artículos 16 – Conservación de datos informáticos almacenados y artículo 17 sobre la Conservación y revelación parcial rápida de los datos relativos al tráfico. De acuerdo a lo definido por el Convenio sobre datos de tráfico, (art 1), estos 2 artículos aplican la obligación de conservación de datos de tráfico, almacenados por medio de un sistema informático y de proteger la integridad de los datos durante un tiempo necesario, hasta un máximo de 90 días y podrán renovar dicho tiempo por las Partes.

Asimismo se tomarán medidas necesarias para garantizar la conservación rápida de datos de tráfico que se encuentran en las proveedoras de servicios de Internet y se asegurará la revelación rápida a la autoridad competente.

Estos artículos que son complementados por el Artículo 29 del Convenio, no establecen mecanismos de conservación, por tanto da lugar a un almacenamiento masivo de metadatos de forma previa, llevando como resultado una vigilancia masiva.

Como dice el Relator Especial de las Naciones Unidas sobre Libertad de Expresión, Frank LaRue

"La vigilancia de las comunicaciones debe ser entendida como un acto altamente intrusivo que potencialmente interfiere con los derechos a la libertad de

10 Idem 7

expresión y a la privacidad, y amenaza las bases de una sociedad democrática"(Consejo de Derechos Humanos, 2013)

Por otro lado, surge la pregunta si el Convenio puede ser un intento de legalizar el espionaje global. Las conocidas divulgaciones de Edward Snowden dejaron en claro que existen agencias gubernamentales y supra poderes que presionan para colocar este tema en la agenda.

Por tanto los metadatos deben ser delimitados bajo condiciones de Estado de derecho y salvaguardia. Para encontrar acuerdo en las medidas de retención de datos de tráfico para la investigación del cibercrimen, que restringen derechos fundamentales reconocidos en la Constitución, la Corte Suprema de Justicia exige la observancia del principio de proporcionalidad[11] de manera que es necesario constatar 3 condiciones:

- Si tal medida es susceptible de conseguir el objetivo propuesto (juicio de idoneidad),
- Si además es necesaria en el sentido de que no exista otra medida más moderada para la consecución de tal propósito con la misma eficacia (juicio de necesidad)
- Si la misma es ponderada y equilibrada por derivarse de ella más beneficios y ventajas para el interés general, que perjuicios sobre otros bienes o valores en conflicto (juicio de proporcionalidad en sentido estricto).

La proporcionalidad de la medida debe ser valorada por el juez competente y usada solamente para los propósitos y durante los lapsos para los cuales se otorgó autorización. Cualquier información excedente no será retenida, siendo en su lugar destruida o devuelta con prontitud. Que las actividades de vigilancia solicitadas y técnicas propuestas no menoscaben la esencia del derecho a la privacidad o de las libertades fundamentales.

Por otro lado se encuentran los artículos 20 – Obtención en tiempo real de datos relativos al tráfico y 21 Interceptación de datos relativos al Contenido del Convenio referidos a investigaciones relativas "a delitos graves que deberán definirse en su derecho interno". Esto genera preocupaciones por las amplias facultades conferidas por el Convenio, que al final se aplican a cualquier investigación del sistema penal que requieran evidencia digital.

Expertos sugieren medidas menos intrusivas, proporcionales y eficaces para perseguir conductas relacionadas a las TIC como ser: la infiltración de agente encubierto en la red de la organización criminal, la interceptación de las co-

11 Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones. Disponible en: https://es.necessaryandproportionate.org/text. Análisis Jurídico Internacional de Apoyo y Antecedentes https://es.necessaryandproportionate.org/analisislegal, Universal Implementation Guide for the International Principles on the Application of Human Rights To Communications Surveillance, https://s3.amazonaws.com/access.3cdn.net/a0ea423a1607c836a3_aqm6iyi2u.pdf[Fecha de consulta: 8 de Febrero, 2018].

municaciones para descubrir sus componentes en tiempo real o solicitudes de retención de datos a partir de la recepción de la denuncia penal. Las informaciones provenientes de delatores y confidentes[12].

Por otro lado se encuentra el artículo 29 del Convenio, referente a la asistencia mutua en materia de medidas provisionales sobre la Conservación rápida de datos informáticos almacenados, que establece:

> "Una Parte podrá solicitar a otra Parte que ordene o imponga de otro modo la conservación rápida de datos almacenados por medio de sistemas informáticos que se encuentren en el territorio de la otra Parte, y en relación con los cuales la Parte requiriente tenga intención de presentar una solicitud de asistencia mutua con vistas al registro o al acceso por medio similar, la confiscación o la obtención por medio similar, o a la revelación de dichos datos"

Rusia, como muchos otros países, tampoco se ha adherido al Convenio, ya que considera inaceptable una de las disposiciones sobre el acceso transfronterizo a los datos durante las investigaciones. Ha expresado constantemente su preocupación de que los artículos 29 y 32 del Convenio prácticamente otorga permiso para penetrar en las redes de otros Estados, violando el principio de la soberanía estatal y contradiciendo el espíritu de cooperación, respeto entre los Estados y los derechos de sus ciudadanos (Clough, 2014).

Dicho artículo 32 estipula que en el marco de la asistencia mutua existe una capacidad de acceso, con consentimiento o cuando sea accesibles al público, una Parte podrá sin autorización de la otra Parte tener acceso informático a datos almacenados disponibles al público (fuente abierta) (párrafo primero), o para datos informáticos almacenados si la Parte obtiene el consentimiento legal y voluntario de la persona que tiene la autoridad legal para divulgar los datos (párrafo segundo). Sin embargo, las disposiciones del artículo son tan vagas que no está claro quién da tal permiso, qué recursos pueden interesar y qué poderes tiene la persona autorizada.

Según EuroISPA (EDRI, 2017), hay un gran aumento en las solicitudes transfronterizas, que pueden crear cargas significativas y subraya 3 principios claves para la realización de las mismas:

1. En un nivel alto, es importante que solo se espere que los servicios más pequeños cooperen con la policía local. Es importante tener reglas claras para construir sobre la buena cooperación existente.

2. Cada vez son más las solicitudes recibidas en idiomas extranjeros de jurisdicciones extranjeras, con poca claridad sobre las obligaciones legales. Algunas veces hay una obligación legal de no responder.

12 La denominación en inglés es "whistleblower"

3. El acceso directo es muy preocupante. También hay problemas relacionados con la financiación de los procedimientos y la carga financiera de la evaluación legal de las solicitudes de datos. Los arreglos de asistencia judicial recíproca deben seguir siendo el núcleo de cualquier nuevo marco en esta área de políticas.

Por tanto, será necesario generar un nuevo documento internacional, probablemente en Naciones Unidas (ONU) que aproveche las experiencias positivas de la misma y al mismo tiempo garantice la soberanía y la no injerencia en los asuntos internos de Estados.

2.4 CONFLICTOS CON LOS DERECHOS HUMANOS

El preámbulo y el artículo 15 – Condiciones y salvaguardias del Convenio son las únicas secciones en que aparece expresamente la obligación de garantizar la protección adecuada de los derechos humanos. Esta limitación ha generado varias críticas sobre la falta de garantías generales y las facultades que confiere el respecto de la privacidad. La redacción del artículo 15 lleva a invisibilizar otros tratados fundamentales como la a Declaración Universal de Derechos Humanos de 1948 y la Convención para la Protección de los Derechos Humanos y las Libertades Fundamentales de 1950 y otros tratados relacionados a la privacidad y protección de datos personales.

Tampoco garantiza ni exige que las Partes cumplan con las normas internacionales de derechos humanos en relación con ninguna ley penal sustantiva interna. Cabe destacar que algunos Estados partes cuentan con leyes que limitan la libertad de expresión en relación con la blasfemia, difamación contra el Estado, cuestiones sexuales o incluso delitos de odio (EDRI, 2017).

Recién en la Conferencia sobre la aplicación de este artículo(Consejo de Europa, 2014), se concluyó la aplicación deberán ampliarse en la legislación penal sustantiva y deberá mejorar a la luz de la evolución de las políticas y la tecnología. Los Estados parte que no observen estas medidas sugeridas por el Consejo de Europa, accederán a las las evidencias digitales poniendo en riesgos de posibles abusos de los datos personales y los derechos humanos de las personas.

Por otro lado, los defensores de la privacidad cuestionan la redacción de los artículos 18 – orden de presentación y articulo 19 – Registro y confiscación de datos informáticos almacenados del Convenio, porque se autoriza a las autoridades a forzar a los individuos a divulgar sus llaves de cifrado, esto pone en riesgo los derechos a la privacidad y criminaliza el derecho al anonimato.

Otra preocupación es que el Convenio no expresa ninguna limitación, ni rigurosidad en el tratamiento de evidencia digital sujeta a los poderes de las Instituciones en la investigación. Por tanto, el proceso y acceso a la evidencia digital debe ser abordada por el principio de proporcionalidad. Es decir, corresponde a las partes individuales determinar si una conducta particular es suficientemente seria como para justificar la aplicación de ciertos poderes de investigación,

y las circunstancias en que se pueden ejercer esos poderes (Clough, 2014). La única limitación específica del Convenio sobre este punto se encuentra en el Art 21 -Interceptación de datos relativos al contenido, en reconocimiento del alto nivel de protección de la privacidad que muchos Estados ofrecen a los contenidos de comunicaciones.

También se menciona graves problemas en las disposiciones procesales, tales como la ausencia de garantías en caso de abuso o error judicial en la búsqueda de interceptación de datos, retención de datos de tráfico y de órdenes de cumplimiento.

Los arreglos de cooperación voluntaria entre las proveedoras de servicios y a la aplicación de la ley a menudo carecen de responsabilidad y previsibilidad. Por esa razón cualquier nueva medida sobre tratamiento de evidencia digital debe cumplir con los estándares internacionales de derechos humanos y protección de datos. Los Estados deben seguir regulando el acceso de datos en su jurisdicción y las adquisiciones tecnológicas para el tratamiento de los mismos.

La iniciativa del Consejo de Europa establece en el marco del Convenio, una nueva propuesta legislativa que está prevista para principios de 2018. El 8 de junio de 2017, el mismo presentó las opciones de medidas prácticas y legislativas a los ministros de la UE. Esta etapa será crucial incluir las salvaguardas para garantizar que la protección de datos y el estado de derecho se apliquen a la nueva legislación, de lo contrario, se impondrá a costa de los derechos humanos de los ciudadanos (EDRI, 2017).

2.5 CONSERVACIÓN DE DATOS DE TRÁFICO

Si bien, los artículos 16, 17, 20 y 21 relativos a conservación de datos de tráfico ya se expuso en la parte procesal de la investigación, en este apartado se busca profunizar para una armonización acorde a los datos personales y derechos fundamentales.

Los artículos que se refieren a los datos de tráfico se encuentran en la parte procesal del Convenio y son: artículo 16 – Conservación rápida de datos informáticos almacenados, artículo 17 - Conservación y revelación parcial rápidas de datos relativos al tráfico, artículo 20 - Obtención en tiempo real de datos relativos al tráfico yartículo 21 – Interceptación de datos relativos al Contenido. Los mismos son considerados “espinosos” al momento de su aplicación por lo expuesto en la sección anterior.Los mismos podrían provocar violaciones de derechos humanos y por lo tanto socavar las bases del sistema democrático.

Expertos argumentan que el Convenio es un tratado de justicia penal por lo que el acceso a datos se refiere al acceso a datos específicos en la investigación penal específica, y no a la recopilación indiscriminada de datos de tráfico ni justificadas para la seguridad nacional (McNamee, 2017).

La persecución de delitos debe realizarse siempre bajo una sospecha justifi-

cada, individualizada, dirigida, con un proceso legal mediante –no violando principios fundamentales como el de la presunción de inocencia, el derecho a la privacidad y la libertad de expresión. Los mismo se aplica al entorno digital. Por lo que existen serias dudas sobre la efectividad de esta herramienta desde el punto de vista tecnológico, además de cuestionamientos de principios.

En primer lugar se debe recordar que los criminales más peligrosos utilizan herramientas de anonimización o cifrado, imposibilitando que sean fácilmente encontrados.

Segundo, en el proceso de dar con unos delincuentes, habrán sido víctimas de vigilancia injustificada demasiadas personas inocentes —he ahí la desproporcionalidad a la que se refiere. En base a unsimple cálculo matemático realizado por un profesor de la Universidad de Tromso en Noruega (Rudmin, 2006), se concluye que "inclusive si el programa de vigilancia masiva tiene un índice de falso positivo[13] de 1 en 1.000 —y no hay tecnología de seguridad que siquiera se acerque a esto—cada vez que le preguntes por sospechosos, marcará a 60.000 personas inocentes".

Pero, inclusive en el hipotético caso que la retención de datos de tráfico sea efectiva, no se tendría por qué legitimarla y menos aún legalizarla. La efectividad jamás puede ser recurso suficiente para aprobar una ley de retención de datos de tráfico en un estado que dice ser democrático. Efectivas han sido muchas herramientas, y al mismo tiempo profundamente dañinas: la bomba atómica, las cámaras de gas, los informantes de la dictadura, los toques de queda, entre otros (Sequera, 2015).

No sólo se trata que la vigilancia debe realizarse con autorización judicial competente sino que ésta debe ser previa, imparcial e independiente de las autoridades encargadas de la vigilancia.

También la autoridad judicial debe estar capacitada en materias relacionadas, y tiene que ser competente para tomar decisiones judiciales sobre la legalidad de la vigilancia, las tecnologías utilizadas y los derechos humanos, además de contar con los recursos adecuados en el ejercicio de las funciones que se le asignen.

Es necesario dejar en claro que el Estado debe demostrar a la autoridad judicial competente, antes de la realización de la vigilancia, que tiene que ser proporcionada. Es decir debe cumplir todas las siguientes condiciones:

- Existir un alto grado de probabilidad de que un delito grave o una amenaza específica para algún fin ha sido o será llevado a cabo
- Existir un alto grado de probabilidad que las evidencias pertinentes y materiales de un delito tan grave o amenaza específica se conseguirían me-

13 Errores de tipo I y de tipo II . Disponible en https://es.wikipedia.org/wiki/Errores_de_tipo_I_y_de_tipo_II

diante el acceso a los datos del usuario solicitado
- Que otras técnicas de investigación, que son menos invasivas ya han sido agotadas o serían inútiles
- La información a la que se accederá será solo la relevante para perseguir el crimen o la amenaza especifica alegada
- Cualquier información excedente no será retenida, siendo en su lugar destruida o devuelta con prontitud.

También es importante destacar que los datos informáticos que deben conservarse son los datos que ya han sido almacenados. Es decir, que el Convenio sólo solicita preservación de datos que ya existen en las proveedoras de servicio de Internet y no de retención de datos (Consejo de Europa, 2001). Cabe destacar que en el Convenio no requiere la retención de datos porque amplia la base de información.

El carácter violatorio de este tipo de normas ya ha sido advertido por instancias del sistema internacional de protección de derechos humanos. El Relator Especial de las Naciones Unidas sobre la promoción y protección de la libertad de opinión y expresión, Frank la Rue, ha señalado que:

> "Las leyes nacionales de conservación de datos son invasivas y costosas, y atentan contra los derechos a la intimidad y la libre expresión. Al obligar a los proveedores de servicios de comunicaciones a generar grandes bases de datos acerca de quién se comunica con quién telefónicamente o por Internet, la duración del intercambio y la ubicación de los usuarios, y a guardar esta información (a veces durante varios años), las leyes de conservación obligatoria de datos [de tráfico] aumentan considerablemente el alcance de la vigilancia del Estado, y de este modo el alcance de las violaciones de los derechos humanos. Las bases de datos de comunicaciones se vuelven vulnerables al robo, el fraude y la revelación accidental" (Consejo de Derechos Humanos, 2013).

La Relatoría Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos (CIDH) ha señalado a su vez que las intervenciones estatales en materia de seguridad en Internet deben ser limitadas y proporcionadas, y deben procurar cumplir con fines legales precisos, que no comprometan las virtudes democráticas que caracterizan a la red.

Cualquier medida que pueda afectar la libertad de expresión en Internet, entre ellas la vigilancia de las comunicaciones, debe satisfacer un triple test de legitimidad a saber: las restricciones deben estar establecidas en la ley en los términos más claros y precisos posible, perseguir una finalidad legítima reconocida por el derecho internacional y ser necesaria para alcanzar dicha finalidad. Cuando las restricciones tienen finalidades penales, a estos requisitos se deben agregar los propios del debido proceso y de legalidad (Relatoría Especial para la Libertad de Expresión, CIDH, 2009).

Una de las jurisprudencias vinculantes a la jurisdicción paraguaya[14], indica que el único mecanismo posible para acceder a los datos de tráfico o metadatos de las comunicaciones es la autorización judicial. La decisión de la Corte Interamericana de Derechos Humanos (CIDH) sobre el caso contencioso, en el que se condenó a Brasil (CIDH, 2009) por el uso ilegal de escuchas telefónicas en un proceso penal, señaló que el derecho a la privacidad protege tanto al contenido de la comunicación electrónica, como a otros datos propios del proceso técnico de la comunicación, es decir, los metadatos o datos de tráfico. Según la resolución, los metadatos son:

> "el destino de las llamadas que salen o el origen de las que ingresan, la identidad de los interlocutores, la frecuencia, hora y duración de las llamadas, aspectos que pueden ser constatados sin necesidad de registrar contenido de la llamada mediante la grabación de las conversaciones".

Entre otras jurisprudencias internacionales está la decisión de la Gran Sala del Tribunal de Justicia de la Unión Europea sobre el caso Digital Rights Ireland Ltd. (Judgment of the Court (Grand Chamber), 2014), que declaró inválida la Directiva de Conservación de datos de la Unión Europea, entre otras palabras, "nunca debería hacer sido aprobada" (Runnegar, 2014).

La Gran Sala considera que la recogida masiva de datos de Internet en Europa supone una

"interferencia de amplio alcance y particularmente grave de los derechos fundamentales a la vida privada y a la protección de los datos personales".

La Gran Sala también sostuvo que, a pesar de que la retención de datos de telecomunicaciones perseguía el objetivo legítimo de la lucha contra "delitos graves", la naturaleza de la obligación implicaba "una injerencia en los derechos fundamentales prácticamente a la totalidad de la población europea", incluidas "las personas para las que no hay pruebas que sugieran que su conducta podría tener una vinculación, incluso indirecta o remota, con un delito grave".

Otra sentencia importante a destacar es la sentencia del Tribunal de Justicia de la Unión Europeade 2016 (Judgment of the Court (Grand Chamber), 2016), donde se decidió que la implementación de retención de datos en Suecia y el Reino Unido era contraria a la legislación de la UE, tras su decisión de invalidar la anterior Directiva de Conservación de datos la UE en el año 2014. Según el

14 En las entrevistas de la investigación "Quién defiende tus datos" surge la preocupación que las ISPs Tigo, Personal y Claro tienen sobre este procedimiento fiscal para la solicitud de información. Ellos alegan desconocimiento de decisiones internacionales vinculantes a la jurisdicción paraguaya, una salida loable para que la Corte Suprema de Paraguay analice con mayores instrumentos el cumplimiento del debido proceso y elevar el estándar de protección de las personas ante posibles abusos de las autoridades. Disponible en https://qdtd.tedic.org/ [Fecha de consulta: 8 de Febrero, 2018].

fallo, una retención “general e indiscriminada” es imposible, ya sea a nivel de la UE o nacional. La retención de datos de comunicación (quién se comunica, cuándo, con quién y dónde) solo se permitirá si existe una conexión entre los datos y un propósito específico. Además, los datos solo se pueden conservar durante un período de tiempo específico y/o área geográfica y/o un grupo de personas que puedan estar involucradas en un delito grave (Anna Biselli, 2017).

En el 2014 en el Congreso Nacional de Paraguay presentó una propuesta legislativa llamada “Que establece la obligación de conservar los datos de tráfico”. La misma obligaba a las proveedoras de servicio de Internet a almacenar masivamente metadatos de las comunicaciones de todos los usuarios por un periodo de 12 meses, para supuestos fines de investigación criminal[15]. Tras una campaña apodada Pyrawebs[16], en alusión a las tareas de espionaje de la policía durante la dictadura militar del General Stroessner, el congreso rechazó la propuesta.

Por tanto, será indispensable que las autoridades paraguayas consideren las interpretaciones expuestas en esta sección, relativas a la retención de datos de tráfico. La aplicación del Conveniodebería ser proporcional y autorizarse únicamente cuando exista riesgo particular de un daño superior al interés general de la sociedad. En este caso el interés general se expresa en el derecho a la privacidad y a la libre expresión y circulación de información. Esta aplicación deberá tener en cuenta la proporcionalidad de la ley, por lo que se sugiere que la conservación de los datos que supuestamente realizan las proveedoras de servicio, se realicen únicamente a partir de su solicitud hacia el futuro, para no socavar los derechos humanos y el sistema democrático.

OBJETIVOS

Un primer objetivo de esta investigación es generar insumos de información y análisis jurídico para fortalecer las normas y las prácticas de la implementación y aplicación del Convenio de la Ciberdelincuencia de Budapest –más conocido como “Convención de Budapest”– al sistema penal paraguayo.

Con esta investigación se busca a sentar las bases argumentativas necesarias para diseñar una propuesta de implementación de la Convención de Budapest que permita actualizar la normativa vigente a los desafíos que imponen las nuevas tecnologías para una persecución penal, acorde a los derechos fundamentales vigentes en el país.

En ausencia de una ley integral de protección de datos personales, existen pro-

15 El proyecto de Ley “Que establece la obligación de conservar datos de tráfico”, obligaba almacenar los datos de tráfico (metadatos), identificación y geolocalización de los usuarios, equipo utilizado para la comunicación, dirección de IP, de origen y destino de la misma, hora y fecha de conexión y desconexión. Año 2014.

16 Pyrawebs. la campaña liderada por TEDIC y Amnistía Internacional de Paraguay contra la retención de datos de tráfico. Disponible en www.pyrawebs.tedic.org [Fecha de consulta: 8 de Febrero, 2018].

blemas en el tratamiento procesal penal de información de carácter personal de la ciudadanía para la persecución de delitos o crímenes cometidos a través de la tecnología. Esta ausencia, deriva en situaciones complejas que pueden poner en peligro los derechos a la intimidad de las personas.

El siguiente objetivo de investigación, es generar un policy paper que sirva como hoja de ruta para la comunidad académica y actores políticos que permita abordar temas relacionados a Tecnología y normativas penales. La generación de instrumentos de análisis para ampliar el repositorio de conocimiento en este área resulta clave. Hasta el momento, no se han encontrado estudios que analizan a nivel local los desafíos que requiere la implementación de la Convención de Budapest.

ESTRATEGIA METODOLÓGICA

Para cumplir con los dos objetivos planteados en el apartado anterior, se identificó el contexto local sobre los usos, manejos y procedimientos, así como normativa legal nacional vigente que definen la implementación de la Convención de Budapest.

Por otro lado, se realizaron entrevistas a responsables del sistema penal, que persiguen los delitos que se cometen a través de la tecnología y delitos informáticos propiamente dichos, para indagar qué principios, protocolos y estándares utilizan para la persecución penal.

La presente investigación se difundirá en los canales de comunicación de la organización y se acercará a los entrevistados y autoridades del Estado que tienen la capacidad de promover una adecuada implementación y aplicación del Convenio de Budapest en el marco de los derechos humanos.

La investigación tiene un abordaje de carácter exploratorio, en vista a que a nivel local, existen pocos trabajos académicos que aborden la implementación de la Convención de Budapest al sistema penal paraguayo. Así como análisis de cuestiones de derecho sustantivo y procesal que estén estrechamente relacionadas con el uso de la tecnología de la información. Se busca conocer el marco legal actual y los desafíos para la implementación de la Convención de Budapest en el marco del derecho penal y procesal, así como los estándares de protección de datos personales y otros derechos humanos.

En la realización de la investigación se utilizarán varias herramientas metodológicas. En primer lugar, el análisis jurídico que servirá como hoja de ruta de la implementación de la Convención de Budapest en el sistema penal paraguayo. Se contemplará el marco conceptual para la implementación sobre la ciberdelincuencia que a la vez servirá para establecer el estado legal actual.

Por otro lado, se utilizará la herramienta metodológica de entrevista semi-estructurada, con la que se buscará indagar en la situación actual de persecución de la ciberdelincuencia en el sistema penal paraguayo. Se hará énfasis en la aplicación

de la legislación sustantiva y procesal en el sistema penal, a la vez que se explorará la existencia de protocolos normativos que robustezcan la legislación local con miras a la implementación del Convenio de Budapest.

Así como identificar limitaciones de la convención y desafíos en su implementación. La duración de las entrevistas son de una hora y serán nominales o anónimas. Este criterio será decisión de la persona entrevistada.

Una tercer herramienta metodológica será la solicitud de acceso a la información pública[17] que buscará complementar la información de las entrevistas. También será una forma de conseguir información a través de un mecanismo legal para el caso de las instituciones que no respondan o que se nieguen a la entrevista.

MARCO MUESTRAL

Se realizó un marco muestral teórico de servidores y servidoras públicas, para la realización de entrevistas porque son los involucrados en la aplicación del sistema penal. El mismo es el siguiente: Ministerio Público a través de la unidad especializada de Delitos Informáticos y Dirección de Medicina Legal y Ciencias Forenses, Poder judicial (juez de garantía penal ordinario), Policía Nacional, Secretaría Nacional Antidroga (SENAD), Centro de Respuestas Ante Incidentes Cibernéticos (CERT) y Ministerio de Relaciones Exteriores (MRE).

A medida que se avanzó en las entrevistas y a partir de las dificultades y posibilidades de contactar a los entrevistados, el número de instituciones se redujo a 5: Ministerio Público, Policía Nacional, Centro de Respuestas Ante Incidentes Cibernéticos y Jueces de Garantías. Sobre este último punto, se realizaron 2 entrevistas a jueces de garantías penal ordinario del Poder Judicial. En este punto se se consideró saturada la muestra para los objetivos fijados en la investigación. Por otro lado, la Secretaría Nacional Antidrogas (SENAD) no accedió a la entrevista y tampoco respondió la consulta a través del portal de acceso a la información pública.

Además se solicitó información relativa la investigación través del portal público información pública al Ministerio Público, de la Policía Nacional y Ministerio de Relaciones Internacionales.

ANÁLISIS DEL MARCO LEGAL

Lo que sigue a continuación es un análisis legal sobre la normativa nacional vigente en el ámbito de los ciberdelincuencia y que guarda relación directa con nuestro objeto de estudio, que es la capacidad de armonización del Convenio en el sistema penal paraguayo.

El Convenio es el primer tratado internacional tratar de abordar la delincuencia informática y los delitos informáticos mediante la armonización leyes naciona-

17 Portal de Acceso a la Información Pública: www.informacionpublica.paraguay.gov.py/portal

les, mejorando las técnicas de investigación y aumentando cooperación entre las naciones.Según se define en el preámbulo del convenio, la armonización en ciberdelincuencia se logra tipificando conductas de delitos informáticos similares en todos los países. Asimismo, la "ley tipo" o modelo de ley del Convenio, no es auto aplicativo, el mismo debe pasar por procesos cuidadosos de armonización de la legislación interna para implementarlo en el ordenamiento jurídico nacional.

1. NORMATIVAS NACIONALES VIGENTES

1.1 LA CONSTITUCIÓN NACIONAL Y TRATADOS INTERNACIONALES SOBRE LOS DERECHOS HUMANOS

En el ámbito internacional existe una serie de tratados que expresamente contemplan la protección de la vida privada como por ejemplo, la Declaración Universal de Derechos Humanos (ONU, 1948), en cuyo artículo 12 señala que nadie será objeto de injerencias arbitrarias en su vida privada, lo que es recogido por el Pacto Internacional de Derechos Civiles y Políticos de Naciones Unidas (art. 17 inc. 1) (ONU, 1966) y la Convención Americana de Derechos Humanos (art. 11 inc. 2) (OEA, 1969). Todos estos tratados y convenciones han sido ratificados por Paraguay, lo que implica que pasa a ser parte de su sistema nacional legal.

En la reforma constitucional del año 1992, se incorporan a la Constitución Nacional (CN) (Asamblea Constituyente, 1992) las siguientes figuras:

Art 33 - Derecho a la Intimidad - "La intimidad personal y familiar, así como el respeto a la vida privada, son inviolables. La conducta de las personas, en tanto no afecte al orden público establecido en la ley o a los derechos de terceros, está exenta de la autoridad pública. Se garantizan el derecho a la protección de la intimidad, de la dignidad y de la imagen privada de las personas".

Art 36 – Inviolabilidad del patrimonio documental y de la comunicación privada: "El patrimonio documental de las personas es inviolable. Los registros, cualquiera sea su técnica, los impresos, la correspondencia, los escritos, las comunicaciones telefónicas, telegráficas o de cualquier otra especie, las colecciones o reproducciones, los testimonios y los objetos de valor testimonial, así como sus respectivas copias, no podrán ser examinados, reproducidos, interceptados o secuestrados sino por orden judicial para casos específicamente previstos en la ley, y siempre que fuesen indispensables para el esclarecimiento de los asuntos de competencia de las correspondientes autoridades. La ley determinará modalidades especiales para el examen de la contabilidad comercial y de los registros legales obligatorios. Las pruebas documentales obtenidas en violación a lo prescripto anteriormente carecen de valor en juicio.

En todos los casos se guardará estricta reserva sobre aquello que no haga relación con lo investigado".

Art 23 – De la prueba de la verdad: "La prueba de la verdad y de la notoriedad no serán admisibles en los procesos que se promoviesen con motivo de publicaciones de cualquier carácter que afecten al honor, a la reputación o a la dignidad de las personas, y que se refieran a delitos de acción penal privada o a conductas privadas que esta Constitución o la ley declaran exentas de la autoridad pública. Dichas pruebas serán admitidas cuando el proceso fuera promovido por la publicación de censuras a la conducta pública de los funcionarios del Estado, y en los demás casos establecidos expresamente por la ley".

Art 28 - Del derecho a Informarse (párrafo final): "(...) Toda persona afectada por la difusión de una información falsa, distorsionada o ambigua tiene derecho a exigir su rectificación o su aclaración por el mismo medio y en las mismas condiciones que haya sido divulgada, sin perjuicio de los demás derechos compensatorios".

Como puede observarse, Paraguay cuenta con fuerte protección constitucional a la intimidad y la inviolabilidad de la comunicación de las personas, así como el derecho a la autodeterminación informativa (Acuña et al., 2017).

1.2 Otras convenciones ratificadas por el Paraguay que se aplican en la lucha transnacional contra el cibercrimen

Se hace imposible luchar contra el cibercrimen transnacional sin un estándar de la legislación penal sobre delitos cibernéticos a nivel internacional. En ese marco, Paraguay ha firmado adhesiones a convenciones que persiguen hechos delictivos a nivel Internacional. Analizaremos las más relevantes[18] que guardan relación con el objeto de estudio.

1.2.1 Convención de las Naciones Unidas contra la delincuencia organizada transnacional

La convención de las Naciones Unidas contra la delincuencia organizada transnacional (Naciones Unidas, 2000) es el principal instrumento internacional en la lucha contra la delincuencia organizada transnacional y entró en vigor el 29 de septiembre de 2003. Paraguay la ratificó a través de la ley Nº 2298 (Congreso Nacional, 2003) en el año 2004[19].

Esta convención se complementa con 3 Protocolos, que se centran en áreas específicas de crimen y sus manifestaciones: el "Protocolo para prevenir, reprimir

18 Se cita una ley que no se desarrollará en el análisis pero complementa otras convenciones que luchan contra la delincuencia en Internet: Ley No. 2378/04 que aprueba la Convención para prevenir y sancionar los actos de terrorismo configurados en delitos contra las personas y la extorsión conexa cuando estos tengan trascendencia internacional. Disponible en http://cambiosalberdi.com/downloads/Ley_2378_04.pdf [Fecha de consulta: 8 de Febrero, 2018].

19 Cuadro de los Estados Americanos partes de la Convención de las Naciones Unidas contra la delincuencia organizada transnacional y sus protocolos. Disponible en http://www.acnur.org/t3/fileadmin/Documentos/BDL/2014/9505.pdf?view=1 [Fecha de consulta: 8 de Febrero, 2018].

y sancionar la trata de personas Personas", especialmente mujeres y niños; el "Protocolo contra el Contrabando de migrantes por tierra, mar y aire"; y el "Protocolo contra la fabricación y el tráfico ilícitos de armas de fuego, sus partes y componentes y municiones".

La Convención representa un importante avance en la lucha contra crimen organizado transnacional y significa el reconocimiento por parte de los Estados miembros de la gravedad de los problemas que plantea, así como de la necesidad fomentar y mejorar la estrecha cooperación internacional para abordar esos problemas. Considerando que el cibercrimen es también un tipo de delito transnacional, el mismo debe ser incluido en las aplicaciones a nivel nacional en el marco de las disposiciones de la Convención.

Un gran número de países buscan desarrollar una Convención en la ONU o fortalecer la Convención de Naciones Unidas contra la delincuencia organizada transfronteriza, para fortalecer esta Convención en el combate del delito cibernético, a la vez que excluir las disposiciones más controvertidas del actual convenio de Budapest (Krutskikh, 2015).

1.2.2 LA CONVENCIÓN INTERAMERICANA SOBRE LA ASISTENCIA MUTUA EN MATERIA PENAL

La "Convención Interamericana sobre la Asistencia mutua en materia Penal", comúnmente denominada Convención de Nassau (OEA, 1992), fue ratificada en el año 2004[20] por Paraguay.

A su vez, debe tenerse presente que la OEA ha creado y mantiene la llamada "Red Hemisférica de Intercambio de Información para la Asistencia Mutua en Materia Penal y Extradición", que será objeto de un análisis más detallado al tratar las herramientas institucionales de apoyo a la cooperación judicial.

No obstante, el principal interés de este tratado internacional resulta de su esfuerzo de sistematización multilateral de las normas de asistencia judicial en materia penal y de su pretensión de vigencia continental.

La "Convención Interamericana sobre la Asistencia mutua en materia Penal" no establece que deba existir doble tipicidad penal para la cooperación transfronteriza. No obstante tiene muchas más excepciones que el Convenio de Budapest sobre este punto, generando un doble estándar de aplicación.

Artículo 5 de la Convención Interamericana sobre la Doble Incriminación:

> "La asistencia se presentará aunque el hecho que la origine no sea punible según la legislación del Estado requerido. Cuando la solicitud de asistencia se refiera a las siguientes medidas:

20 Cuadro de información general de la Convención de Nassau. Disponible en https://www.oas.org/juridico/spanish/firmas/a-55.html [Fecha de consulta: 8 de Febrero, 2018].

a) Embargo y secuestro de bienes; e,

b) Inspecciones e incautaciones, incluidos registros domiciliarios y allanamientos, el Estado requerido podrá no prestar la asistencia si el hecho que origine la solicitud no fuera punible conforme a su ley".

Y luego el Artículo. 6:

> "Para los efectos de esta convención, el hecho debe ser punible con pena de un año o más de prisión en el Estado requirente".

Este aspecto debe ser especialmente subrayado, ya que en materia de extradición, respecto de todos estos actos no rige el principio de doble incriminación. Por tanto la Parte requerida debe prestar asistencia, aunque el hecho no sea punible en la legislación interna. Sin embargo, a pesar de que no rija este principio, se producen algunos efectos determinados tanto en el artículo precedente como en el artículo 9 – Denegación de asistencia, que refiere a las causas de denegación facultativa de asistencia resultantes de la aplicación del principio de non bis in idem de la Convención.

1.2.3 Protocolo de San Luis sobre Ayuda Jurídica Mutua en Asuntos Penales - MERCOSUR

Este protocolo nace hace años luego de la constitución del Mercado Común del Sur (MERCOSUR) en el año 1991. El Protocolo del San Luis (MERCOSUR, 1996) fue ratificado por Paraguay en el año 1997. Los aspectos principales de este protocolo coinciden con la Convención de Nassau.

El artículo 5 del protocolo expresa:

1. El Estado Parte requerido podrá denegar la asistencia cuando:

a) la solicitud se refiera a un delito tipificado como tal en la legislación militar pero no en su legislación penal ordinaria;

b) la solicitud se refiera a un delito que el Estado requerido considerare como político o como delito común conexo con un delito político o perseguido con una finalidad política;

c) la solicitud se refiera a un delito tributario;

d) la persona en relación a la cual se solicita la medida ha sido absuelta o ha cumplido condena en el Estado requerido por el mismo delito mencionado en la solicitud. Sin embargo, esta disposición no podrá ser invocada para negar asistencia en relación a otras personas; o

e) el cumplimiento de la solicitud sea contrario a la seguridad, el orden público u otros intereses esenciales del Estado requerido.

2.- Si el Estado requerido deniega la asistencia, deberá informar al Estado requirente por intermedio de la Autoridad Central, las razones en que se funda la denegatoria, salvo lo dispuesto en el artículo 15, literal b)

Es decir, que si no existiere la doble incriminación en una de las Partes y la parte que recibe la solicitud de cooperación mutua no cuente con la figura penal perseguido por la otra Parte, entonces se podrá negar invocando las reservas del estándar de la Convención Interamericana o el Protocolo de MERCOSUR, socavando la efectividad del Convenio de Budapest. Por tanto es necesario profundizar sobre este conflicto que se genera en la aplicación de los tratados internacionales vigentes en el país, pero excede el alcance de este investigación.

1.2.4 OTRAS NORMATIVAS DE ACUERDO DE EXTRADICIÓN FIRMADOS POR PARAGUAY

Paraguay es parte de la "Convención Interamericana sobre Extradición", del "Acuerdo de Extradición Centroamericano" de 1924 y del "Tratado de Extradición" de 1903, cuyos instrumentos reconocen y facilitan mutuamente la extradición penal de personas sujetas a procesos legales con la gran mayoría de Países latinoamericanos. Asimismo, nuestro país ha suscrito y ratificado tratados y convenciones de extradición sobre cooperación judicial internacional en materia penal con los siguientes países: Argentina, Brasil, Canadá, Chile, Colombia, Costa Rica, Ecuador, España, Estados Unidos, México, Panamá, Perú, Uruguay y Venezuela[21].

1.3 EL CÓDIGO PENAL

Esta legislación aplicable en materia penal contempla normas jurídicas punitivas que protegen el patrimonio y la intimidad en la jurisdicción paraguaya que pueden ser aplicadas en el ámbito cibernético y que complementa los delitos informáticos propiamente dichos.

La ley N° 1160 (Congreso, 1997) del Código Penal, a través de su modificación Ley Nº 3440 (Congreso Nacional, 2008) tipifica en el capítulo VI el hecho punible contra niños y adolescentes, incluyendo a la Pornografía relativa a niños

21 La lista oficial de tratados y convenciones de extradición sobre cooperación judicial internacional en materia penal que Paraguay ha concluido y ratificado, se encuentra disponible en: https://www.oas.org/juridico/mla/en/pry/index.html

y adolescentes en su artículo 140[22]. La misma tuvo una segunda modificación Ley Nº 4439 (Congreso Nacional, 2011) que incluyó re-formulaciones en los primeros párrafos y se introdujo el aumento de las penas.

El Convenio, a través del artículo 9 relacionado con pornografía infantil, sugiere la tipificación de la misma. Entonces la norma paraguaya cumple con la armonización, aunque muy distante en el abordaje sustantivo sugerido, porque pareciese que el Legislador ha tomado las mismas reservas expuestas más arriba, al igual que otros países con relación a este hecho punitivo.

También se encuentra el capítulo VII los hechos punibles contra el ámbito de vida y la intimidad de la persona (Congreso, 1997). Entre ellos están, artículo 141.- Violación de domicilio,artículo 144.- Lesión del derecho a la comunicación y a la imagen, artículo 146.- Violación del secreto de la comunicación y el artículo 143.- Lesión a la intimidad de la persona. Este último hace alusión directa a la exposición pública de la intimidad de la persona, de su vida familiar, sexual y su estado de salud.

Es importante recalcar que la Ley Nº 4439/11 es la que introduce los delitos informáticos en la legislación nacional. Sin embargo, no se contempla expresamente el concepto de ciberdelito ni delito informático en ningún parte de la ley, sino que se definen las distintas conductas delictivas en las que interviene de alguna manera una actividad relacionada con las nuevas tecnologías de la información y las comunicaciones. Se centra en la protección mediante el derecho penal de datos y sistemas informáticos, excluyendo a los delitos cibernéti-

22 Esta ley es complementada con las siguientes normas:
Ley 1680 / 2001 Código de Niños y Adolescentes (Artículos 31 y 32),
La ley Nº 2861/2006 "Que reprime el comercio y la difusión comercial o no comercial de material pornográfico, utilizando la imagen u otra representación de menores o incapaces". Disponible en www.oas.org/juridico/spanish/cyb_par_ley_2861_2006.pdf,
La ley 57/1990 por la que se aprueba y ratifica la "Convención de las Naciones Unidas sobre los Derechos del Niño", y se protege a niños y menores de todas las formas de explotación y abuso sexuales (artículos 34 y 36).
La Ley N° 2134/2003 que aprueba el "Protocolo facultativo de la Convención sobre los Derechos del Niño" relativo a la venta de niños, la prostitución infantil y el uso de niños en la pornografía en los arts. 1, 2, 3 y 10.
Ley Nº 5653/16 "De protección de los niños, niñas y adolescentes contra contenidos nocivos de Internet". Disponible en http://www.bacn.gov.py/leyes-paraguayas/5167/proteccion-de-ninos-ninas-y-adolescentes-contra-contenidos-nocivos-de-internet Esta normativa fue muy polémica ver más información en https://www.tedic.org/censurar-internet-para-proteger-a-ninos-y-ninas-no-es-la-solucion
Regulación del art. 32 de la Ley N° 1.680/01 del "Código de Niños, Niñas y Adolescentes" con el objetivo de establecer medidas técnicas y administrativas para evitar el acceso a niños y adolescentes a cualquier tipo de información o material pornográfico (Ordenanza municipal núm. 259, de 16 de abril de 2005, por la que se medidas para evitar el acceso de niños y adolescentes a material pornográfico a través de Internet. Regula el artículo 32 de la Ley Nº 1680/01 y establece sanciones para aquellos que prestan dichos servicios sin el filtro).
Registro ante CODENI de establecimientos que ofrecen servicios de Internet de manera comercial o gratuitos al público en la ciudad de Asunción, de los cuales deben tener una dirección de IP pública debidamente provista por el ISP que brinda el servicio de Internet (Ordenanza Municipal Nº 287 , de 30 de mayo de 2006 por la que se modifica el artículo 3 de la Ordenanza municipal Nº 259/05).

cos en general. Se espera que con el Convenio se pueda profundizar elementos ausentes o pocos claros en los tipificación y la graduación de las penas de la legislación nacional.

El artículo 146b del código penal paraguayo sobre el Acceso indebido a datos, se tipifica y se adapta a la recomendación del art. 2 del Convenio, sancionando dicha conducta con hasta 3 años de pena privativa de libertad o multa. El artículo dice:

> "1º El que sin autorización y violando los sistemas de seguridad obtuviere para sí o para terceros, el acceso a datos no destinados a él y especialmente protegidos contra el acceso no autorizado, será castigado con pena privativa de libertad de hasta 3 años o multa. 2º Como datos en sentido del inciso 1º se entenderá sólo aquellos, que se almacenen o transmiten electrónicamente, magnéticamente o de otra manera no inmediatamente visible"

Por otra parte el art. 146c del código penal relacionado a la Interceptación de datos, no satisface los requerimientos señalados en el artículo 3 de la Convención, por tener serios problemas de forma y fondo que pueden conllevar interpretaciones erróneas. En especial, la ambigüedad del texto se encuentra en los incisos 2° y 3° que se exponen a continuación:

> "El que sin autorización y utilizando medios técnicos: 1º obtuviere para sí o para tercero, datos en el sentido del Artículo 146 b,inciso 2º, no destinados para él; 2º diera a otro una transferencia no pública de datos; o 3º transfiera la radiación electromagnética de un equipo de procesamiento de datos, será castigado con pena privativa de libertad de hasta dos años o multa, salvo que el hecho sea sancionado por otra disposición con una pena mayor"

La ambigüedad, la expresa abogado Ricardo Preda[23] de la siguiente forma:

> "Erróneamente el legislador enunció los incisos 2° y 3° del 146c de una manera tal que lo que se tipifican son: a) dar a otro un transferencia no pública de datos b) transferir la radiación electromagnética. Sin embargo, lo que se debe castigar es la obtención con medios técnicos de datos no autorizados, cuando estos provengan de: a) una transmisión no pública de datos, o b) de la emisión electromagnética de un sistema de procesamiento de datos".

Sobre el artículo 146d del código penal paraguayo Preparación de acceso indebido e interceptación de datos afirma lo siguiente:

---

23 Ley contra los delitos informáticos. Breve reseña. Abogado Ricardo Preda. Enero 2012. Disponible en http://www.abc.com.py/articulos/ley-contra-los-delitos-informaticos-breve-resena-358709.html [Fecha de consulta: 8 de Febrero, 2018].

> "1º El que prepare un hecho punible según el Artículo 146b o el Artículo 146c produciendo, difundiendo o haciendo accesible de otra manera a terceros:
>
> las claves de acceso u otros códigos de seguridad, que permitan el acceso a datos en sentido del Artículo 146 b, inciso 2º; o
>
> los programas de computación destinados a la realización de tal hecho, será castigado con pena privativa de libertad de hasta un año o multa
>
> 2º Se aplicará, en lo pertinente, lo preisto en el artículo 266, inciso 2º y 3º"

Este artículo busca tipificar como delito el acto de fabricar, diseñar, desarrollar o utilizar un software de "hacking"[24], con un castigo de hasta un año de prisión. Sin embargo este artículo no incluye excepciones sobre el hacking ético[25] o prueba de vulnerabilidad para detectar vacíos que pueda tener un sistema informático. El Convenio cuenta con una norma similar pero incluye esta excepción expresa en su artículo 6 punto 2:

> "No se interpretará que el presente artículo impone responsabilidad penal cuando la producción, venta, obtención para la utilización, importación, difusión o cualquier otra forma de puesta a una disposición mencionada en el párrafo 1 del presente artículo no tenga por objetivo la comisión de uno de los delitos previstos en la conformidad con el artículo 2 a 5 del presente Convenio, como en el caso de las pruebas autorizadas o de la protección de un sistema informático".

La interpretación del artículo 146d debe saber conjugar la intención o no de hacer un daño a los sistemas informáticos, centrándose en la conducta como cumplimiento de los presupuestos del tipo penal.

Vale la pena también analizar el artículo 174b – Acceso indebido a sistemas informáticos que expresa lo siguiente:

> "1º el que accediere a un sistema informático o a sus componentes, utilizando su identidad o una ajena; o excediendo una autorización, será castigado con pena privativa de libertad de hasta tres años o multa.

---

24 Cabe diferenciar los verbos hackear y crackear así como los sustantivos hacker y cracker. Hacker se suele entender como "pirata informático" mientras que existen personas y movimientos que se enfrentan a dicho concepto por dos razones: primero por utilizar la palabra pirata que ya tiene una acepción de "asaltante de barcos" y en segundo lugar por la connotación negativa de invasión ilegítima de sistemas que suelen imputar a los crackers. Los hackers por el contrario se auto-definen como apasionados en resolver problemas, con una ética específica del trabajo y el uso del tiempo. Para más detalles consultar "La ética del hacker y el espíritu de la era de la información" (Himanen, Pekka, 2001).

25 Existe otro concepto más concreto y acotado que es el de Hacking ético. En este caso sería la utilización de conocimiento informático para realizar pruebas de seguridad en redes y encontrar vulnerabilidades, para luego reportarlas, sin hacer daño a los sistemas.

2º Se entenderá como sistema informático a todo dispositivo aislado o al conjunto de dispositivos interconectados o relacionados entre sí, cuya fusión, o la de algunos de los componentes, sea el tratamiento de datos por medio de un programa informático"

Dicho artículo se encuentra en la parte de "Hechos punibles contra otros derechos patrimoniales" del código penal paraguayo, no obstante su descripción guarda una mayor relacióncon el derecho a la intimidad, por lo que confunde el espíritu de la conducta castigada. Además el objetivo de este hecho punible ya se encuentra tipificado en el artículo reseñado anteriormente (art 146b).

Por otra parte, en el inciso 2º se define el concepto de sistema informático de tal forma que una computadora entra en dicha definición. Por lo tanto, si una persona accede a una computadora consistema con su identidad estaría cumpliendo la condición de este dispositivo penal. De tal forma, este hecho punible es inconsistente y absurdo.

Si se analiza el Artículo 175 Sabotaje de sistemas informáticos, se observa una modificación por laley 4439/11 que cambia la denominación de "Sabotaje de computadoras" a "Sabotaje de sistemas informáticos". Esto provoca la ampliación de su aplicación penal.

El Artículo 175b – Instancias expresa:

> "En los casos de los Artículos 174 y 175, la persecución penal dependerá de la instancia de la víctima; salvo que la protección del interés público requiera la persecución de oficio".

Es importante recalcar que el artículo Nº 174b que se refiere al "Acceso indebido a sistemas informáticas" no se incluye en este artículo. Se desconoce si el legislador pretendía el objetivo de que sea tipificado como acción penal privada.

Por otra parte se encuentra el artículo Nº 188 que en su versión original era denominado "Operaciones fraudulentas por computadoras" y fue modificado por la ley 4439/11, pasando a denominarse: "Estafa mediante sistemas informáticos". El contenido del tipo penal se mantuvo en líneas generales, con algunos nuevos incisos, vinculando a los actos preparatorios de la tipificación y sus excepciones.

El artículo Nº 248b - Falsificación de tarjetas de débito o de crédito y otros medios electrónicos de pago crea una nueva conducta anti-jurídica, que busca castigar cualquier falsificación o alteración de los medios de pago electrónico, así como la forma de adquirir, ofrecer, entregar y utilizar, siempre y cuando el sujeto actúe con dolo.

Por otra parte, el artículo N° 249 - Equiparación para el procesamiento de datos, aborda la manipulación que perturbe un procesamiento de datos conforme al artículo 174, inciso 3º que será equiparada a la inducción al error en las

relaciones jurídicas.

El artículo N° 253 - Destrucción o daño a documentos o señales

"1º El que con la intención de perjudicar a otro: 1. destruyera, dañara, ocultara o de otra forma suprimiera un documento o una graficación técnica, en contra del derecho de otro a usarlo como prueba; 2. borrara, suprimiera, inutilizara o alterara, en contra del derecho de disposición de otro, datos conforme al artículo 174, inciso 3º, con relevancia para la prueba; o 3. destruyera o de otra forma suprimiera mojones u otras señales destinadas a indicar un límite o la altura de las aguas, será castigado con pena privativa de libertad de hasta cinco años o con multa

2º En estos casos, será castigada también la tentativa"

Estos artículos que preceden no se han profundizado por autoexplicarse y ser claros en la tipificación de la modificación del código penal paraguayo.

Y por último, se encuentran los delitos contra la propiedad intelectual que ingresaron al cuerpo legislativo penal a través de la Ley Nº 3440 (Congreso Nacional, 2008)y se encuentran en el artículo Nº 184 del capítulo sobre Propiedad intelectual:el artículo 184a – Violación del Derecho del Autor y hechos conexos, artículo 184b – Violación de los derechos de marca, artículo 184c – Violación sobre los derechos de dibujos y diseños industriales[26].

En resumen, hasta la fecha el legislador no se ha hecho cargo de las deficiencias y errores de la actual normativa sobre los delitos informáticos. También es cierto que ninguna de las críticas expuestas en los párrafos precedentes son novedosas. Sin embargo hay supuestos legales que no se encuentran necesariamente tipificados en el Código Penal, sino que se debe acudir a legislaciones complementarias que regulan la sociedad de la información, entre ellas: datos personales, comercio electrónico, responsabilidad del intermediario en Internet, etc..

1.4 CÓDIGO PROCESAL PENAL

Entre los artículos del Código procesal penal (CPP) (Congreso Nacional, 1998a) que se aplican para la investigación y persecución del cibercrimen se encuentran:

El artículo 173 del CPP, es denominado Libertad probatoria y permite la admisibilidad en los procesos y juicios penales de pruebas electrónicas, expresando que cualquier medio de prueba será admitido si se refiere directa o indirectamente, al objeto de la investigación penal, siempre que no se vulneren garantías procesales consagradas en la Constitución Nacional, en el Derecho inter-

26 Se complementa con la Ley N° 1328/98: De Derecho de Autor y Derechos Conexos. Disponible en http://www.wipo.int/wipolex/es/text.jsp?file_id=129428 [Fecha de consulta: 8 de Febrero, 2018].

nacional vigente y las leyes.

Otros artículos a citar son el artículo 183 y 192 del CPP, que permiten el registro de un lugar y se podrán ordenar operaciones técnicas o científicas a los efectos de una mayor eficacia y calidad de los registros e inspecciones.

Por otro lado se encuentran los artículo 52 a 57 del CCP que otorgan facultades a los fiscales para integrar los elementos necesarios de una investigación en un proceso penal. También se pueden observar los artículos 195 a 186 del CPP que generan el procedimiento para la búsqueda e incautación de personas y objetos.

A continuación se listan 4 artículos que se auto-explican en relación al objeto de estudio:

Artículo 198°.- Intercepción y secuestro de correspondencia

Siempre que sea útil para la averiguación de la verdad, el juez ordenará, por resolución fundada, bajo pena de nulidad, la intercepción o el secuestro de la correspondencia epistolar, telegráfica o de cualquier otra clase, remitida por el imputado o destinada a él, aunque sea bajo nombre supuesto. Regirán las limitaciones del secuestro de documentos u objetos.

Artículo 199°.- Apertura y examen de correspondencia

Recibida la correspondencia o los objetos interceptados, el juez procederá a su apertura haciéndolo constar en acta. Examinará los objetos y leerá para sí el contenido de la correspondencia. Si guardan relación con el procedimiento ordenará el secuestro; en caso contrario, mantendrá en reserva su contenido y dispondrá la entrega al destinatario.

Artículo 200°.- Intervención de comunicaciones

El juez podrá ordenar por resolución fundada, bajo pena de nulidad, la intervención de las comunicaciones del imputado, cualquiera sea el medio técnico utilizado para conocerlas. El resultado sólo podrá ser entregado al juez que lo ordenó, quien procederá según lo indicado en el artículo anterior; podrá ordenar la versión escrita de la grabación o de aquellas partes que considere útiles y ordenará la destrucción de toda la grabación o de las partes que no tengan relación con el procedimiento, previo acceso a ellas del Ministerio Público, del imputado y su defensor. La intervención de comunicaciones será excepcional.

Artículo 228°.- Informes

El juez y el Ministerio Público podrán requerir informes a cualquier persona o entidad pública o privada. Los informes se solicitarán verbalmente o por escrito, indicando el procedimiento en el cual se requieren, el nombre del imputado, el lugar donde debe ser entregado el informe, el plazo para su presentación y las consecuencias previstas para el incumplimiento del deber de informar.

A pesar que el artículo 288 de CPP otorga potestad de solicitud de informe al Ministerio Público, en el caso de datos de tráfico o metadatos como forman parte del contenido de las comunicaciones, se debe aplicar lo expuesto en la Constitución Nacional artículo 36 de la Inviolabilidad de las Comunicaciones.

En síntesis, ni en la norma procesal penal ni en la norma penal se establece que en caso delito específico el órgano de persecución penal –Ministerio Público– pueda vulnerar el derecho a la privacidad, si no cuenta con la autorización judicial previa en el marco de una investigación criminal.

1.5. SOBRE LA INVIOLABILIDAD DE LAS COMUNICACIONES EN OTRAS NORMATIVAS

La ley N° 642/95 de Telecomunicaciones (Congreso Nacional, 1995) crea la Comisión Nacional de Telecomunicaciones (Conatel), que es el ente regulador de las telecomunicaciones en el país. Entre sus funciones está la de proteger expresamente la inviolabilidad de las comunicaciones establecida en los artículos 89 y 90 de dicha ley.Además, el Decreto del Poder Ejecutivo 14135/96 por el cual se aprueba las normas reglamentarias, de dicha ley también protege la inviolabilidad de las comunicaciones.

Estas normativas refuerzan lo establecido en la normativa procesal en cuanto a lo siguiente:

La inviolabilidad de las comunicaciones;

La obligación que tienen los prestadores públicos o privados o cualquier persona que tenga conocimiento del contenido de una comunicación de preservar y garantizar la inviolabilidad o secreto de la misma o no hacerla accesible a un tercero;

La necesidad de autorización judicial para cada caso.

1.6 OTRAS NORMATIVAS QUE COMPLEMENTAN LA ARMONIZACIÓN DEL CONVENIO

1.6.1 LEY Nº 1334 DE DEFENSA DEL CONSUMIDOR Y USUARIO

Esta normativa se armoniza con el capítulo primero en su artículo 1 – Definiciones del Convenio. El inciso C describe a los “proveedores de servicio” de la siguiente manera:

> “i. toda entidad pública o privada que ofrezca a los usuarios de sus servicios la posibilidad de comunicar a través de un sistema informático, y ii. Cualquier otra entidad que procese o almacena datos informáticos para dicho servicio de comunicación o para los usuarios del mismo”

La norma que actualmente describe al “Prestador de servicio” en la legislación

interna es la Ley 1334 “De defensa del consumidor y usuario” (Congreso Nacional, 1998b). Lo hace de la siguiente forma:

> “Tercero o Persona Jurídica pública o privada que desarrolle actividades de producción, fabricación, importación, distribución, comercialización, venta o arrendamiento e bienes o de prestación de servicios a consumidores o usuarios respectivamente por lo que cobre un precio o tarifa”

Se deberá tomar en cuenta lo citado en la sección de Reservas del Convenio sobre este artículo.

1.6.2 LA LEY Nº 4468/13 DE COMERCIO ELECTRÓNICO

Es una normativa que en el artículo 10 – Deber de retención de datos de tráfico relativos a las comunicaciones electrónicas de la Ley Nº 4468 (Congreso Nacional, 2013) , obliga a las empresas proveedoras de Internet en Paraguay (ISPs) y proveedores de servicios de alojamiento de datos a almacenar como mínimo 6 meses los datos de tráfico o “relativos a la comunicaciones electrónicas”.

Algunas ISPs en Paraguay limitan el acceso al poder judicial y policial, porque su interpretación se basa en que la misma es exclusivamente para fines comerciales (Sequera, 2017). Sin embargo, la ISP estatal COPACO facilita los datos de tráfico para las persecuciones penales solicitadas a través de pedidos de Informes del Ministerio Público[27].

Esta medida es preocupante porque se interpretan los datos de tráfico como información “insignificante” en el conjunto de la comunicación del usuario, por lo que no se considera parte de la comunicación. Como se expuso en la sección anterior “sobre los datos de tráfico o metadatos”, esto es erróneo, ya que existe jurisprudencia internacional que ha demostrado que los metadatos forman parte de la comunicación y su inviolabilidad, obligando a las autoridades penales a otorgar acceso a los mismos solo de forma excepcional y a través de una orden judicial debidamente justificada.

---

27 TEDIC ¿Se cumple el estándar de protección del tratamiento de datos de nuestras comunicaciones, cuando la fiscalía accede a nuestros datos sin orden judicial? Disponible en https://www.tedic.org/se-cumple-el-estandar-de-proteccion-del-tratamiento-de-datos-de-nuestras-comunicaciones-cuando-la-fiscalia-accede-a-nuestros-datos-sin-orden-judicial/ [Fecha de consulta: 14 de Febrero, 2018].

Esta ley se armonizaría con la Convención a través de los artículos 17 – Conservación y revelación parcial rápida de los datos relativos al tráfico, siempre y cuando se cumplan los principios de proporcionalidad de la ley y los estándares mínimos de salvaguarda de información y datos privados de los usuarios.

1.6.3 LA RESOLUCIÓN 1350/2002 DE COMISIÓN NACIONAL DE TELECOMUNICACIONES (CONATEL)

Esta resolución establece la obligatoriedad de registro de detalles de llamadas por el plazo de 6 meses por parte de las operadoras, que tendrán los datos de todos los usuarios de Paraguay:

Artículo. 1.- Establecer el plazo de seis (6) meses, como periodo obligatorio de conservación del registro de detalles de llamadas entrantes y salientes de todas las líneas que conforman la cartera de clientes de las diferentes operadoras del servicio de telefonía móvil celular (STMC) y/o Sistema de Comunicación Personal (PCS) (Conatel, 2002).

Los registros de llamadas telefónicas, los SMS y los datos de localización de dispositivos móviles ya son almacenados por un periodo de 6 meses mediante la Resolución de Conatel que data del año 2002, tiempo donde ocurrieron varios secuestros extorsivos que sacudieron a la sociedad paraguaya[28] y se forzaron a extraer los registros de llamadas a un tiempo superior a 6 meses[29] violentando principios Constitucionales y derechos humanos.

Las normas nacionales expresan que la intervención de las comunicaciones son de carácter excepcional, sin embargo la forma de interceptar las comunicaciones de forma masiva y previa a un hecho consumado para la investigación penal como esta Resolución de CONATEL contradice el Principio de Legalidad por lo expuesto en la sección anterior sobre las reservas.

1.6.4 RESOLUCIÓN 1134/2006 REGLAMENTO DEL SERVICIO DE ACCESO INTERNET COMISIÓN NACIONAL DE TELECOMUNICACIONES (CONATEL)

Art. 17: " El Prestador instalará en el país, un sistema de gestión, cuyo propósito es la gestión técnica y administrativa del servicio. El sistema deberá registrar al menos:

Habitación/deshabilitación, de estaciones del usuario, velocidad de transmisión, volumen de tráfico, datos de facturación. Se deberá mantener archivos históricos de los registros.

---

28 Última Hora. Los casos de secuestros en Paraguay. Disponible en: http://www.ultimahora.com/los-casos-secuestros-paraguay-n460811.html [Fecha de consulta: 28 de Diciembre, 2017].

29 TEDIC. Los registros de llamadas: Entre el derecho a la privacidad y la persecución de delitos. Disponible en https://www.tedic.org/los-registros-de-llamadas/ [Fecha de consulta: 8 de Febrero, 2018].

Este artículo guarda relación con el artículo 17 – Conservación y revelación parcial de los datos relativos al tráfico del Convenio en armonización de sus incisos a y b.

2. Cuadro del estado actual de armonización del Convenio en la normativa paraguaya

Capítulo I – Terminología	Si	No	Observación
Sistema informático		X	No hay definición
Datos Informáticos	X		Art. 174
Proveedor de servicios	X		Ley 1334/98 Ley de defensa de consumidor
Datos de tráfico		X	No hay definición

Capítulo II – parte sustantiva	Si	Parcial	No	Observación
Artículo 2: Acceso ilícito	X			CP Art. 174b
Artículo 3: Interceptación ilícita		X		CP Art. 146b, CP Art. 146c (Inaplicable)
Artículo 4: Ataques a la integridad de datos	X			CP Art. 175
Artículo 5: Ataques a la integridad de sistemas	X			CP Arts. 175. 175a, 175b
Artículo 6: Abuso de dispositivo	X			CP Arts. 146d y 188
Artículo 7: Falsificación informática	X			CP Arts. 248, 248b, 249 y 253
Artículo 8 Fraude informático	X			CP Art 188 y 187
Artículo 9: Pornografía infantil	X			CP Art. 140
Artículo 10: Delitos contra la propiedad intelectual y derechos afines	X			CP Arts. 184, 184a, 184b, 184c
Artículos 11: Tentativa y complicidad	X			Tentativa: Todos los artículos de delitos informático sugeridos por el Convenio. CP Art. 31 - Complicidad
Artículo 12: Tentativa y complicidad y responsabilidad de las personas jurídicas	X			CP Art. 16 – Actuación en representación de otro
Artículo 13: Sanciones y medidas	X			Ley 3440, Art. 2 – Principios de reprochabilidad CP Art. 13 – Clasificación de Hechos Punibles, CP Art. 37 – Clases de Penas, Art. 38 - Duración de la Pena Privativa de Libertad Ley 3440, Art. 30 - Objeto y Bases de la Ejecución

Sección 2 – Derecho Procesal	Si	Par-cial	No	Observaciones
Artículo 14 – Ámbito de aplicación	X			Artículos del CPP: 173 - Libertad probatoria, 176 - Inspección del lugar de los hechos, 183 – Registro, 192 – Operaciones técnicas, 195 – Orden de secuestro, 198 – Interceptación y secuestro de correspondencia, 199 Apertura de examen de correspondencia, 200 –Intervención de las comunicaciones
Artículo 15 – Condiciones y salvaguardias		X		Artículos de la Constitución Nacional: 33 – Derecho a la Intimidad, 36 – Inviolabilidad del patrimonio documental y de la comunicación privada, 16 – De la defensa en juicio, 17 – De los Derechos procesales, 18 – De las restricciones de la declaración, 19 – De la prisión preventiva, 20 – El objeto de las penas, 21 – De las reclusión de personas, 30 – De las señales de comunicación electromagnética CPP Art 1 – Juicio Previo Ley N° 642/95 de Telecomunicaciones: Arts. 89 y 90. Decreto del Poder Ejecutivo 14135/96, Art. 9. Ley 5241/14 – Que crea el Sistema Nacional de Inteligencia, Art. 6. No cuenta con una ley de protección de datos personales y tampoco con supervisión independiente para la vigilancia de las comunicaciones.
Artículo 16 – Conservación rápida de datos informáticos almacenados		X		No cuenta con una regulación para la conservación rápida de datos de tráfico en Internet. En su defecto se aplica el Art 36 de la CN – Inviolabilidad de las Comunicaciones, excepto por orden judicial para los casos de conservación de datos de tráfico a partir de la sospecha o en tiempo real. La resolución 1350/2002 de CONATEL, Art. 1 – Retención de datos de registro de llamadas telefónicas durante 6 meses.

Artículo 17 – Conservación y revelación parcial rápida de los datos relativos al tráfico		X		CN Art. 36 –Inviolabilidad de las Comunicaciones, excepto por orden judicial. CPP Art200 -Intervención de las comunicaciones para los casos de conservación a partir de la sospecha o en tiempo real. Art 228 – Informe: Para casos que no corresponden a datos de tráfico pero se encuentran en poder de la ISP. La ley Nº 4468/13 de Comercio electrónico, Art. 10, excluye a casos penales (Salvo la ISP COPACO). La resolución 1350/2002 de CONATEL, Art. 1 – Retención de datos de registro de llamadas telefónicas durante 6 meses. Resolución 1134/2006 "Reglamento del Servicio de Acceso Internet"Art. 17.
Art 18 – Orden de presentación	X			CPP: Para casos de datos de tráfico (parte de la comunicación) Art. 42 – Jueces Penales: Competencia para actuar como juez de garantías y del control de la investigación. Art. 228 – Informe: Para casos que no corresponden a datos de tráfico pero se encuentran en poder de las ISP. Art. 52 – Funciones de Investigación (Ministerio Público). Art. 58 – Función (Policía Nacional). Ley Nº 1881 Que Modifica La Ley Nº 1340/88 – Ley especial sobre represión al tráfico de drogas y estupefacientes (SENAD) Arts. 88, 89 y 91. Ley 5241/14 – Que crea el Sistema Nacional de Inteligencia: Arts.24, 25, 26 y 27.
Artículo 19 – Registro y confiscación de datos informáticos almacenados	X			CPP: Art. 183 – Registro, Art. 192 – Operaciones técnicas, Art. 195 – Orden de secuestro, Art. 193 – Entrega de cosas y documentos Art. 196 – Procedimiento (orden judicial) Art. 198 – Interceptación y secuestro de correspondencia
Artículo 20 – Obtención en tiempo real de datos relativos al tráfico	X			No cuenta con una regulación para la conservación rápida de datos de tráfico en Internet. En su defecto se aplica el Art. 36 de la CN –Inviolabilidad de las Comunicaciones, excepto por orden judicial para los casos de conservación de datos de tráfico a partir de la sospecha o en tiempo real. La resolución 1350/2002 de Conatel, Art. 1 – Retención de datos de registro de llamadas telefónicas durante 6 meses.

Artículo 21 – Interceptación de datos relativos al contenido	X			CPP: Art. 198 – Interceptación y secuestro de correspondencia, Art. 199 – Apertura de examen de correspondencia, Art.200 –Intervención de las comunicaciones Ley 5241/14 – Que crea el Sistema Nacional de Inteligencia: Arts.24, 25, 26 y 27. Ley Nº 1881 Que Modifica La Ley Nº 1340/88 – Ley especial sobre represión al tráfico de drogas y estupefacientes (SENAD) Arts. 88, 89 y 91.
Artículo22 – Jurisdicción	X			Ley 3440 Art. 6 – Hechos realizados en el territorio Nacional CP Art. 7 – Hechos realizado en el extranjero con bienes jurídicos paraguayos Ley 3440, Art. 8 – Hechos realizados en el extranjero con bienes jurídicos con protección universal. Ley 3440 Art .9 – Otros Hechos realizados en el extranjero. CP Art 11. – Lugar del Hecho
Artículo 24 – Extradición	X			CPP: Art. 146 – Exhorto Art. 147 – Extradición Art. 148 – Extradición activa Art. 150 – Medidas cautelares Lista de convenio de extradición con países: Argentina, Brasil, Canadá, Chile, Colombia, Costa Rica, Ecuador, España, Estados Unidos, México, Panamá, Perú, Uruguay y Venezuela. La lista oficial de tratados y convenciones de Extradición sobre cooperación judicial internacional en materia penal que Paraguay ha concluido y ratificado, se encuentra disponible en: https://www.oas.org/juridico/mla/en/pry/index.html

Artículo 25 – Principios generales relativos a la asistencia mutua	X			CPP Art. 143 - Principios Generales Multilaterales: Convención de las Naciones Unidas contra la delincuencia organizada transnacional, año 2000 La Convención Interamericana sobre la Asistencia mutua en materia Penal, 1992 Protocolo de San Luis sobre Ayuda Jurídica Mutua en Asuntos Penales, MERCOSUR,1996 Protocolo de asistencia jurídica mutua en asuntos penales Convención Interamericana sobre recepción de pruebas en el extranjero Convención Interamericana para el cumplimiento de condenas penales en el extranjero Convenio sobre extradición de Montevideo, suscrito en Montevideo,Uruguay, 1933 Convención Interamericana de recepción de pruebas en el extranjero, adoptada en la ciudad de Panamá, 1975 Protocolo adicional a la Convención Interamericana de recepción de pruebas en el extranjero, suscrito en la ciudad de la Paz, Bolivia, 1984 Convención Interamericana contra corrupción Convención internacional contra la toma de rehenes, Nueva York, 1979. D.O. No.217, de fecha 18 de noviembre de 1980 Convenio internacional para la represión de la financiación del terrorismo Protocolo adicional a la Convención Interamericana sobre exhortos o cartas rogatorias, adoptado en Montevideo, Uruguay, 1979 Convención Interamericana sobre exhortos o cartas rogatorias, adoptada en Panamá, 1975 Convención contra la delincuencia organizada transnacional, 2003 Convención Interamericana contra la fabricación y el tráfico ilícito de armas de fuego, municiones, explosivos y otros materiales relacionados, suscrita en Washington D.C., 1997 Bilaterales Argentina: Convenio con Paraguay sobre legalización de firmas en comisiones rogatorias, Ley 24.968, 10.081, 1916 Convenio de asistencia judicial con Paraguay, Ley 24.847, 1997 Colombia: Acuerdo de cooperación para la prevención, control y represión del lavado de activos derivado de cualquier actividad ilícita entre el Gobierno de la República de Colombia y el Gobierno de la República del Paraguay Costa Rica: Acuerdo de Cooperación para la Lucha contra el Tráfico Ilícito de Estupefacientes y Sustancias Psicotrópicas, y Delitos Conexos entre la República de Costa Rica y la República del Paraguay Convenio sobre Asistencia Judicial en Materia Penal entre la República del Paraguay y la República de Costa Rica Ecuador: Acuerdo de cooperación para la lucha contra el trafico ilícito de estupefacientes y sustancias psicotrópicas, y delitos conexos entre la República del Ecuador y la República del Paraguay, firmado en la ciudad de Asunción, 1997 Convenio sobre asistencia judicial en materia penal con Paraguay, firmado en la ciudad de Asunción, 1997 Perú: Convenio entre la República del Paraguay y la República del Perú sobre Asistencia Judicial en Materia Penal Uruguay: Convenio de Asistencia Judicial Internacional entre las Autoridades Centrales de la República Oriental del Uruguay y de la República del Paraguay

Artículo 26 – Información espontánea	X			Ministerio de Defensa Nacional, Ministerio de Relaciones Exteriores y Organismos competentes internacionalmente: INTERPOL
Artículo 27 – Procedimientos relativos a las solicitudes de asistencia mutua en ausencia de acuerdos internacionales aplicables.			X	No se aplica[1]
Artículo 28 – Confidencialidad y restricciones de uso		X		Art. 148 – Revelación de secretos privados por funcionarios o personas con obligación especial. Ley 3440. Ley Nº 5241/14 Que crea el Sistema Nacional de Inteligencia: Art. 22–Modalidad. Los documentos, expedientes y archivos relativos a actividades de inteligencia y contrainteligencia, tendrán carácter reservado de hasta un plazo máximo de 20 (veinte) años. Art. 23–Obligación de guardar secreto. Los funcionarios y demás personal de las instituciones que integran el Sistema Nacional de Inteligencia (SINAI).
Artículo 29 – Conservación rápida de datos informáticos almacenados			x	Al finalizar la presente investigación no se ha encontrado información acerca de los mecanismos alternativos en caso de ausencia de Tratados de asistencia legal mutua (MLAT)
Artículo 30 – Revelación rápida de datos conservados			x	idem
Artículo 31 – Asistencia mutua en relación con el acceso a datos almacenados			x	idem
Artículo 32 – Acceso transfronterizo a datos almacenados con consentimiento o cuando sean accesibles al público			x	idem
Artículo 33 – Asistencia mutua para la obtención en tiempo real de datos relativos al tráfico			x	idem
Artículo 34 – Asistencia mutua en relación con la interceptación de datos relativos a contenido			x	idem
Artículo 35 – Red 24/7	x			El Ministerio Público a través de la Unidad especializada de delitos informático es la Institución asignada, a través del REMJA2

3. INSTITUCIONES NACIONALES PARA LA PERSECUCIÓN DEL CIBER-CRIMEN

3.1 INSTITUCIONES ESPECIALIZADAS

La Unidad Especializada de Delitos Informáticos[30] fue creada conforme a la resolución de la Fiscalía General del Estado Nº 4408/2011, que es la autoridad a cargo de la investigación y el enjuiciamiento judicial del delito cibernético en todo el país. Según las Resoluciones Nº 3459/10 y 4408/11, los tipos penales de competencia exclusiva de la Unidad Especializada en Delitos Informáticos. Los poderes y atribuciones del Ministerio Público están contenidos en los artículos 266-272 de la Constitución Nacional y los artículos 52 a 57 y 315 a 326 del Código Procesal Penal y su respectiva Ley Orgánica.

El Equipo de Respuesta de Computación y Emergencias (CERTpy)[31] que opera bajo la órbita de la Secretaría Nacional de Tecnologías de la Información y la Comunicación (SENATICS), que es la autoridad nacional oficial designada en seguridad cibernética. Fue creada el 30 de noviembre del 2012 con el objetivo principal de actuar como coordinador central para las notificaciones de incidentes de seguridad en Paraguay, brindando el apoyo necesario para dar respuesta a estos incidentes y haciendo que las partes afectadas e involucradas entren en contacto para la solución de los mismos.

3.2 Autoridades competentes para investigar en el sistema penal y/o que tienen potestad legal de realizar vigilancia específica de las comunicaciones

Además del Ministerio Público a través de la Unidad Especializada de Delitos Cibernéticos se encuentran las siguientes autoridades:

La Policía Nacional[32]:Los poderes, deberes y atribuciones de la Policía Nacional en funciones de investigación están previstos en los artículos 58 a 61 del Código Procesal Penal y los poderes y atribuciones de la Policía Judicial–que atiende directamente al Ministerio Público– están contenidos en los artículos 62 a 66 del Código Procesal Penal.

Sistema Nacional de Inteligencia (SINAI): Creada por la Ley Nº 5241 (Congreso Nacional, 2014) tiene la función de realizar trabajos de recolección y procesamiento de información de todos los ámbitos del nivel nacional e internacional, con el fin de producir inteligencia, previstos en los artículos 13 al 16 de la ley.

Poder Judicial: El órgano jurisdiccional representado por la figura de Juez es responsable en la etapa preparatoria del control del respeto de las garantías

30 Ministerio Público – Unidad especializada de Delitos Informáticos. Disponible en http://ministeriopublico.gov.py/delitos-informaticos-i242

31 CERT Paraguay. Página oficial disponible en https://www.cert.gov.py/index.php

32 Policía Nacional de Paraguay. Página oficial disponible http://www.policianacional.gov.py

y deberes de las partes conforme a los artículos 42 y 282 del Código Procesal Penal, por tanto, se le denomina Juez Penal de Garantías.

El tribunal de sentencias puede ser unipersonal así como también estar compuesto por 3 jueces queactúan como moderadores de la confrontación del juicio oral, valoran las pruebas presentadas mediante el sustento fáctico y normativo de los sujetos del proceso buscando la verdad y basando sus decisiones en la imparcialidad, según el artículo 41 del Código Procesal Penal.

SENAD: la Secretaría Nacional Antidrogas fue instituida como el organismo gubernamental responsable de ejecutar y hacer ejecutar la política del Estado para la interdicción del narcotráfico, la prevención, el tratamiento y la recuperación de farmacodependientes y el control del lavado de bienes provenientes del tráfico ilícito de drogas y otros hechos punibles conexos conforme se define en el artículo 3 del decreto N° 5279/2005[33].

Entre las funciones del Secretario Ejecutivo (con rango ministerial) de la SENAD se encuentra, entre otras el poder realizar con autorización judicial y dirección fiscal, procedimientos especiales de investigación, como la entrega vigilada, empleo de agentes encubiertos, filmaciones, grabaciones, control de comunicaciones sospechosas y otros, sobre presuntos hechos punibles castigados por la ley Nº 1.340/88 "Que reprime el tráfico ilícito de estupefacientes y drogas peligrosas" y sus modificaciones según el articulo 7, inc. J del decreto N° 5279/2005.

Para realizar extradiciones entre Estados parte, se utilizan las disposiciones de la Constitución Nacional del Paraguay y las disposiciones sobre extradición contenidas en los artículos 146 a 150 del Código de Procedimiento Penal y el correspondiente tratado de extradición con el país donde se procesa a la parte acusada. Las autoridades y los canales oficiales para llevar a cabo una extradición en Paraguay son la Oficina del Fiscal General, el Ministerio de Relaciones Exteriores[34], el Ministerio de Justicia y la Corte Suprema de Justicia[35].

4. ADQUISICIONES DEL ESTADO PARA LA VIGILANCIA DE LAS COMUNICACIONES

Paraguay se expande tecnológicamente con sistemas avanzados de vigilancia de las comunicaciones, pero sin las salvaguardas adecuadas. No existen regulaciones que obliguen a la rendición de cuentas, la supervisión pública con respecto al uso, y el alcance de los poderes y técnicas de vigilancia de las comunicaciones, ni a la presentación de reportes de transparencia tanto en el proceso penal y/o de inteligencia.

---

33 Decreto Nº 5279/2005 "Por el cual se reglamenta la Ley N° 1340/88", sus modificaciones, las leyes Nº 108/91, 68/92, 171/93, 396/94 y 1881/02, y se reorganiza la Secretaría Nacional Antidrogas (SENAD). Disponible en: http://www.senad.gov.py/pagina/106-marco-legal.html

34 Ministerio de Relaciones Exteriores de Paraguay. Página oficial disponible en http://www.mre.gov.py

35 Corte Suprema de Justicia de Paraguay. Página oficial disponible en www.csj.gov.py

La investigación sobre "Vigilancia de las Comunicaciones en Paraguay" (Jorge Rolón Luna, Maricarmen Sequera Buzarquis, 2016) resalta la gravedad que supone la adquisición de alta tecnología para la interceptación de las comunicaciones por parte del Estado paraguayo. Específicamente, se refiere a los siguientes sistemas de vigilancia:

Software FinFisher[36]: adquirido por el gobierno en el año 2012, fue revelada su existencia y uso en Paraguay, por Citizen Lab de la Universidad de Toronto.

Software Galileo – Remote Control System (RCS): los cables de WikiLeaks[37] filtraron las comunicaciones de intención de compra de dicho software entre la empresa HackingTeam y el Ministerio Público. En octubre de 2014, el socio local de Hacking Team solicitó un equipo adicional, lo que evidencia que hubo un seguimiento de la oferta por parte de las autoridades paraguayas.

Equipos de escuchas telefónicas[38]: WikiLeaks ha filtrado conversaciones diplomáticas entre el Ministerio del Interior en el año 2010 por esta compra. En el 2012, el Gobierno del ex presidente Federico Franco adquirió también un equipo de escuchas telefónicas por valor de US$ 2,5 millones, que misteriosamente desapareció de las oficinas del Ministerio del Interior, según relató un informe de la Auditoría General del Poder Ejecutivo en noviembre de 2013.

Las revelaciones sobre adquisición de software malicioso por parte del Estado paraguayo, causa serias preocupaciones: este tipo de software no deberá utilizarse como excusa para la armonización del Convenio. Su uso en el país no está claramente autorizado por la legislación interna, ni mucho menos regulada a su forma de utilización y alcance. En algunos casos, las normas son tan imprecisas que dejan abierta la puerta para el uso futuro de dichas herramientas, que pueden requerir garantías adicionales a las establecidas en una mera interceptación de comunicaciones. La existencia de estas normas imprecisas inhiben una discusión pública en el Congreso sobre la necesidad de establecer normas y garantías adicionales.

---

36 Bill Marczak, John Scott-Railton, Adam Senft, Irene Poetranto, and Sarah McKune, "Pay No Attention to the Server Behind the Proxy: Mapping FinFisher's Continuing Proliferation," [No prestes atención al servidor detrás del proxy: continúa proliferación de Mapeo de FinFisher], CitizenLab. Octubre de 2015. Disponible en: https://citizenlab.org/2015/10/mapping-finfishers-continuing-proliferation/ [Fecha de consulta: 8 de Febrero, 2018] y TEDIC. Más preguntas y dudas sobre software malicioso adquirido por SENAD. Mayo 2016 Disponible en https://www.tedic.org/mas-preguntas-y-dudas-sobre-software-malicioso-adquirido-por-senad/ [Fecha de consulta: 8 de Febrero, 2018].

37 WikiLeaks - The Hackingteam Archives. Paraguay - Uruguay Report. Disponible en: https://wikileaks.org/hackingteam/emails/emailid/249535 [Fecha de consulta: 8 de Febrero, 2018].

38 WikiLeaks https://wikileaks.org/plusd/cables/10ASUNCION97_a.html[Fecha de consulta: 8 de Febrero, 2018] e informe Canal 4 Telefuturo: Escuchas telefónicas sin orden judicial se darán en caso de extorsión y secuestro - 26/11/2014 https://www.youtube.com/watch?v=3Bkdspxhae8 [Fecha de consulta: 8 de Febrero, 2018].

5. ESTRATEGIAS POLÍTICAS PARA LA PERSECUCIÓN DEL CIBERCRIMEN

Paraguay cuenta con un Plan Nacional de Ciberseguridad (CERT, SENATICS, 2016) que fue coordinado por el Centro de Respuestas a Incidentes Cibernéticos CERT, con el apoyo del Programa de Seguridad Cibernética de la Secretaría del Comité Interamericano contra el Terrorismo (CICTE)[39] de la Organización de los Estados Americanos (OEA). Y aprobado por Decreto presidencial Nº 7052/2017 (Poder Ejecutivo, 2017).

El plan tuvo varios comentarios de la sociedad civil, en especial sobre el enfoque de seguridad que se aplica a la infraestructura crítica, sin incluir a 2 pilares importantes para la Ciberseguridad: Derechos Humanos y Economía Digital, y situar a la persona como objetivo central de esta política pública[40].

Existen capacitaciones de las Instituciones especializadas del Estado, sin embargo no se encuentra o se encuentra dispersa, la información oficial acerca de la participación de servidores públicos en foros, encuentros y cursos de capacitación en materia de Cibercrimen a nivel local y global.

El desafío está en seguir convocando a un equipo multidisciplinario (Hilbert, Miles, & Othmer, 2009), como hizo el grupo de trabajo de Ciberseguridad[41], pero con los mecanismos de Gobierno de Abierto[42]: que los grupos de trabajo estén integrados por representantes de los gobiernos, sector privado (usuarios y proveedores), organizaciones civiles y organismos internacionales, para conocer los avances de la región en materia de infraestructura e identificar potencialidades y limitantes en la creación de instituciones similares a las propuestas por la Unión Europea. Todo, con la finalidad de identificar la opción técnica más viable para la región.

Análisis de Entrevistas

Las entrevistas fueron realizadas con el fin de conocer la situación actual de persecución de la ciberdelincuencia en el sistema penal paraguayo, con miras a la armonización con el Convenio de Budapest.

Las instituciones elegidas para realizar las entrevistas son aquellas que aplican y deben velar por el cumplimiento de las leyes existentes en el Paraguay referentes a la ciberdelincuencia. Cada institución tiene una función diferente y específica, por lo

39 CICTE: Página oficial disponible en https://www.sites.oas.org/cyber/ES/Paginas/default.aspx

40 Ver mas en Desafíos del Plan de Ciberseguridad en Paraguay disponible en https://www.tedic.org/aspecto-positivos-y-negativos-del-plan-de-ciberseguridad-en-paraguay/ y Buscando a las mujeres en el Plan de Ciberseguridad en Paraguay disponible en https://www.tedic.org/buscando-a-las-mujeres-en-el-plan-nacional-de-ciberseguridad/ [Fecha de consulta: 8 de Febrero, 2018].

41 Participantes del Plan Nacional de Ciberseguridad en Paraguay, disponible en https://www.senatics.gov.py/application/files/2614/6316/2380/Participantes.pdf

42 Gobierno Abierto. Página oficial disponible en http://www.gobiernoabierto.gov.py/

cual las preguntas fueron elaboradas teniendo en cuenta esa situación.

Se entrevistó a los siguientes interlocutores claves, cuyas intervenciones se encuentran anonimizadas hasta un cierto grado (se alude al cargo, pero no a la identidad concreta):

- Agente Fiscal de la Unidad Especializada de Delitos Informáticos del Ministerio Público.
- Dos Jueces Penales de Garantía del Poder Judicial.
- Funcionario del Centro de Respuestas Ante Incidentes Cibernéticos (CERTpy) de la Secretaría Nacional de Tecnologías de la Información y la Comunicación (SENATICS)

En lo que respecta a las preguntas generales, sólo la Unidad Especializada de Delitos Informáticos del Ministerio Público y el Centro de Respuestas Ante Incidentes Cibernéticos (CERTpy) tienen conocimiento del Convenio, y algunas implicancias sobre su aplicación.

Ministerio Público

La Unidad Especializada de Delitos Informáticos fue creada para combatir los hechos punibles cometidos a través del uso de la tecnología que a su vez requieran un tratamiento especializado, desde la investigación, recolección, manejo de evidencia y prueba digital.

La entrevista con esta Unidad fue realizada el día 30 de enero de 2018, con la persona representante del Ministerio Público a cargo de una de las Unidades Fiscales de la Unidad Especializada de Delitos Informáticos.

A la consulta de si existe algún protocolo para recibir las denuncias sobre delitos informáticos refirió que sí existe un protocolo por el cual las denuncias deben ser recibidas, mencionando que en la Resolución de la Fiscalía General del Estado N° 4408/2011 se establece la competencia de los tipos penales sobre los cuales debe actuar dicha Unidad que son nueve. Los mismos están específicamente contemplados en los artículos 146, incisos b, c y d, artículo 174, inciso b, artículos 175, 188, 248 y 248, inciso b del Código Penal Paraguayo.

Al abordar la pregunta sobre los protocolos existentes para la recolección y análisis de las evidencias, la respuesta fue:

> "Sí, existe un protocolo que siguen y que cuidan, por sobre todas las cosas la cadena de custodia" según la Agente Fiscal.

Con respecto al protocolo referido, cabe mencionar que es el mismo utilizado para el manejo de todas las evidencias de cualquier índole. El Paraguay no cuenta con un protocolo específico para manejo de evidencias digitales particularmente, a pesar de que el tratamiento debe ser muy diferente con respecto a cualquier evidencia común.

El Ministerio Público dentro de su estructura cuenta con un Gabinete Técnico de Investigación, en cual está incluido la Dirección de Evidencias. Esta Dirección fue creada por Resolución F.G.E. N.º 575/2005, pasando en el 2015 a depender del Gabinete Técnico de Investigación[43].

La Dirección de Evidencias tiene por objetivo la recepción, guarda y custodia de las evidencias y/o bienes incautados que sean presentadas en el marco de un proceso penal. Del mismo modo, la Dirección de Evidencias tiene a su cargo la administración de todos los depósitos de evidencias, tanto en Asunción, Central, Regionales y Zonales[44].

La labor en el manejo de las evidencias es fundamental: la obtención de Información (elementos de convicción) se constituye en una de las facetas más útiles dentro del éxito de una investigación penal, aspecto que exige de los investigadores encargados de la recolección preservación, análisis y presentación de las evidencias digitales, una eficaz labor que garantice la autenticidad e integridad de dichas evidencias, a fin de ser utilizadas posteriormente ante el Tribunal de Sentencia. El manejo de las evidencias digitales se rige por ciertos principios, y al no contar con un manual o protocolo específico para tal efecto, se corre el riesgo de que puedan contaminarse o dañarse y no ser utilizados como pruebas que puedan confirmar o desvirtuar la verdad en un juicio.

Por otro lado, al consultarle al Representante del Ministerio Público sobre los criterios que tienen en cuenta al solicitar los datos de las personas a las diferentes operadoras telefónicas respondió que siempre tienen en cuenta lo establecido en la legislación pertinente. Al mismo tiempo manifestó que las compañías telefónicas son reacias a cooperar con la Unidad Especializada, dilatando los procesos por meses e incluso obligando muchas veces a archivarlos.

A través del Portal de Información Pública[45] se solicitó la cantidad de denuncias recibidas en el último año, que fueron un total de 586, discriminadas de la siguiente manera:

---

43 Resolución F.G.E. N° 1832/2015 “Por la cual se crea el Gabinete Técnico de Investigación y se aprueba su estructura orgánica”.

44 Estructuras y Manual de Funciones del Ministerio Público. Disponible en: http://www.ministeriopublico.gov.py/userfiles/files/manual_funcion_ultimo%282%29.pdf

45 Portal de Acceso a la Información Pública: www.informacionpublica.paraguay.gov.py/portal

Acceso indebido a sistemas informáticos	176
A determinar	157
Pornografía relativa a niños y adolescentes	119
Estafa mediante sistemas informáticos	90
Alteración de datos Inc. 3	31
Sabotaje de sistemas informáticos, Inc. 1°	7
Falsificación de tarjetas de débito o crédito y otros medios electrónicos de pago.	4
Pornografía relativa a niños y adolescentes, Inc. 1°	1
Extorsión	1
TOTAL	586

Entre algunas de las preocupaciones del representante del Ministerio Público están el desconocimiento que tienen sus colegas de las Unidades de delitos ordinarios sobre el rol y los delitos que persigue la Unidad especializada. Desde la creación de esta Unidad, hasta la fecha reciben casos ordinarios que tienen como evidencia el uso de tecnología. Este tipo de casos derivados genera retardos enla persecución efectiva del delito, ya que no se determina cual Unidad ser hará responsable para la investigación fiscal.

Por otro lado se encuentra las limitaciones del Ministerio Público sobre algunos de los delitos informáticos e inclusive delitos ordinarios que la ciudadanía acude a denunciarlos pero son de acción privada. Por tanto, los datos sobre acoso cibernético no se encuentran en sus bases de datos.

Entre otros puntos mencionados por el representante del Ministerio público se encuentran la necesidad de la Ley de Datos Personales, así como penalizar varias figuras tales como la usurpación de identidad, la lesión al derecho de la comunicación y la imagen, y el acoso y hostigamiento realizado por redes sociales.

Con respecto a las capacitaciones en materia de ciberdelito, destacó que son las empresas privadas quienes extienden invitaciones a la Unidad Especializada con los gastos pagados incluidos, ya que el Estado paraguayo difícilmente financia los viajes para formar a los funcionarios en cursos, talleres o seminarios.

PODER JUDICIAL

El juez penal de garantías es el que tiene la función de velar por el cumplimiento del debido proceso y el respeto a las garantías establecidas en la Constitución Nacional. Fueron entrevistados dos jueces penales de garantías, en las fechas 29 de enero de 2018 y 13 de febrero de 2018, respectivamente.

A los representantes del Poder Judicial se les realizó una sola pregunta que fue: “Cuando el Ministerio Público solicita autorización judicial para acceder a datos en casos de delitos informáticos, ¿cuál es el criterio que utiliza para sopesar que la información que se requiera no sea excesiva para los fines de la investigación?”.

El primero de ellos, respondió que tienen en cuenta lo que les solicita el Ministerio Público que tieneun sistema de alerta cuando en Paraguay se registran casos de pornografía infantil. Añadió que este sistema emite dicha alerta ya con todos los datos del sospechoso: ese es el documento que presenta el Ministerio Público y ellos otorgan las autorizaciones con los datos solicitados en él.

El sistema de alerta al que se refiere el Juez, es del Centro Nacional para Niños Desaparecidos y Explotados (NMEC por sus siglas en inglés) de Estados Unidos, quienes firmaron un acuerdo con la Unidad Especializada de Delitos Informáticos. El juez desconoce esta situación, afirmando que el sistema pertenece al Ministerio Público, no sopesando las informaciones requeridas, si no otorgando tal cual el pedido de los agentes fiscales.

El segundo juez de garantías, al ser abordado con la misma consulta contestó que los pedidos del Ministerio Público suelen ser muy concretos, que no hay limitaciones y que otorga lo que solicitan. Sostuvo que como la limitación la ley lo deja a criterio del Juzgado, una vez que el Ministerio Público recabe los datos y los presente, ellos sopesan y admitirían lo que hace objeto a la causa y deben omitir lo que atañe a la privacidad de las personas.

Así también, hizo mención a la necesidad y posibilidad de que los jueces penales cuenten con una persona, funcionario del Poder Judicial con conocimientos tanto jurídicos como informáticos que puedan ayudarlos a evacuar sus dudas en estos casos, antes de emitir una autorización. Además, cree necesario impartir talleres de difusión y capacitación sobre el Convenio de Budapest en los Juzgados.

Es preocupante que los jueces penales de garantías sostengan que no realizan un examen exhaustivo de los pedidos de autorización recibidos por parte del Ministerio Público ya que su función principal es salvaguardar las garantías establecidas en la Constitución Nacional y en las diferentes leyes. Cuando un Juez Penal de Garantías afirma que recién una vez que los agentes fiscales recaben la información y la presenten, hará el correspondiente análisis que debió haber hecho antes de otorgar la autorización, deja a la persona sometida al proceso sin un mínimo de garantías, a merced de que se violen los derechos de privacidad y con el peligro de que los datos recabados sean excesivos dentro de una investigación que todavía no tiene una sentencia y la persona sospechosa aún goza del derecho a ser considerada inocente hasta que se demuestre lo contrario.

CERTPY

El Centro de Respuestas Ante Incidentes Cibernéticos (CERTpy) se encarga del tratamiento de los incidentes de seguridad en sistemas computacionales en las que estén involucradas redes o infraestructuras del país. La entrevista a la Representante del CERTPy, fue llevada a cabo el día 28 de febrero de 2018.

Al ser consultada sobre si conoce el Convenio de Budapest y sobre las impli-

cancias del mismo en el sistema penal, respondió que si conoce el Convenio y sobre las implicancias sostuvo que ellos no forman parte de los órganos de aplicación de justicia, pero sí colaboran con los aspectos técnicos de los incidentes cibernéticos. Sostuvo que la Convención ayuda a tener un marco normativo común con otros países para definir los diferentes delitos de manera más igual.

Por otro lado, al preguntarle sobre los conocimientos que posee acerca del Convenio, los obtuvo a través de capacitaciones nacionales e internacionales, refirió que reciben invitaciones para capacitaciones de diversas índoles, pero no específicamente con un enfoque exclusivo sobre el Convenio. Cuando llegan invitaciones las derivan a los organismos de aplicación del sistema penal y estas invitaciones las suelen hacer organismos internacionales o gobiernos de otros países en alianza con empresas privadas.

CONCLUSIONES Y RECOMENDACIONES

Como se ha podido observar a lo largo del trabajo, el estado de situación actual en materia de cibercrimen presenta variados y complejos desafíos que deben ser seriamente analizados a fin de buscar alternativas para su superación o, al menos, su mitigación.

Los esfuerzos deberán estar fundados en espacios de diálogo y consenso, ya que no solo existe la necesidad de legislar y prevenir sino de respetar los derechos y las libertades de las personas. Por ello es necesario llegar a un acuerdo o pacto social y regional que brinde sostenibilidad y viabilidad al nuevo sistema legal en la materia.

Diseñar y promover una cultura del buen uso de la red, donde los ciudadanos adquieran conciencia de que los riesgos son reales y que es necesario aprender a reducirlos o evitarlos. La mejor respuesta para luchar contra el cibercrimen es la prevención, y ésta se obtiene educando e incentivando a los ciudadanos a involucrarse activamente en el compromiso de salvaguardarse en la red.

El Convenio de Budapest debería tomarse como una norma modelo a seguir, no como algo para aplicar: por un lado porque no tiene en cuenta la diversidad cultural, política y económica de los países, y por otro lado porque disminuye las barreras de seguridad nacional, entra en conflicto con el interés público y los derechos humanos. Es necesario realizar salvedades para no ceder jurisdicción y la privacidad de forma desproporcionada.

Para la armonización del Convenio de Budapest con nuestra legislación nacional, se debería de priorizar el conocimiento sobre el contenido y alcance del mismo. Debe darse un debate calmo y sereno entre todos los sectores de la sociedad con plena participación ciudadana a nivel nacional y regional, para conjuntamente elaborar una armonización eficaz y que respete los derechos humanos.

La convergencia legislativa es crucial para lograr una cooperación efectiva en la persecución de los delitos transnacionales y así reducir la incidencia de “refugios seguros” para el cibercrimen. Aunque existen problemas de soberanía nacional que pueden obstaculizar las investigaciones de los crímenes cibernéticos, Paraguay determinará lo que considera necesario para combatirlos eficazmente en el marco de la cooperación mutua y los derechos humanos y tratados internacionales.

Paraguay cuenta con legislación para la asistencia legal mutua en materia penal, anterior al Convenio de Budapest. Según el análisis, esto puede generar divergencias en la aplicación del Convenio con relación a otros tratados vigentes, socavando su efectividad. Esto se debe a que muchos países basan su asistencia legal mutua en el principio non bis in idem o principio de doble incriminación, o cuentan con diferentes o amplias excepciones que el Convenio. Sin embargo, estas diferencias se deben resolver con miras a lograr este desafío global.

Exigimos la conformación de una mesa multi-sectorial para debatir sobre una Ley de Protección de Datos Personales, que brinde garantías y control de la información personal depositada en sistemas de almacenamiento digital, asegurando que personas que vendan y distribuyan cualquier dato de carácter personal de forma ilegítima sean llevados a la justicia. No podemos debatir un proyecto de Retención de Datos sin antes contar con una Ley de Protección de Datos Personales.

Establecer garantías para la tutela judicial efectiva de los datos de carácter personal, que permitan a las personas que hayan sido afectadas por una medida abusiva de vigilancia específica o masiva, una debida restitución de sus derechos vulnerados y una reparación adecuada. Es necesario también la creación de un órgano independiente que proteja estas garantías.

Es necesario fortalecer las instituciones penales para una mejor interpretación de la leyes nacionales e internacionales sobre vigilancia de las comunicaciones, dado el avance de las técnicas y tecnologías de vigilancia. Para que los jueces del Poder Judicial realicen un análisis de proporcionalidad de ley o el uso de software malicioso como FinFisher o cualquier forma interpretación de las comunicaciones incluyendo los metadatos, deberán estar capacitados para conocer y justificar su uso, y así evitar negligencias o abusos por parte de los otras Instituciones del sistema penal como SENAD, Policía Nacional o Ministerio Público.

Las leyes de vigilancia de las comunicaciones tales como la Ley 4868/13 de Comercio Electrónico y La resolución 1350/2002 de Conatel, son normativas que no cuentan con los estándares mínimos para salvaguardar la información privada de los usuarios, ni criterios para justificar más datos de lo que la empresa privada necesita. Deberán ser modificados por no cumplir con los principios de proporcionalidad, necesidad, idoneidad y debido proceso. Por tanto será necesario reforzar a través de una ley de protección de datos personales para una armonización con el el Convenio acorde a los estándares de derechos humanos regidos en la Constitución Nacional y tratados internacionales vigentes.

La Constitución Nacional es clara al exigir que las autoridades designadas por ley, deben obtener una autorización judicial para solicitar acceso al contenido de las comunicaciones. Por tanto, no se puede invocar el Art. 228 del CPP de pedidos de informes por parte del Ministerio Público para acceder a los datos de tráfico o metadatos, considerados contenidos de las comunicaciones. Por tanto los usuarios y/o las ISPs deberían presentarse ante la justicia en el caso que ocurran procedimientos que no cumplen los preceptos constitucionales. Para ello pueden utilizar la jurisprudencia que establece mayores garantías de protección de las personas, en todo lo referente a sus comunicaciones privadas, que como ya se mencionó, tiene el carácter de vinculantes a nuestra jurisdicción. Por ejemplo, pueden basarse en el caso Esher vs. Brasil.

Las autoridades no han informado sobre la forma de procedimiento y el protocolo de actuación para operar plataformas como FinFisher, por lo que es de

importancia conocerlas causas y motivos por los que operaron u operan con semejante sistema de vigilancia electrónica en el país. Es Estado deberá publicar el uso y alcance de las leyes de vigilancia de las comunicaciones y estar en estricta vigilancia por parte de autoridades para evitar abusos. Deben publicar como mínimo, información global sobre el número de solicitudes aprobadas y rechazadas, un desglose de las solicitudes por proveedor de servicios, por autoridad investigadora, el tipo y propósito, y el número específico de personas afectadas por cada una y según el tipo de investigación y sus propósitos. El Estado paraguayo debe proporcionar a las personas información suficiente para que puedan comprender plenamente el alcance, naturaleza y aplicación de las leyes que permiten la vigilancia de las comunicaciones.

Se precisa mayor calidad en el debate político en el Congreso Nacional en particular y ciudadanía en general para discutir con mayor profundidad los estándares mínimos que autorizan la vigilancia de las comunicaciones y evitar proyectos de ley tales como la retención obligatoria de datos de tráfico (“Pyrawebs”).

En vista a la vigencia del Plan Nacional de Ciberseguridad, se deberá tomar en cuenta los comentarios acerca de la forma de aplicación y enfoque integral de la Seguridad Digital y abrir una mesa de diálogo colaborativo con otros sectores. Asimismo, se sugiere quela Comisión Nacional de Ciberseguridad mantenga una agenda y materiales actualizados de capacitación a los servidores públicos de forma pública y accesible para la ciudadanía.

Desarrollar áreas que permitan contar medios de investigación académica y capacitación para ofrecer respuestas a los delitos con y en las TIC. Así también la promoción de espacios técnicos que permitan a los diferentes actores interactuar e intercambiar experiencias y opiniones. Esto es además una necesidad para el diseño de las políticas públicas en la materia, por los requerimientos técnicos que implica.

Elaborar un catálogo de estadísticas sobre el Cibercrimen en formato abierto y accesible. La fragmentación de información en la materia, es un aspecto problemático y central. Liberar información pública en formatos de datos abiertos, es un compromiso de los planes de acción de Gobierno Abierto de Paraguay, cumpliendo los estándares de acceso a la información.

BIBLIOGRAFÍA

Access to e-evidence: Inevitable sacrifice of our right to privacy? (2017, junio 14). Recuperado 21 de febrero de 2018, a partir de https://edri.org/access-to-e-evidence-inevitable-sacrifice-of-our-right-to-privacy/

Acuña, J., Alonzo, L., & Sequera, M. (2017). La protección de Bases de Datos en Paraguay. Setiembre, 2017, 1(1). Recuperado a partir de https://www.tedic.org/wp-content/uploads/sites/4/2017/09/La-protecci%C3%B3n-de-Bases-de-Datos-en-Paraguay_Documento-Final.pdf

Anna Biselli. (2017, mayo 31). EU diskutiert über Zukunft der Vorratsdatenspeicherung: «Anlasslose Speicherung nicht mehr möglich». Recuperado 27 de febrero de 2018, a partir de https://netzpolitik.org/2017/eu-diskutiert-ueber-zukunft-der-vorratsdatenspeicherung-anlasslose-speicherung-nicht-mehr-moeglich/

Asamblea Constituyente. (1992). Constitución Nacional de la República del Paraguay. Recuperado 20 de enero de 2017, a partir de http://www.bacn.gov.py/constitucion-nacional-de-la-republica-del-paraguay.php

Carlos Reusser, M. (2017, julio 9). Reservas de Chile al Convenio de Budapest. Explicaciones de la prof. Rosenblut. Recuperado 23 de febrero de 2018, a partir de http://www.reusser.cl/budapest-segun-rosenblut/

CERT, SENATICS. (2016, noviembre 9). Plan Nacional de Ciberseguridad. Recuperado a partir de http://gestordocumental.senatics.gov.py/share/s/m2uDswEUTDmrDBY2NFttIg

CIDH. (2009, julio 6). Caso Escher y otros vs. Brasil. Sentencia de 6 de Julio de 2009. Recuperado a partir de http://www.corteidh.or.cr/docs/casos/articulos/seriec_200_esp1.pdf

Clough, J. (2014). A World of Difference: The Budapest Convention on Cybercrime and the Challenges of Harmonisation (SSRN Scholarly Paper No. ID 2615789). Rochester, NY: Social Science Research Network. Recuperado a partir de https://papers.ssrn.com/abstract=2615789

Conatel. Resolución No 1350/2002 Por el Cual se establece la obligatoriedad de registros de detalles de llamadas por el plazo de seis /6) meses (2002). Recuperado a partir de http://www.buscoley.com/pdfs/r_1350_2002.pdf

Congreso, N. Código Penal paraguayo (1997). Recuperado a partir de https://www.oas.org/dil/esp/Codigo_Penal_Paraguay.pdf

Congreso Nacional. Ley N° 642/95 de Telecomunicaciones, 1 § (1995). Recuperado a partir de https://www.conatel.gov.py/images/iprincipal/LEY%20642/Ley_N_642-95.pdf

Congreso Nacional. Ley 1286/98 Código procesal penal de Paraguay, 1 1 S (1998). Recuperado a partir de http://www.ministeriopublico.gov.py/userfiles/files/Paraguay_Codigo_Procesal_Penal%281%29.pdf

Congreso Nacional. Ley No 1334/98 de Defensa del Consumidor y del Usuario (1998). Recuperado a partir de http://www.mic.gov.py/v1/sites/172.30.9.105/files/Ley%2016_0.pdf

Congreso Nacional. LEY No 2.298 Que aprueba la Convención de las Naciones Unidas contra la delincuencia organizada transnacional (2003). Recuperado a partir de www.seprelad.gov.py/includes/descargar.php?file=ley_n_229803.pdf

Congreso Nacional. Ley 3440/08 que modifica el Código penal paraguayo (2008). Recuperado a partir de http://www.pj.gov.py/images/contenido/ddpi/leyes/ley-3440-2008-que-modifica-el-codigo-penal.pdf

Congreso Nacional. Ley 4439 que modifica y amplia varios artículos de la Ley No 1160/97 «Código penal» (2011). Recuperado a partir de http://www.bacn.gov.py/archivos/3777/20150817113434.pdf

Congreso Nacional. Ley 4468 de Comercio Electrónico (2013). Recuperado a partir de https://www.acraiz.gov.py/adjunt/Leyes%20y%20Decretos/ley_4868_comercio_electrnico_26-02-13.pdf

Congreso Nacional. Ley No 5241/14 Que crea el Sistema Nacional de Inteligencia. (2014). Recuperado a partir de http://www.bacn.gov.py/leyes-paraguayas/4620/crea-el-sistema-nacional-de-inteligencia

Consejo de Derechos Humanos. (2013). Report of the Special rapporteur on thepromotion and protection of the right to freedomof opinion and expression, Fran de la Rue. Recuperado a partir de http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf

Consejo de Europa. Explanatory Report to the Convention on Cybercrime (2001). Recuperado a partir de https://rm.coe.int/16800cce5b

Consejo de Europa. (2014, junio). Such solutions need to provide for safeguards, conditions and respect rule of law and human rights,including data protection, principles. Recuperado a partir de https://rm.coe.int/1680303ebe

Council of Europe. (2003). Additional Protocol to the Convention on Cybercrime, concerning thecriminalisation of acts of a racist and xenophobic nature committed throughcomputer systems. Recuperado 22 de febrero de 2018, a partir de https://rm.coe.int/168008160f

EDRI. (2017, enero). Cybercrime Convention - cross-border access to electronic evidence. Recuperado a partir de https://edri.org/files/surveillance/cybercrime_accesstoevidence_positionpaper_20170117.pdf

EPIC. (2004, junio). Senate Committee on Foreign Relations Letter. Recuperado a partir de https://www.epic.org/privacy/intl/senateletter-061704.pdf

Hilbert, Miles, & Othmer. (2009). Foresight tools for participate policy-making in inter-governmental processes in developing countries: Leesons learned from the eLAC Policy Priorities Delphi. Recuperado 25 de febrero de 2018, a partir de http://www.martinhilbert.net/Hilbert_etal.eLACdelphi.pdf

Himanen, Pekka. (2001). La ética del hacker y el espíritu de la era de la información. Random House.

Jorge Rolón Luna, Maricarmen Sequera Buzarquis. (2016, marzo). Vigilancia Estatal de las comunicaciones y derechos fundamentales en Paraguay. Recuperado a partir de https://www.tedic.org/wp-content/uploads/sites/4/2016/05/Paraguay-ES.pdf

Judgment of the Court (Grand Chamber). (2014). Digital Rights Ireland Ltd (C-293/12) v Minister for Communications, Marine and Natural Resources,Minister for Justice, Equality and Law Reform,Commissioner of the Garda Síochána, Ireland. Recuperado a partir de http://curia.europa.eu/juris/document/document.jsf?doclang=EN&text=&pageIndex=1&part=1&mode=req&docid=150642&occ=first&dir=&cid=572131

Judgment of the Court (Grand Chamber). In Joined Cases C-203/15 and C-698/15, REQUESTS for a preliminary ruling under Article 267 TFEU, made by the Kammarrätten i Stockholm (Administrative Court of Appeal, Stockholm, Sweden) and the Court of Appeal (England & Wales) (Civil Division) (United Kingdom), by decisions, respectively, of 29 April 2015 and 9 December 2015, received at the Court on 4 May 2015 and 28 December 2015, in the proceedings (2016). Recuperado a partir de http://curia.europa.eu/juris/document/document.jsf?text=&docid=186492&doclang=EN

Krutskikh, S. (2015, mayo 8). International Law and International Information Security: Recuperado 22 de febrero de 2018, a partir de https://www.ccdcoe.org/multimedia/international-law-and-international-information-security-response-krutskikh-and-streltsov

Lara, J. C., Martínez, M., & Viollier, P. (2014). Hacia una regulación de los delitos informáticos basada en la evidencia. Revista Chilena de Derecho y Tecnología, 3(1). https://doi.org/10.5354/rchdt.v3i1.32222

McNamee, J. (2017, abril). RightsCon session on cross-border access to e-evidence – key interventions. Recuperado a partir de https://edri.org/rightscon-session-on-cross-border-access-to-e-evidence-key-interventions/

MERCOSUR. Protocolo de Asistencia juridica mutua en asuntos penales. (1996). Recuperado a partir de https://www.oas.org/juridico/spanish/tratados/sp_proto_asis_jur%C3%AD_mutua_asun_pena_mercosur.pdf

Naciones Unidas, A. G. Convención de las Naciones Unidas contra la delincuencia organizada transnacional y sus protocolos. (2000). Recuperado a partir de https://www.oas.org/juridico/spanish/tratados/sp_conve_nu_cont_delin_organi_transna.pdf

OEA. Convención Americana sobre Derechos Humanos Suscrita en la Conferencia Especializada Interamericana sobre Derechos Humanos (B-32), B-32 § (1969).

OEA. Convención Internamericana sobre asistencia mutua en materia penal (1992). Recuperado a partir de https://www.oas.org/juridico/spanish/tratados/a-55.html

ONU. (1948, diciembre 10). Declaración Universal de los Derechos Humanos. Recuperado a partir de http://www.ohchr.org/EN/UDHR/Documents/UDHR_Translations/spn.pdf

ONU. (1966, diciembre 16). Pacto Internacional de Derechos Civiles y Políticos. Recuperado 20 de enero de 2017, a partir de http://www.ohchr.org/SP/ProfessionalInterest/Pages/CCPR.aspx

Poder Ejecutivo. (2017, abril 24). DECRETO 7052 Que aprueba el Plan Nacional de Ciberseguridad y se intergra la Comisión Nacional de Ciberseguridad. Recuperado 25 de febrero de 2018, a partir de https://www.presidencia.gov.py/archivos/documentos/DECRETO7052_5cq17n8g.pdf

Relatoría Especial para la Libertad de Expresión, CIDH. (2009, diciembre 30). El derecho de acceso a la información en el marco jurídico interamericano. Recuperado a partir de http://www.oas.org/es/cidh/expresion/docs/publicaciones/ACCESO%20A%20LA%20INFORMACION%20FINAL%20CON%20PORTADA.pdf

Rudmin, F. (2006, mayo 24). Why Does the NSA Engage in Mass Surveillance of Americans When It's Statistically Impossible for Such Spying to Detect Terrorists? Recuperado 27 de febrero de 2018, a partir de https://www.counterpunch.org/2006/05/24/why-does-the-nsa-engage-in-mass-surveillance-of-americans-when-it-s-statistically-impossible-for-such-spying-to-detect-terrorists/

Runnegar, C. (2014, mayo 14). A Win for Privacy: 8-Year-Old EU Directive on Data Retention Ruled Invalid. Recuperado 27 de febrero de 2018, a partir de https://www.internetsociety.org/blog/2014/05/a-win-for-privacy-8-year-old-eu-directive-on-data-retention-ruled-invalid/

Sequera, M. (2015, abril 15). #Pyrawebs: Las claves de una ley que no funciona. Recuperado 27 de febrero de 2018, a partir de https://www.tedic.org/pyrawebs-las-claves-de-una-ley-que-no-funciona/

Sequera, M. (2017, abril). ¿Quién defiende tus datos?Buscando la transparencia de los intermediarios de Internet en Paraguay. Recuperado a partir de https://qdtd.tedic.org/

Susan Brenner. (2012). La Convención sobre Cibercrimen del Consejo de Europa. Revista Chilena de Derecho y Tecnología, 1(1). https://doi.org/10.5354/rchdt.v1i1.24030

Téllez Valdez, Julio,. (2003). Derecho Informático, 3a ed., Ed. Mac Graw Hill, México, 2003. 514p. Recuperado 23 de febrero de 2018, a partir de https://doctrina.vlex.com.mx/vid/tellez-valdes-informatico-mac-graw-hill-42392427

Wingyan Chung, Weiping Chang, & Shihchieh Chou. (2004). Fighting cybercrime: a review and the Taiwan experience. Recuperado a partir de https://pdfs.semanticscholar.org/cab2/e593bffbd8e940d12770d6eeab51c5cf5c47.pdf

ANEXOS

A.1. Guión de entrevista

A continuación se presentan las preguntas-guía que se utilizaron en las entrevistas para cada una de las instituciones públicas.

Preguntas generales para todas las instituciones

¿Conoce el Convenio de Ciberdelincuencia de Budapest?

¿Conoce sobre las implicancias del Convenio en el sistema penal?

¿Ha recibido capacitación o entrenamiento sobre la armonización del Convenio?¿Si es así cuales y donde?

Preguntas específicas a cada Institución de persecución del sistema penal y ciberdelincuencia

Secretaria Nacional Antidrogas (SENAD)

¿A que se refiere con operaciones de contra-inteligencia? ¿Que implican?

¿Para las intervenciones, tienen autorización judicial y acompañamiento fiscal?

¿Realizan operaciones de oficio?

Con respecto al software Finfisher: ¿Cuál es el protocolo para operar el software?

¿Cuáles son los propósitos para los cuales se utiliza?

¿A cuántas personas se ha aplicado?

¿Cuáles han sido los resultados?

MINISTERIO PÚBLICO:

¿Cuántas denuncias sobre delitos informáticos recibieron en el último año?

Al solicitar los datos de las personas a las diferentes operadoras telefónicas, ¿cual es el criterio que utilizan?

Al realizar la recolección y análisis de las evidencias, ¿cual es el protocolo que siguen? ¿Existe alguno?

¿Existe algún protocolo para recibir las denuncias sobre delitos informáticos?

JUEZ PENAL DE GARANTÍAS:

Cuando el Ministerio Público solicita autorización judicial para acceder a datos en casos de delitos informáticos, ¿cuál es el criterio que utiliza para sopesar que la información que se requiera no sea excesiva para los fines de la investigación?

POLICÍA NACIONAL

Solicitar la cantidad de denuncias recibidas con respecto a delitos informáticos.

MINISTERIO DE RELACIONES EXTERIORES

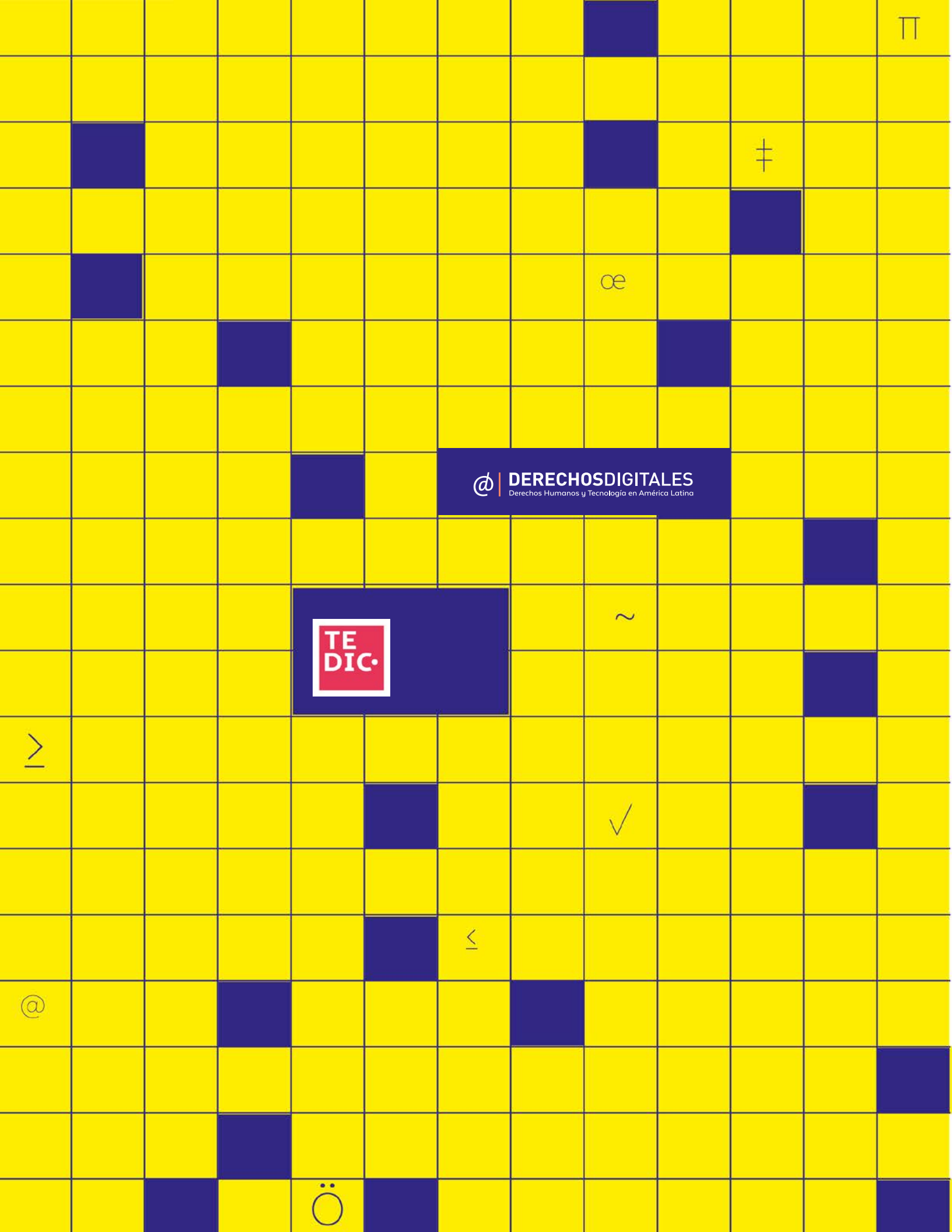
Solicitar la lista de Convenios Internacionales relativos a la cooperación Internacional en materia penal firmado y ratificados por Paraguay.

Mecanismos alternativos de asistencia mutua Internacional en caso de ausencia de cooperación internacional para la persecución de delitos transaccionales.

(Footnotes)

1 Al finalizar la presente investigación se ha encontrado información acerca de los mecanismos alternativos en caso de ausencia de Tratados de asistencia legal mutua (MLAT)

2 OEA – REMJA. Disponible en https://www.oas.org/en/sla/dlc/remja/background.asp


@ | DERECHOSDIGITALES
Derechos Humanos y Tecnología en América Latina
TE
DIC·