GLACY+

Global action on Cybercrime Extended
Action Globale sur la Cybercriminalité Elargie

Versión 27 de junio de 2019

Confidencial y Restringido

# Reporte Comparativo

Misión Consultiva y Taller de Trabajo sobre
ciberdelito y prueba electrónica y la implementación
del Convenio de Budapest en los países que forman parte del FORPEL

## Reporte Final

## Preparado bajo el Proyecto GLACY+

www.coe.int/cybercrime

Funded
by the European Union
and the Council of Europe

EUROPEAN UNION

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

Implemented
by the Council of Europe

# Índice

# 1. Prefacio

El presente informe se prepara en el marco del Proyecto sobre Acción Global en contra de la Ciberdelincuencia (GLACY+) en estrecha colaboración con la Oficina del Programa al Combate contra el Ciberdelito (C-PROC) del Consejo de Europa en Rumania.

El informe examina la legislación vigente sobre cibercriminalidad tanto en materia de derecho penal sustantivo como de derecho procesal penal en los 10 países miembros del Foro de Presidentes y Presidentas de Poderes Legislativos de Centro América y la Cuenca del Caribe (FOPREL). El objetivo es identificar aquellas áreas de reformas legislativas que pueden requerir apoyo a través del proyecto GLACY+, a fin de contribuir a que los países miembros de FOPREL modernicen la legislación sobre esta materia. La promulgación de leyes penales sustantivas y procesales de conformidad con el Convenio de Budapest no solo ayudará a la investigación, la adjudicación y el enjuiciamiento de los delitos informáticos y la obtención de pruebas electrónicas, sino que también ayudará a mejorar la cooperación internacional y equipará a los países con los requisitos mínimos para solicitar la adhesión al Convenio de Budapest.

Para obtener una visión más completa de la situación actual, se llevará a cabo un taller de dos días con Diputadas y Diputados dentro la Comisión Interparlamentaria de Seguridad Ciudadana y Administración de Justicia y Asuntos Internacionales e Integración Regional del FOPREL con el objeto de apoyarlos en el proceso de armonización legislativa en materia de ciberdelito y prueba electrónica y de promover y apoyar desde los poderes legislativos en los países miembros de FOPREL la adhesión al Convenio de Budapest para que puedan adoptar un marco legislativo uniforme basado en dicho instrumento, encaminado a la protección de la sociedad y el fomento de la cooperación internacional en materia del combate al ciberdelito en la región.

En el taller participarán y contribuirán al trabajo de esta misión miembros del Secretariado del FOPREL y Diputados y Diputadas de los siguientes 10 países:

- Belice
- Costa Rica
- El Salvador
- Guatemala
- Honduras
- Nicaragua
- México
- Panamá
- Puerto Rico
- República Dominicana

## 2. El Convenio de Budapest en países de Latinoamérica y el Caribe

El Convenio de Budapest ha sido firmado y ratificado por 63 países, de los cuales solo seis países de la región de Latinoamérica y el Caribe lo han ratificado tal y como se muestra en el siguiente cuadro ordenado por fecha más reciente de ratificación.

| País | Ratificado | Entrada en Vigor | Reservas y/o Declaraciones |
|---|---|---|---|
| 1. Paraguay | 30/07/2018 | 01/11/2018 | Sin Reservas. Tres Declaraciones del 30.07.2018 https://goo.gl/1vxMsE |
| 2. Argentina | 05/06/2018 | 01/10/2018 | Cinco Reservas y Dos Declaraciones del 05.06.2018 https://goo.gl/GiXuT9 |
| 3. Costa Rica | 22/09/2017 | 01/01/2018 | Dos Reservas y Dos Declaraciones del 22.09.2017 https://goo.gl/j9zZXj |
| 4. Chile | 20/04/2017 | 01/08/2017 | Cinco Reservas y Dos Declaraciones del 20.04.2017 https://goo.gl/sS7x2W |
| 5. Panamá | 05/03/2014 | 01/07/2014 | Sin Reservas. Tres Declaraciones del 05.03.2014 https://goo.gl/14eG23 |
| 6. República Dominicana | 07/02/2013 | 01/06/2013 | Sin Reservas. Dos Declaraciones del 07.02.2013 https://goo.gl/snnXxV |

Costa Rica, República Dominicana y Panamá son los únicos países miembros de FOPREL que han ratificado el Convenio de Budapest.

Chile y Argentina actualmente se encuentran en procesos de reforma de su legislación penal sustantiva y procedimental para uniformarlas conforme a las disposiciones previstas en el Convenio de Budapest. Argentina trabaja en un proceso de reforma de la legislación procesal penal tanto a nivel federal como de los diferentes Estados provinciales para cumplir con las exigencias de la Convención de Budapest en materia procesal. Es posible afirmar que en América Latina existe un mayor grado de avance en las reformas de las leyes penales de fondo que en lo que respecta a las normas penales en materia procesal.

Vale la pena destacar que México fue invitado por el Consejo de Europa a adherirse al Convenio en 2009 y Colombia en 2012 y más recientemente Perú, pero a la fecha ninguno ha formalizado ante el Consejo de Europa su adhesión a dicho instrumento.

# 3. Legislación sustantiva y procedimental sobre ciberdelito y prueba electrónica en países miembros del FORPEL

Se revisó el reporte del FOPREL respecto al desarrollo del marco normativo en materia de ciberdelito en los países miembros de esa organización, así como las legislaciones penales vigentes y proyectos de ley de los 10 países que forman parte del FORPEL. Podemos evaluar que una gran mayoría de los países cuentan con legislación sustantiva para castigar algunos tipos de delitos informáticos, pero no todas las conductas y delitos contenidos en los Arts. 2 a 11 del Convenio de Budapest. Para algunos países, su legislación penal requiere una interpretación muy amplia (no totalmente compatible con la prohibición de aplicar el derecho penal sustantivo por analogía que rige los sistemas constitucionales de la mayoría de estos países) para incluir y castigar algunas de las conductas previstas en el Convenio de Budapest.

Asimismo, se pudo constatar que casi ningún país de FOPREL, excepto República Dominicana cuenta con normas procesales penales que regulen la preservación de la evidencia digital. Así, los Códigos revisados no prevén un conjunto de normas que establezcan con claridad los poderes procesales previstos en la Convención: aseguramiento de datos, orden de presentación, registro y secuestro de datos informáticos, intervención en tiempo real de datos de tráfico y datos de contenido. Antes bien, existe una tendencia a aplicar las "viejas" normas sobre pruebas pensadas para la evidencia física por analogía. Para ello, se utiliza como fundamento el principio de "libertad probatoria" presente en casi todos los Códigos Procesales. Entendemos que este uso forzado del principio de "libertad probatoria" más allá de sus posibilidades afecta tanto la eficiencia de las investigaciones como la vigencia de garantías individuales.

Por otro lado, muy pocos países cuentan con medidas de cooperación internacional y de asistencia jurídica mutua diseñadas especialmente para solicitar información y acceso a datos informáticos almacenados a proveedores de servicios globales de Internet y menos aún, disposiciones sobre acceso transfronterizo a datos informáticos albergados en países extranjeros. Asimismo, en la región solo la República Dominicana, Costa Rica y Chile han establecido la red 24/7 prevista en el Artículo 35 del Convenio de Budapest como órgano central de asesoramiento vinculado con la Fiscalía y los organismos de investigación policial para garantizar la asistencia jurídica inmediata relacionada con investigaciones penales en el contexto tecnológico o para solicitar pruebas en formato electrónico a otras autoridades a través de las redes de contacto de países que forman parte del Convenio de Budapest.

La siguiente sección contiene un resumen acerca de la legislación penal sustantiva y procesal relacionada con ciberdelito y evidencia electrónica de los 10 países miembros del FOPREL. La valoración se hizo conforme a las disposiciones de carácter sustantivo y procedimental previstas en el Convenio de Budapest.

## 3.1. Belice

Belice es quizás de los pocos países del FOPREL que todavía no cuentan con una legislación penal sustantiva sobre ciberdelitos. El Código Penal de 31 de diciembre de 2000 (Criminal Code Chapter 101) no contiene disposiciones que permitan la investigación y el castigo de conductas cometidas a través del uso de tecnologías de información y tampoco prevé alguna de la conductas y delitos contenidos en los Arts. 2 a 11 del Convenio de Budapest.

En materia procedimental, Belice cuenta con una ley específica para el uso de evidencias electrónicas en procedimientos judiciales (*Electronic Evidence Act of May 2003*) que reconoce la validez del uso de información y datos contenidos en formato electrónico para ser utilizados y reconocidos en todo tipo de procedimientos, incluidos procedimientos en materia penal. Sin embargo, esa ley no contiene disposiciones especiales para ordenar la preservación, producción e incautación de datos informáticos (datos de suscriptor, tráfico) ni tampoco disposiciones de cooperación judicial para solicitar el acceso transfronterizo a pruebas y evidencias contenidas en sistemas informáticos y servidores localizadas en otros países.

Belice se encuentra actualmente trabajando en una estrategia nacional de ciberseguridad a través de un Task-Force Multisectorial en donde las instituciones representadas en dicho task-force están analizando la posibilidad de reformar la legislación sustantiva y procedimental para introducir y castigar ciberdelitos y establecer disposiciones procedimentales y mecanismos en materia de investigaciones sobre ciberdelito y prueba electrónica con base en las disposiciones del Convenio de Budapest.

## 3.2. Costa Rica

Costa Rica ratificó el Convenio de Budapest 22 de septiembre de 2017 y previo a su adhesión a dicho instrumento ya contaba con una legislación penal sustantiva que castiga y sanciona la gran mayoría de las conductas y delitos previstos en los Arts. 2 al 11 del Convenio de Budapest. Como parte de las actividades del Proyecto GLACY +, el Consejo de Europa ha llevado a cabo tres misiones para reforzar las capacidades del sistema de justicia penal relacionadas con legislación sustantiva y procesal en materia de ciberdelito y pruebas electrónicas en ese país. La primera misión que se llevó a cabo del 21 al 24 de mayo de 2018 se hicieron algunas recomendaciones en materia de legislación procesal. Por ejemplo, se encontró que los supuestos de conservación de datos y la conservación y revelación parcial rápidas de datos de tráfico no se encuentran previstos propiamente en el Código Procesal Penal (Ley No. 7594) sino únicamente en la Ley *sobre Registro, Secuestro y Examen de Documentos Privados e Intervención de las Comunicaciones* (Ley No. 7425) por lo que se recomendó incluir los supuestos y plazos para obligar la conservación de datos, así como establecer procedimientos y mecanismos necesarios para ordenar la conservación y revelación rápida de datos sobre tráfico dentro del Código Procesal Penal conforme a los Arts. 16 y 17 del Convenio de Budapest, respectivamente.

En la segunda misión que se llevó a cabo del 8 al 11 de octubre de 2018, los expertos del CoE recomendaron incluir una disposición que facilite la conservación rápida y simple de todas las categorías de datos durante un período específico sin la necesidad de una orden judicial y que la conservación sea renovable al menos una vez. Con respecto a la orden de presentación o producción de datos informáticos, se encontró que el Art. 226 del Código Procesal Penal puede funcionar como una orden de producción para ciertos tipos de datos, pero no cubre las diferentes clases de datos, como el contenido de una cuenta de correo electrónico almacenada con un proveedor de servicios de Internet por lo que se recomendó incluir un mecanismo especifico para exigir su producción.

En la tercera y más reciente misión sobre legislación procedimental en ciberdelito y prueba electrónica llevada a cabo el 16 y 17 de mayo de 2019 se revisó el *Proyecto de Ley para Combatir la Ciberdelincuencia* presentado por el Diputado Erwen Masis y se sometió a discusión con fiscales de la Unidad de Capacitación y Supervisión del Ministerio

Público, de la Oficina de Asesoría Técnica y Relaciones Internacionales (OATRI) de la Fiscalía General, de la Procuraduría General de la República (PGR) y representantes del Organismo de Investigación Judicial, entre otros. Entre algunas de los hallazgos y recomendaciones que los expertos del CoE hicieron sobre dicho proyecto de ley es que no cuenta con disposiciones que faciliten la obtención de los datos de suscriptor y datos de tráfico que sean aplicables a entidades públicas y privadas ni tampoco prevé supuestos, mecanismos y procedimientos para ordenar la conservación de datos.

Otro hallazgo relevante fue que la legislación procedimental vigente no contiene disposición alguna que establezca el deber de conservación de datos por parte de los proveedores de servicios, y que el plazo de cuatro años para la conservación de datos previsto en el proyecto de ley no resulta acorde con el derecho comparado y las mejores practicas en otros países, y en particular que dicho proyecto carece de normas procedimentales que den respuesta a la totalidad de las necesidades y supuestos normativos que fueron puestos de manifiesto por los fiscales costarricenses.

Por último, se recomendó difundir ampliamente entre los operadores del sistema de justicia penal relacionados con el uso y manejo de la evidencia electrónica el punto de contacto nacional 24/7, fomentando su uso por parte de los órganos investigación policial y del Ministerio Público y someter a consulta y discusión el Proyecto de Ley con todos los operadores y entidades que tienen relación con la materia a regular, tanto jurídicos, como partícipes en la investigación, incluyendo los proveedores de servicios nacionales e internacionales.

## 3.3. El Salvador

**Infracciones Penales:** La República de El Salvador no forma parte del Convenio de Budapest. En 2016 se aprobó el Decreto Legislativo número 260, referido a la Ley Especial contra Delitos Informáticos y Conexos (en lo sucesivo LEDIC). Dicha ley, además de incorporar tipos penales con cierta consonancia con el Convenio de Budapest, regula delitos que no están presentes en dicho Convenio.

El objeto de la ley conforme explica el art. 1, es proteger los bienes jurídicos de aquellas conductas delictivas cometidas por medio de las Tecnologías de la Información y la Comunicación, así como la prevención y sanción de los delitos cometidos en perjuicio de los datos almacenados, procesados o transferidos; los sistemas, su infraestructura o cualquiera de sus componentes, o los cometidos mediante el uso de dichas tecnologías que afecten intereses asociados a la identidad, propiedad, intimidad e imagen de las personas naturales o jurídicas en los términos aplicables y previstos en esa ley.

Artículo 2 Convenio de Budapest: el art. 4 de la LEDIC, castiga el acceso, interceptación o uso total o parcial de un sistema informático. El Convenio dice *ilegítimo,* mientras que la ley dice sin autorización o excediendo la que posea.

Artículo 3 Convenio de Budapest: respecto a la interceptación deliberada e ilegítima de datos informáticos, el art. 5 de la LEDIC castiga el acceso parcial o total a cualquier programa o a datos en él almacenados, con el propósito de apropiarse de ellos. De la lectura del artículo vemos que no se castiga la interceptación *per se*, si no más bien un acceso indebido a datos con una intención de apropiarse de ellos o cometer otro delito con ellos. Conforme se establece en el Reporte Explicativo del Convenio de Budapest, la interceptación puede realizarse por varias modalidades, no solamente el acceso a los

datos. Por lo que el delito de la LEDIC es más restrictivo y al exigir la ultraintención mencionada limita el ámbito de punición. El art. 21 penaliza a quien sin justificación intercepte por medios tecnológicos cualquier transmisión hacía, desde o dentro de un sistema informático que no está disponible al público, o las emisiones electromagnéticas que están llevando datos de un sistema informático. Lo que llama la atención es la elevada escala penal, dado que es de siete a diez años, sin poseer agravantes.

Artículo 4 Convenio de Budapest: el art. 7 de la LEDIC sanciona a quien destruya, dañe, modifique, ejecute un programa o realice cualquier acto que altere el funcionamiento o inhabilite parcial o totalmente un sistema informático que utilice las Tecnologías de la Información y la Comunicación o cualquiera de los componentes que las conforman. El tipo penal previsto por el Convenio de Budapest apunta a que la conducta delictiva recaiga sobre datos informáticos, en cambio el artículo de la ley salvadoreña sobre el *sistema informático o cualquiera de los componentes que las conforman*. Interpretar que los datos informáticos están incluidos en la frase *cualquiera de los componentes* podría ser violatorio del principio de legalidad penal. No obstante, los art. 19 y 20 de la mencionada ley castigan a quien violando la seguridad de un sistema informático destruya, altere, duplique, inutilice o dañe la información, datos o procesos, en cuanto a su integridad, disponibilidad y confidencialidad en cualquiera de sus estados de ingreso, procesamiento, transmisión o almacenamiento. Por lo que ahí sí se prevé el daño sobre los datos. Asimismo, se penaliza a quien interfiera, obstruya o interrumpa el uso legítimo de datos o los produzca nocivos e ineficaces, para alterar o destruir los datos de un tercero. Hay un agravante para cuando los datos son públicos, financieros, de salud, transporte o energía.

Artículo 5 Convenio de Budapest: el art. 6 de la LEDIC castiga a quien intencionalmente y por cualquier medio interfiera o altere el funcionamiento de un sistema informático, de forma temporal o permanente. El art. 6 de la LEDIC no se menciona la manera de cometer esa alteración o interferencia. Se incorpora un agravante si el sistema es público, de salud, energía, transporte o cualquier servicio público o financiero.

Artículo 6 Convenio de Budapest: respecto al abuso de dispositivos, el art. 8 de la LEDIC sanciona la posesión, producción, facilitación o venta de equipos, dispositivos, programas informáticos, contraseñas o códigos de acceso; con el propósito de vulnerar, eliminar ilegítimamente la seguridad de cualquier sistema informático, ofrezca o preste servicios destinados a cumplir los mismos fines para cometer cualquiera de los delitos establecidos en la LEDIC. La pena de hasta cinco años parece muy elevada en relación a otras conductas previstas.

Artículo 7 Convenio de Budapest: en relación a la falsificación informática, no se castiga con un tipo penal específico.

Artículo 8 Convenio de Budapest: en lo referido al fraude informático, la LEDIC posee dos artículos. El art. 10 castiga la modalidad de defraudación penada en el art. 8.a) del Convenio de Budapest, o sea cuando la conducta es realizada sobre los datos, tanto el input como en el output o en su procesamiento. El art. 10 de la ley se dirige a castigar la conducta sobre el procesamiento de datos y/o el resultado de los datos, siempre que esté presente el beneficio patrimonial. El art. 11 de la LEDIC castiga la manipulación en

el sistema o sus componentes que genere un provecho para el autor o un perjuicio para un tercero.

Artículo 9 Convenio de Budapest: respecto a pornografía infantil, el art. 28 de la LEDIC castiga las conductas relacionadas con material de pornografía infantil . La definición de pornografía infantil es brindada por el art. 3.o) de dicha ley, siendo coincidente en su núcleo con la de Convenio de Budapest. Se castiga la adquisición y la posesión.

Artículo 10 Convenio de Budapest: en los art. 226 y 227 del CP se castigan conductas relacionadas con infracciones a la propiedad intelectual. La LEDIC no posee conductas relacionadas con la propiedad intelectual.

**Medidas Procesales de evidencia digital:** El Salvador posee algunas medidas relacionadas con evidencia digital reguladas en el Decreto Legislativo Número 904 Código Procesal Penal de la República de El Salvador. Por ejemplo, regula en el art. 201 medidas para la obtención, resguardo o almacenamiento de la información, sin perjuicio que se ordene el secuestro respectivo. Asimismo, posee en los art. 250 a 252 tres disposiciones sobre la cadena de custodia. Dichas medidas, sin embargo, son limitadas y no reflejan el conjunto de medidas procesales previstas por el Convenio de Budapest.

## 3.4. Guatemala

**Infracciones Penales:** Guatemala posee en su Código Penal (Decreto N° 17-73, en lo sucesivo CP), Capítulo VII, titulado "De los delitos contra el derecho de autor, la propiedad industrial y delitos informáticos", art. 274 inciso "A" al "G", delitos relacionados con la materia. Sin embargo, dichos tipos penales no están completamente homologados conforme al Convenio de Budapest. En febrero de 2017 se elaboró un proyecto de legislación sobre ciberdelito específica con el apoyo del Consejo de Europa y, posteriormente en enero de 2019 el Consejo de Europa organizó una misión para apoyar al gobierno de Guatemala para aclarar una nota técnica de la Comisión Interamericana de Derechos Humanos de la OEA y aclarar dudas con respecto al alcance de las disposiciones contenidas en el nuevo proyecto de ley sobre ciberdelincuencia del Diputado Rodrigo Valladares en donde participaron representantes del Ministerio de Tecnologías de Información, miembros de la Comisión del Congreso de Diputados, Fiscales del Ministerio Público, académicos y representantes de la sociedad civil.

Cabe resaltar que Guatemala no ha solciitado al Consejo de Europa formalmente el acceso al Convenio de Budapest.

**Compatibilidad de las normas vigentes con el Convenio de Budapest:**

En relación al Artículo 2 Convenio de Budapest: no se castiga el acceso deliberado e ilegítimo a un sistema informático. El art. 274 F del CP, castiga el uso u obtención indebida de datos contenidos en registros informáticos, pero no el acceso *per se* al sistema donde se encuentre el mencionado registro. El art. 8 del Proyecto tipifica este delito conforme al Convenio, incluyendo supuestos de datos confidenciales como agravante.

Artículo 3 Convenio de Budapest: no se castiga la interceptación deliberada e ilegítima de datos informáticos. El art. 9 del Proyecto de ley sí tipifica este delito conforme al Convenio.

Artículo 4 Convenio de Budapest: respecto a la comisión deliberada e ilegítima de actos que dañen, borren, deterioren, alteren o supriman datos informáticos, el art. 274 A del CP castiga la destrucción, borrado, inutilización, alteración, daño de *registros informáticos.* El CP no posee un apartado de definiciones que indique qué significa dicho término, lo que puede limitar la punición a bases de datos, excluyendo al dato informático *per se.* El art. 10 del Proyecto tipifica este delito conforme al Convenio, incluyendo supuestos de datos comerciales e información pública como agravantes.

Artículo 5 Convenio de Budapest: en relación a la obstaculización grave, deliberada e ilegítima del funcionamiento de un sistema informático, el art. 274 B del CP solamente castiga la alteración, borrado o inutilización de programas o instrucciones de programas, pero no el sistema. El art. 11 del Proyecto tipifica este delito conforme al Convenio, incluyendo supuestos de obstaculización de sistemas públicos o registros oficiales o bancarios, como agravantes.

Artículo 6 Convenio de Budapest: respecto al abuso de dispositivos, el art. 274 G del CP solamente castiga al que distribuyere o pusiere en circulación programas o instrucciones destructivas, que puedan causar perjuicio a los registros, programas o equipos de computación. No prevé ninguna conducta al productor, vendedor, al adquirente para uso ni importador. Tampoco establece la ultrafinalidad de uso delictivo por parte del autor. Respecto al objeto material del delito, el CP se ciñe a la capacidad de daño de tales materiales, mientras que los instrumentos mencionados en el Convenio son más amplios y refiere a que sirvan para cometer cualquier delito de los art. 2 a 5, no solo daño. No castiga la posesión de tales instrumentos. El art. 14 del Proyecto tipifica este delito conforme al Convenio.

Artículo 7 Convenio de Budapest: no se castiga la falsificación informática. Por ejemplo, el art. 274 A del CP castiga la destrucción, alteración, borrado, daños de registros informáticos de investigaciones penales. Pero no la falsificación ni nada asimilable a lo previsto en el art. 7 del Convenio. El art. 12 del Proyecto tipifica este delito conforme al Convenio.

Artículo 8 Convenio de Budapest: solamente se castiga la estafa por medio de tarjetas de crédito o débito en el art. 264bis del CP, no haciendo mención alguna a la estructura del art. 8 del Convenio. El art. 15 del Proyecto tipifica este delito conforme al Convenio.

Artículo 9 Convenio de Budapest: respecto a pornografía infantil, el CP castiga en el art. 193 ter la producción, fabricación o elaboración de dicho material. En el tipo se incluyen imagen o voz real o simulada de una o varias personas menores de edad. La posesión de material a sabiendas es castigada junto a la adquisición. La enumeración del objeto del delito del Convenio es más amplia.

Artículo 10 Convenio de Budapest: el Art. 274 del CP posee conductas relacionadas con infracciones a la propiedad intelectual.

Medidas Procesales de evidencia digital: Guatemala no posee una regulación especial sobre medidas procesales diseñadas para los desafíos que plantea la evidencia digital. En la practica este vacío legal se llena con la aplicación analógica de las normas sobre prueba del CPP (rige el Decreto número 51-92, Código Procesal Penal de la República de Guatemala, que no regula las medidas procesales del Convenio de Budapest). El proyecto de ley de febrero de 2017 antes citado elaborado con el apoyo del Consejo de Europa y la OEA sí incluye dichas medidas procesales. En concreto, en los Arts. 25 a 29 del mismo se regulan conforme a los establecido en el Convenio de Budapest. Entre ellas, el aseguramiento de datos, la orden de presentación, registro y secuestro de datos, interceptaciones datos.

## 3.5. Honduras

**Infracciones Penales:** La República de Honduras no forma parte del Convenio de Budapest. En el Decreto 144-83, Código Penal de la República de Honduras, hay ciertos delitos tradicionales adaptados a las nuevas tecnologías, como los artículos 149, 214, 215, 223 y 254. En 2018, Honduras comenzó el debate de un proyecto de ley denominado *'Ley de Ciberseguridad y medidas de protección ante los actos de odio y discriminación en internet y redes sociales'*. Dicho proyecto de ley no regula tipos penales en la materia. No obstante, lo interesante es que, en el dictamen preliminar que posee dicho proyecto, se recomienda que se inicien las acciones por parte del Poder Ejecutivo para la adhesión de Honduras al Convenio de Budapest.

Asimismo, en mayo de 2019 se publicó en la Gaceta el nuevo Código Penal de Honduras. El mismo regirá a partir de noviembre de 2019. A continuación, analizaremos el tipo penal vigente junto al nuevo, en contraste con el Convenio de Budapest.

Artículo 2 Convenio de Budapest: el Art. 398 del nuevo CP castiga a quien, vulnerando las medidas de seguridad establecidas para impedirlo, accede sin autorización a todo o en parte de un sistema informático. Asimismo, hay un agravante si el sistema es un servicio esencial. El artículo, que entrará en vigor en noviembre, está redactado conforme a lo previsto en el Convenio de Budapest. El actual CP no prevé este delito.

Artículo 3 Convenio de Budapest: el Art. 214 del actual CP prohíbe la interceptación o apoderamiento de comunicaciones en cualquier soporte. No menciona al dato en sí, si no a la comunicación. No todo dato informático puede ser comunicación. El art. 272 del nuevo CP castiga la interceptación de comunicaciones o acceso a datos, así como el uso de artificios técnicos de escucha, transmisión, grabación o reproducción del sonido, la imagen o secuencia de imágenes. Todas estas conductas deben ser realizadas *para conocer los secretos o vulnerar la intimidad de otro y sin consentimiento,* para ser punibles.

Artículo 4 Convenio de Budapest: el Art. 254 del vigente CP, castiga a quien, por cualquier medio destruya, altere, inutilice o de cualquier otro modo dañe los datos, programas o documentos electrónicos ajenos, contenidos en redes, soportes o sistemas informáticos. El nuevo CP, en el art. 399 castiga este delito en su primer párrafo. Asimismo, agrega un agravante cuando son servicios esenciales.

Artículo 5 Convenio de Budapest: el Art. 399 del nuevo CP, en su párrafo segundo sanciona a quien, sin estar autorizado inutiliza, total o parcialmente, el funcionamiento

de un sistema informático, impidiendo el acceso al mismo o imposibilitando el desarrollo de alguno de sus servicios. El tipo penal no menciona el modo de cometer el delito, comparado con lo dispuesto por el Convenio de Budapest. Asimismo, el nuevo CP agrega un agravante cuando son servicios esenciales. El vigente CP lo castigaba en el delito de daños del art. 254, agregando simplemente la palabra *programas,* junto a los objetos sobre los que recae el delito.

Artículo 6 Convenio de Budapest: respecto al abuso de dispositivos, no se castiga actualmente. El nuevo CP lo sanciona en el Art. 400 conforme al Convenio de Budapest. La nueva figura no prohíbe la posesión de tales elementos.

Artículo 7 Convenio de Budapest: en relación a la falsificación informática, no se castiga con un tipo penal específico. Tanto el CP vigente como el nuevo, poseen tipos penales generales de falsificación de documentos públicos, mercantiles y privados.

Artículo 8 Convenio de Budapest: en lo referido al fraude informático, el nuevo CP sanciona en el Art. 365 a quien, con el propósito de obtener un provecho ilícito, consigue la transferencia no consentida de cualquier activo patrimonial en perjuicio de tercero, mediante una manipulación informática o el uso de otro artificio semejante. El Convenio de Budapest establece que debe realizarse mediante cualquier introducción, alteración, borrado o supresión de datos informáticos, o cualquier interferencia en el funcionamiento de un sistema informático. En cambio, el tipo penal del nuevo CP solamente dice *mediante una manipulación informática o el uso de otro artificio semejante.* No especifica si debe recaer sobre datos, programas, o ambos.

Artículo 9 Convenio de Budapest: respecto a pornografía infantil, el Art. 261 del nuevo CP prohíbe la elaboración, venta, distribución o difusión de pornografía infantil. Se prohíbe la tenencia de material cuando es para propio consumo con una pena reducida. No se castiga el acceso ni la adquisición de pornografía infantil. Respecto al concepto de pornografía infantil, el art. 262 del nuevo CP dice que es cualquier material audiovisual que, con finalidad de excitación sexual, recoge cualquier clase de actos sexuales o conductas sexualmente explícitas, realizados por menores de dieciocho años, así como la reproducción de sus órganos sexuales o, eventualmente, de otras partes del cuerpo en un contexto sexual. Asimismo, se establece que es necesario que las imágenes o voces de los niños sean al menos parcialmente reales. Por lo cual, el objeto material del delito simulado de los incisos b y c del art. 9.2 del Convenio de Budapest son más amplios y no fueron incluidos en el nuevo CP.

Artículo 10 Convenio de Budapest: en los Arts. 389 a 392 del CP se castigan conductas relacionadas con infracciones a la propiedad intelectual.

**Medidas Procesales de evidencia digital:** Honduras no posee medidas relacionadas con evidencia digital reguladas en el Decreto 1999-12-30 Código Procesal Penal de la República de Honduras.

## 3.6. Nicaragua

**Infracciones Penales:** Nicaragua no forma parte del Convenio de Budapest. Hay algunos tipos penales relacionados con ciberdelitos en la Ley número 641 que contiene el Código Penal, aprobado en 2007 (en lo sucesivo CP).

Artículo 2 Convenio de Budapest: no se castiga en forma directa el acceso deliberado e ilegítimo a un sistema informático. Los Arts. 197 y 198 del CP solamente refieren al uso y acceso no autorizado a bancos de datos o información, pero no al sistema donde son contenidos. El art. 417 del CP sanciona a quien se introduzca en programas informáticos relativos a la seguridad nacional o defensa nacional.

Artículo 3 Convenio de Budapest: no se castiga la interceptación deliberada e ilegítima de datos informáticos. El Art. 194 del CP únicamente prohíbe la escucha de comunicaciones privadas o telefónicas que no le estén dirigidas mediante procedimientos técnicos. El Art. 275 del CP castiga a quien se apodere por cualquier medio de información, datos, documentos escritos o electrónicos, registros informáticos que contengan un secreto empresarial. El Convenio de Budapest no plantea restringir la interceptación a cuestiones comerciales.

Artículo 4 Convenio de Budapest: el Art. 245 del CP castiga a quien destruya, borre o de cualquier modo inutilice registros informáticos, pero no refiere a datos informáticos. No define qué es un registro informático.

Artículo 5 Convenio de Budapest: no se castiga la obstaculización grave, deliberada e ilegítima del funcionamiento de un sistema informático.

Artículo 6 Convenio de Budapest: respecto al abuso de dispositivos, el Art. 246 del CP penaliza a quien, con la intención de producir un daño, adquiera, distribuya o ponga en circulación programas o instrucciones informáticas destructivas, que puedan causar perjuicio a los registros, programas o a los equipos de computación. No prevé ninguna conducta al productor ni al adquirente para uso propio. Respecto a la ultrafinalidad de uso delictivo por parte del autor, el CP menciona el daño, mientras que la intención del Convenio refiere a cometer los delitos de los art. 2 a 5, por lo que es más amplio. No castiga la posesión de tales instrumentos.

Artículo 7 Convenio de Budapest: no se castiga la falsificación informática.

Artículo 8 Convenio de Budapest: en lo que refiere a la estafa informática, el CP castiga en el art. 229 a quien, con el propósito de obtener un provecho ilícito, consiga la transferencia no consentida de cualquier activo patrimonial en perjuicio de tercero, mediante la manipulación de registros informáticos o programas de computación o el uso de otro artificio semejante. El Articulo restringe la estafa a un perjuicio patrimonial de trasferencias de activos, cuando no sería la única forma de realizar un perjuicio patrimonial. El verbo típico menciona el hecho de manipular registros (…), término que no queda claro su significado. El Convenio, en cuanto a la manipulación de datos, menciona toda la cadena: introducción, alteración, borrado o supresión.

Artículo 9 Convenio de Budapest: respecto a pornografía infantil, el CP castiga en el Art. 175 verbos típicos de la cadena de producción y difusión de material para fines de explotación sexual, por cualquier medio sea directo, mecánico, digital, audio visual, o con soporte informático, electrónico o de otro tipo, la imagen, o la voz de persona menor de dieciocho años en actividad sexual o eróticas, reales o simuladas, explicitas e implícitas o la representación de sus genitales con fines sexuales. No menciona el término pornografía infantil, aunque lo describe. Respecto a la posesión la prohíbe solamente cuando la misma sea con fines de explotación sexual, algo muy difícil de probar, lo que excluiría los casos de mero consumo.

Artículo 10 Convenio de Budapest: los Arts. 247 a 251 del CP prohíben conductas relacionadas con la propiedad intelectual.

Medidas Procesales de evidencia digital: En lo que respecta a las medidas procesales, en la Ley 406, Código Procesal Penal del 2001, solamente hay una disposición aislada. El art. 214 habla de interceptación de comunicaciones electrónicas en delitos graves, lo que podría ser asimilable a interceptación de datos de contenido, aunque sin ningún límite ni criterio similar al Convenio de Budapest.

## 3.7. México

Aún y cuando México cuenta con algunas disposiciones en su Código Penal Federal (CPF) para castigar ciertos delitos cometidos a través de sistemas informáticos tales como el acceso ilícito a sistemas (Art. 211 bis 2 CPF), ataques a la integridad del sistema (Art. 221 bis 1 CPF), la distribución, difusión y venta de contenidos de abuso sexual de menores a través de Internet (Arts. 202 y 202 BIS CPF), consideramos que el marco penal sustantivo debe ser reforzado para regular conductas tales como la interceptación ilícita, ataques a la integridad de datos, el abuso de dispositivos -tales como la obtención y el uso ilícito de contraseñas y códigos de acceso para acceder a dispositivos informáticos-, la falsificación de datos informáticos y el fraude informático, figuras que aún no se encuentran previstas en el Código Penal Federal. Asimismo, la posesión de material de pornografía infantil tampoco se encuentra regulada en el Código Penal Federal ni tampoco en Ley General para Prevenir, Sancionar y Erradicar los Delitos en Materia de Trata de Personas y para la Protección y Asistencia a las Victimas de estos Delitos.

Con respecto a medidas de carácter procesal en materia de investigaciones sobre ciberdelito, el Art. 381 del Código Nacional de Procedimientos Penales (CNPP) únicamente reconoce los datos y la información contenida en medios digitales, electrónicos, ópticos o cualquier otra tecnología como medios de admisión de prueba en tribunales en materia penal, sin embargo no se han desarrollado aún reglas o lineamientos específicos para el uso y admisión de la evidencia electrónica basada en estados internacionales tales como la Norma ISO/IEC 2703, 2012 y los Lineamientos sobre Prueba Electrónica desarrollados por el Consejo de Europa.

La Ley Federal de Telecomunicaciones y Radiodifusión y el CNPP contienen obligaciones para los proveedores de servicios de telefonía móvil para la conservación de datos e información de comunicaciones móviles para propósitos de investigaciones penales, en situaciones de emergencia o cuando este en peligro la vida de una persona, sin embargo, no resulta claro que dichas disposiciones apliquen directamente a los proveedores de servicios globales de internet. Asimismo, el CNPP carece de los procedimientos,

mecanismos y plazos necesarios para ordenar la preservación, producción e incautación de datos informáticos (datos de suscriptor, tráfico), así como el acceso transfronterizo a datos ubicados en terceros países, tal y como lo prevé el Convenio de Budapest.

Aún y cuando la Suprema Corte de Justicia invalidó en Marzo de 2018 el Art. 303 del CNPP con relación a la obtención de la ubicación geográfica en tiempo real de dispositivos móviles por parte de las autoridades para propósitos de investigaciones penales, se requiere revisar esa disposición para permitir por los menos la obtención de datos de tráfico de comunicaciones electrónicas en tiempo real en casos de emergencia con el debido respeto a las salvaguardas y la protección de los derechos fundamentales previstos en la legislación nacional, la jurisprudencia de la Suprema Corte de Justicia de la Nación y el Art. 15 del Convenio de Budapest.

Con relación a las medidas de asistencia jurídica mutua y cooperación internacional, México cuenta con una red de convenios bilaterales y multilaterales con diversos países en materia de cooperación penal internacional, sin embargo es prioritario que México se adhiera al Convenio de Budapest para mejorar la cooperación no solo con las autoridades investigadoras de los países que forman parte del Convenio de Budapest, sino en particular para fortalecer los lazos de cooperación con los proveedores de servicios globales de Internet para que las autoridades investigadoras se les pueda facilitar el acceso a información y datos informáticos que puedan ser útiles en investigaciones relacionadas con ciberdelitos conforme a un marco jurídico internacional.

Cabe destacar que algunos legisladores de la presente Legislatura recientemente han presentado iniciativas de ley para reformar el CPF y sancionar conductas tales como tráfico y comercialización de contenidos de pornografía infantil, venta de armas a través de Internet, entre otros. Sin embargo, se trata solo de iniciativas y es poco probable que sean aprobadas. Ninguna de las iniciativas que se han generado en el Congreso Mexicano esta dirigida a reformar e introducir las conductas en materia sustantiva que hace falta regular en el CPF o para mejorar los mecanismos y procedimientos para el uso y reconocimiento de la prueba electrónica en los procedimientos penales.

Por último, consideramos que la iniciativa de ley presentada en noviembre de 2017 por dos exdiputados cubría en gran medida gran parte de las disposiciones sustantivas, procedimentales y de cooperación internacional del Convenio de Budapest, sin embargo, habría que ser retomada por la actual legislatura y someterla a discusión y aprobación en las respectivas comisiones de la Cámara de Diputados y el Senado de la República.

## 3.8. Panamá

**Infracciones Penales:** La República de Panamá forma parte del Convenio de Budapest desde julio de 2014. En el Código Penal de Panamá de 2010 se encuentran algunas conductas relacionadas con ciberdelitos. Específicamente, en el Título VIII del Libro II del Código Penal, hay una sección que contiene un capítulo denominado Delitos contra la Seguridad Informática, compuesto por los artículos del 289 al 292. Asimismo, en el Título VIII del Código Penal se tipifican los Delitos contra el Orden Económico y los Delitos Contra la Seguridad Colectiva.

En el año 2017 se presentó el Proyecto de Ley número 558, que modifica el Código Penal, actualizando los tipos penales vigentes para homologarlos conforme al Convenio de Budapest, así como agregar conductas nuevas. En concreto, dicho proyecto prevé

modificar los art. 166, 184, 185, 195, 200, 204, 224, 226, 243, 289, 290, 291, 292, y 365 del Código Penal.

Artículo 2 Convenio de Budapest: el Art. 289 del CP castiga a quien ingrese o utilice una base de datos, red o sistema informático. No menciona cómo debe ser el aspecto subjetivo de la conducta.

Artículo 3 Convenio de Budapest: el Art. 290 del CP prohíbe el apoderamiento, copia, utilización o modificación de datos en tránsito o contenidos en una base de datos o sistema informático, o interfiera, intercepte, obstaculice o impida su transmisión. Tanto este artículo como el mencionado Art. 289, poseen agravantes cuando son realizados contra oficinas públicas, financieros o con fin lucrativo. Asimismo, hay un agravante para los casos en que la conducta básica la comete el encargado o responsable de la base o del sistema o usando información privilegiada. El proyecto de ley separa la interceptación de datos de un sistema, de los datos de una base de datos, y agrega más supuestos típicos.

Artículo 4 Convenio de Budapest: respecto a la comisión deliberada e ilegítima de actos que dañen, borren, deterioren, alteren o supriman datos informáticos, no se castiga. El Art. 230 del CP simplemente incorpora al tipo de daño físico a modo de agravante cuando el daño se ocasione utilizando instrumentos o medios informáticos, computadora, dato, red o programa de esa naturaleza. O sea, utilizar a la tecnología como medio para dañar los objetos contenidos en los incisos 1 a 6. Esto quiere decir que menciona a la tecnología como medio, pero no como fin. El objeto dañado es una cosa mueble o inmueble, pero no datos informáticos. El mencionado proyecto de ley prevé incorporar expresamente la conducta de quien dañe, borre, altere, obstruya, interrumpa, interfiera o niegue el acceso a datos informáticos contenidos en un sistema informático o cualquier medio de almacenamiento.

Artículo 5 Convenio de Budapest: en relación a la obstaculización grave, deliberada e ilegítima del funcionamiento de un sistema informático, el art. 290 del CP prevé en su segundo párrafo una parte de la conducta prevista por el Convenio de Budapest. El proyecto de ley incorpora un tipo penal específico a fin de modificar el art. 289 y 290 del CP.

Artículo 6 Convenio de Budapest: respecto al abuso de dispositivos, no se castiga actualmente. El proyecto de reforma planea modificar el art. 292 del CP a fin de castigar esta conducta, con una alta amplitud de verbos típicos a fin de abarcar la cadena de elaboración, importación, distribución, uso y posesión de claves, contraseñas, códigos de acceso, programas informáticos, equipos, materiales o dispositivos cuyo uso esté destinado a la alteración o destrucción de datos informáticos o a la comisión de delitos.

Artículo 7 Convenio de Budapest: en relación a la falsificación informática, el art. 366 del CP castiga la falsificación o alteración de la firma digital informática de un documento. El proyecto de ley agrega en el Art. 289 del CP la conducta de falsificación de encabezados de mensajes electrónicos.

Artículo 8 Convenio de Budapest: en lo referido al fraude informático, el Art. 226 del CP sanciona a quien, para procurarse para sí o para un tercero un provecho ilícito, altere, modifique o manipule programas, bases de datos, redes o sistemas informáticos, en perjuicio de un tercero, así como un agravante cuando lo cometa el encargado o responsable de la base de datos, o del sistema o usando información privilegiada. Utiliza la expresión *provecho ilícito,* en lugar de perjuicio patrimonial como lo estipula el Convenio de Budapest, o provecho patrimonial. El Convenio de Budapest diferencia eficazmente el caso donde la conducta recae en los datos, de cuando recae en el funcionamiento de un sistema informático. El art. 226 refiere a *base de datos*, pero no a realizar las conductas típicas sobre datos aislados. El proyecto de ley incorpora expresamente el término *datos,* conforme el Convenio de Budapest, sin necesidad de que constituyan una base de datos. Asimismo, agrega más verbos típicos sobre esos datos.

Artículo 9 Convenio de Budapest: respecto a pornografía infantil, el CP establece en los Arts. 184 y 185, verbos típicos de la cadena de producción y difusión de pornografía infantil real o simulada, por cualquier medio. Respecto a la posesión la prohíbe cuando la misma sea para uso propio y haya sido voluntariamente adquirido. El proyecto de ley número 558 de modificación del CP ya mencionado, prevé incorporar en el art. 185 la obtención y el acceso a través de un sistema informático o sistema electrónico a pornografía infantil.

Artículo 10 Convenio de Budapest: en los Art. 262 a 266 del CP se prohíben conductas relacionadas con infracciones a la propiedad intelectual.

**Medidas Procesales de evidencia digital:** en el Código Judicial, Libro Tercero, referido al procedimiento penal, hay algunas medidas procesales pensadas para la evidencia física que se aplican a la digital. Por ejemplo, el art. 2178 que habla de registro y secuestro dice *"o cualesquiera otros objetos que puedan servir para comprobar el hecho punible o para descubrir a sus autores y partícipes".* Frase utilizada para incluir evidencia digital. Lo mismo respecto del art. 311 del Código Procesal de Panamá que regula las interceptaciones de comunicaciones. Dicho artículo habla de *comunicaciones cibernéticas,* pudiéndose interpretar que alude a interceptación de datos de contenido.

No obstante, y a fin de lograr una mayor adecuación al Convenio de Budapest, el mencionado Proyecto de Ley número 558, busca incorporar y modificar medidas relacionadas con evidencia digital a los art. 338 A-F, como la conservación de datos informáticos, orden de presentación, acceso transfronterizo de datos abiertos, obtención en tiempo real de datos de tráfico y de contenido.

## 3.9. Puerto Rico

El Código Penal de Puerto Rico (Ley 146-2012) ha sido reformado en diversas ocasiones y actualmente castiga gran parte de las conductas y delitos previstos en los Arts. 2 a 11 del Convenio de Budapest tales como el acceso ilícito a sistemas informáticos, interceptación ilícita, atentados contra la integridad del sistema, falsedad informática, fraude informático, delitos relacionados con la explotación sexual de menores en Internet, delitos contra el derecho a la intimidad y delitos relacionadas con la usurpación de identidad, entre otros.

En el ámbito procedimental, Puerto Rico cuenta con Reglas Generales de Evidencia que fueron aprobadas por el Tribunal Supremo el 9 de febrero de 2009 y que son utilizadas para distintos tipos de procedimientos incluyendo la materia procesal penal, este último procedimiento se rige exclusivamente bajo las Reglas para el Procedimiento Criminal. El capítulo IX de la Reglas Generales de Evidencia establece metodologías y requisitos para la autenticación e identificación de la evidencia electrónica.

Puerto Rico cuenta con una División de Crímenes Cibernéticos adscrita a la Policía Nacional (en lo sucesivo 'DCC'). El 25 de abril de 2018, la DCC publicó una Orden General que tiene el propósito de establecer la estructura organizacional y funcional de la DCC, así como establecer obligaciones, normas y procedimientos para solicitar, intervenir y procesar las actividades y equipos electrónicos relacionados con la comisión de delitos, incluida la preservación de datos para evitar que la evidencia electrónica se altere o desaparezca.[1]

Puerto Rico es un país con un sistema jurídico mixto de derecho anglosajón y derecho civil y cuyo sistema político esta influenciado primordialmente por los Estados Unidos. Las leyes federales de los EUA aplican por supremacía en el territorio de Puerto Rico, por tanto, leyes como el Computer Fraud and Abuse Act[2] y US Cloud Act[3] son de aplicación directa en ese país. Las medidas de cooperación con los proveedores de servicios de internet y facultades para que las autoridades investigadoras puedan ordenar a los proveedores de servicio la preservación, producción e incautación de datos informáticos (datos de suscriptor, tráfico), conservación rápida en tiempo real de datos de tráfico y conexión, así como acceso transfronterizo a datos ubicados en los servidores de los proveedores de servicios en terceros países se rigen conforme al US CLOUD Act. Sin embargo, el US Cloud Act requiere que los países tengan celebrados convenios bilaterales de cooperación y asistencia jurídica mutua con el país que requiere la producción y el acceso a datos de proveedores de servicios ubicados en los EUA, a través de sus autoridades respectivas. Con respecto a las medidas para la producción de datos en particular datos de contenido, la legislación procesal de Puerto Rico requiere de una orden judicial de un tribunal para que las autoridades investigadoras puedan tener acceso a la información.

## 3.10. República Dominicana

República Dominicana fue el primer país del Caribe y Latinoamérica en haber firmado y ratificado el Convenio de Budapest el 7 de febrero de 2013, entrando en plena vigencia en ese país desde el 1o. de junio de 2013.

República Dominicana cuenta con una legislación independiente para investigar, perseguir y sancionar delitos informáticos vigente desde enero de 2007 "*Ley No. 53-07 sobre Crímenes y Delitos de Alta Tecnología* (en lo sucesivo Ley No. 53-07) y que castiga la gran mayoría de las conductas y delitos previstos bajo el Convenio de Budapest, entre ellos: Delitos contra la confidencialidad, integridad y disponibilidad de datos y sistemas

[1] La Orden No. 613 del 25 de abril de 2018 de la División de Crímenes Cibernéticos se encuentra en: https://policia.pr.gov/orden-general/division-de-crimenes-ciberneticos/
[2] Ver Title 18 § 1030 of the United States Code en: https://www.law.cornell.edu/uscode/text/18/1030
[3] El texto completo del US Cloud Act y algunos documentos relevantes en relación con esa legislación se encuentran en la pagina del Departamento de Justicia de los Estados Unidos en: http://bit.do/ePx9n

de información (Capítulo I); Delitos de contenido (Capítulo II); Delitos de propiedad intelectual y afines (Capítulo III); Delitos contra las telecomunicaciones (Capítulo IV); Delitos contra la nación y actos de terrorismo (Capítulo V); entre otros. Adicionalmente el marco jurídico relacionado con la investigación del ciberdelito y la prueba electrónica se complementa con las siguientes leyes:

- Código Penal;
- Código Procesal Penal;
- Ley No.126-02 sobre Comercio Electrónico, Documentos, y Firmas Digitales;
- Ley No. 153-98 General de Telecomunicaciones;
- Ley No. 65-00 sobre Derecho de Autor;
- Ley No. 20-00 sobre Propiedad Industrial;
- Ley No. 137-03 sobre Tráfico Ilícito de Migrantes y Trata de Personas;
- Ley No. 136-03 Código para el Sistema de Protección y los Derechos Fundamentales de Niños, Niñas y Adolescentes; y
- Ley No. 278-98 que modifica la Ley No. 489 del 22 de octubre de 1969 sobre Extradición.

La Ley 53-07 (Arts. 52, 53, 54, 55, 56) y el Código Procesal Penal (Arts. 30, 31 y 192) establecen disposiciones para la investigación, persecución, y adjudicación de ciberdelitos y el manejo de la prueba electrónica, así como medidas para ordenar la obtención, preservación y conservación de datos informáticos para propósitos de investigación de delitos, así como obligaciones de los proveedores de servicios para cooperar con las autoridades del sistema de justicia penal y la interceptación de telecomunicaciones a través de redes públicas y privadas.

Durante la última misión del Proyecto GLACY + sobre *Optimización de los procedimientos para la Asistencia Jurídica Mutua en materia de ciberdelito y prueba electrónica* llevada acabo en Santo Domingo el 2 y 3 de abril de 2019, se pudo conocer que existe una propuesta de reforma a la Ley 53/07 presentada por un Diputado. Los representantes de las organizaciones e instituciones reunidas durante esa actividad -entre ellas el Departamento de Investigación y Crímenes y Delitos de Alta Tecnología (DICAT) y la Procuraduría Especializada contra Crímenes y Delitos de Alta Tecnología (PEDATEC) consideran que la Ley 53/07 ha sido rebasada no solo por la evolución de los cambios tecnológicos sino en particular con respecto a las recientes tendencias y técnicas de investigación, y por tanto, consideran pertinente incluir en el proyecto de ley algunas cuestiones de carácter sustantivo y procedimental para mejorar las disposiciones que les han presentado obstáculos en la practica. Algunas de las cuestiones que pretenden incorporar en ese proyecto de reforma a la Ley 53/07 se encuentran:

- Responsabilidad de las personas morales para reportar incidentes a la infraestructura crítica nacional;
- Regular ampliamente la cadena de custodia en el entorno digital;
- Obligaciones de certificación para los peritos y expertos en el ámbito judicial;
- La figura del agente encubierto y el agente de reserva;
- Obligaciones de mejorar los sistemas de reportes estadísticos para los expedientes judicializados;
- Incluir y mejorar la sección de definiciones;
- Delimitar claramente los delitos que serán perseguidos por acción pública y los delitos a instancia privada;

- Obligaciones de los prestadores de servicios de Internet globales de entregar información en un plazo de 24 hrs. para casos de emergencia y ordenar la conservación de datos por un periodo mínimo de 3 años, que incluya a los datos de conexión;
- Obligación del INDOTEL de crear un registro de proveedores de servicios de internet y de usuarios a los que se les asigne direcciones IP y obligaciones de registro.

# 4. Conclusiones y Recomendaciones

## 4.1. Conclusiones

El estudio ha podido constatar la necesidad de realizar importantes cambios en la legislación penal y procesal penal de los países miembros de FOPREL a fin de asegurar un marco normativo apropiado tanto para la persecución penal de los delitos informáticos como para la obtención de evidencia digital con la finalidad de ser utilizada en cualquier proceso penal. Si bien el grado de profundidad y necesidad de las reformas difiere de país a país, es posible encontrar problemas comunes y diseñar soluciones normativas homogéneas tomando como modelo orientador las propuestas del Convenio de Budapest y su Reporte Explicativo.

La falta de regulación es mayor en el ámbito del derecho procesal penal que en el derecho penal sustantivo en el que algunos de los países objeto de este informe, aunque parcialmente, regulan figuras específicas referidas a los delitos informáticos. En materia procesal (al igual que en la gran mayoría de los países de América Latina) los códigos procesal penales modernos vigentes en la mayoría de los países analizados, basados en la idea de un sistema acusatorio, no han previsto medios de prueba eficaces tomando en consideración las necesidades propias de la evidencia digital. Estos Códigos han sido implementados en la región en un importante movimiento iniciado en la década de los 90's sobre la base de las propuestas del Código Procesal Penal Modelo para Iberoamérica. Este origen normativo común facilita la idea de pensar en herramientas procesales para la evidencia digital reguladas de manera similar.

Una legislación homogénea tanto a nivel de derecho penal sustantivo (descripción de las conductas punibles -tipos penales-) como en lo que se refiere a los poderes procesales para la obtención de evidencia digital redundará también en una mejor cooperación internacional en materia penal tanto entre los países miembros de FOPREL como con el resto de los países que forman parte del Convenio de Budapest.

Tanto en el establecimiento de las normas penales sustantivas como en las medidas procesal penales, resulta indispensable atender también a un adecuado régimen de garantías atendiendo especialmente al grado de intromisión importante que los medios de prueba en entornos digitales pueden significar para la intimidad y privacidad de los ciudadanos, la libertad de expresión y el derecho de defensa. En este sentido, deberá prestarse especial atención a los precedentes y la doctrina emanada de los órganos de aplicación de las convenciones internacionales sobre derechos humanos. Sin perjuicio de ello, los documentos y estudios sobre la materia realizados en el marco del Convenio de Budapest, pueden resultar de suma utilidad en esta definición de nuevos límites a los poderes estatales.

## 4.2. Recomendaciones

El texto de la Convención de Budapest reúne un conjunto de normas penales y procesales cuya utilidad ha sido probada por la experiencia del derecho comparado de todos los países que lo han usado como modelo (a modo de ejemplo, España, Francia, Italia, Alemania, Portugal en el ámbito europeo; Costa Rica, República Dominicana, Argentina, en el ámbito de América Latina). Constituye un **mínimo normativo** sobre la materia que puede ser complementado con nuevas herramientas de acuerdo con las necesidades y características normativas de cada país. En este sentido, recomendamos tomar como base de los proyectos normativos el texto del Convenio de Budapest como estándar

mínimo, agregando aquellas cuestiones novedosas tanto en materia de conductas no previstas como nuevas herramientas de investigación de acuerdo con las necesidades de cada país.

Entendemos que en el diseño de las nuevas leyes tanto penales como procesales resulta de suma utilidad no solamente el texto del Convenio de Budapest y su Reporte Explicativo, sino también todas las notas interpretativas y los documentos y estudios realizados por el Consejo de Europa desde la vigencia del Convenio.

En el proceso de elaboración de los proyectos nacionales de ley, es recomendable convocar en un proceso amplio y de múltiples partes interesadas al sector académico, legisladores de las comisiones de justicia, seguridad y comunicaciones, jueces, magistrados, fiscales, fuerzas de seguridad y policía, proveedores de servicios de Internet y telefonía y representantes de la sociedad civil. La presencia y apoyo de expertos de otros países y del Consejo de Europa con experiencia práctica sobre la temática puede resultar fundamental.