ACADEMIA DIPLOMÁTICA DEL PERÚ
"JAVIER PÉREZ DE CUÉLLAR"

PROGRAMA DE MAESTRÍA EN DIPLOMACIA Y RELACIONES INTERNACIONALES

TEMA DE INVESTIGACIÓN:

Desafíos y oportunidades de la adhesión del Perú al Convenio de Budapest sobre la Ciberdelincuencia

PRESENTADO POR:

Julio Eduardo Tenorio Pereyra

ASESORES:

Tema de Fondo: Ministra María del Pilar Castro Barreda.

Metodológico: Ph.D. Milagros Aurora Revilla Izquierdo.

Lima, 5 de noviembre de 2018

A mi familia, en especial a mi madre y hermana,
por motivarme continuamente ser una mejor
persona y creer siempre en mi; a mis seres
queridos, principalmente a mi enamorada,
por estar junto a mi cuando la necesito; a los
pioneros en el ciberespacio y a las siguientes
generaciones que continuarán nuestro camino.

AGRADECIMIENTOS

A mi asesora temática, Ministra María del Pilar Castro Barreda, por todo el apoyo, consejos, guía y tiempo brindado durante la elaboración y mejora de la presente tesis.

A los funcionarios de la Dirección de Ciencia y Tecnología, especialmente a la Embajadora Milagros Castañón Seoane y la Primera Secretaria Carmen Rocío Echevarría Sierra por todos los conocimientos y apoyo durante el proceso de investigación.

Al Mg. Erick Iriarte Ahon por los conocimientos brindados y los consejos relacionados al avance de la presente tesis.

Y al profesor Jaime Medina Huerta por guiarme en el camino correcto y brindarme las herramientas necesarias para conseguir todas las metas que me proponía en el tiempo.

RESUMEN

La presente tesis tiene como objetivo dar a conocer la importancia de la adhesión por parte del Estado peruano al Convenio de Budapest sobre la Ciberdelincuencia y las oportunidades que se deben explotar, así como los desafíos que se deberán enfrentar una vez que el Perú sea un Estado Parte.

Esta se inicia con la presentación de conceptos relacionados a la ciberdelincuencia y a los tratados internacionales. Posteriormente, se analizará el Convenio para identificar los principales beneficios, y la posición de los Estados Parte al momento de dar su consentimiento a obligarse al instrumento, y el avance en el proceso de adhesión de la región de América Latina. Finalmente, se presenta el proceso de adhesión al Convenio y de perfeccionamiento interno seguido por el Estado peruano, así como las declaraciones y reservas que se presentarán al momento de la adhesión, los desafíos y oportunidades que deberán considerarse, junto a una serie de conclusiones y recomendaciones a seguir en pro de los intereses nacionales relacionados al ciberespacio y la población peruana.

Palabras clave: Adhesión, Convenio, Budapest, Perú, Ciberdelincuencia, Delitos, Informáticos, Desafíos, Oportunidades.

ABSTRACT

The objective of this thesis is to make known the importance of the adhesion by the Peruvian State to the Budapest Convention on Cybercrime and the opportunities that must be exploited, as well as the challenges that will have to be faced once Perú becomes a State Part.

It begins with the presentation of concepts related to cybercrime and international treaties. Subsequently, the Convention will be analyzed to identify the main benefits, and the position of the States Parties when giving their consent to be bound to the instrument, and the progress in the accession process of the Latin American region. Finally, the process of adhesion to the Agreement and internal improvement followed by the Peruvian State, as well as the declarations and reservations that will present at the time of adherence, the challenges and opportunities to be considered, together with a series of conclusions and recommendations, are presented to continue in favor of the national interests related to cyberspace and the Peruvian population.

Keywords: Adhesion, Accession, Convention, Budapest, Peru, Cybercrime, Crimes, Computing, Challenges, Opportunities.

LISTA DE ACRÓNIMOS

ADPIC
Aspectos de los Derechos de Propiedad Intelectual relacionados con el Comercio

BID
Banco Interamericano de Desarrollo

CCI
Centro de Ciberseguridad Industrial (Perú)

CDI
Comisión de Derecho Internacional

CDPC
Comité Europeo para Problemas Criminales

COE
Consejo de Europa

DDoS
Ataque de denegación de servicios distribuidos

DCT
Dirección de Ciencia y Tecnología del Ministerio de Relaciones Exteriores (Perú)

DGPCP
Dirección General de Asuntos Criminológicos del Ministerio de Justicia y Derechos Humanos (Perú)

DGT
Dirección General de Tratados del Ministerio de Relaciones Exteriores (Perú)

DIRINCRI
Dirección de Investigación Criminal (Perú)

DIVINDAT
División de Investigación de Delitos de Alta Tecnología (Perú)

FBI
Oficina Federal de Investigación (EE.UU)

ITU
Unión Internacional de Telecomunicaciones

MINJUSDH
Ministerio de Justicia y Derechos Humanos (Perú)

ODILA
Observatorio de Delitos Informáticos de América Latina

ODS
Objetivos de Desarrollo Sostenible

OEA
Organización de los Estados Americanos

ONU
Organización de las Naciones Unidas

ONGEI
Oficina Nacional de Gobierno Electrónico e Informática (Perú)

OSCE
Organización de Seguridad y Cooperación en Europa

OTAN
Organización del Tratado del Atlántico Norte

PBI
Producto Bruto Interno

PCM
Presidencia del Consejo de Ministros (Perú)

PeCERT
Coordinación de Emergencias en Redes Teleinformáticas (Perú)

PNP
Policía Nacional del Perú

SEGDI
Secretaría de Gobierno Digital (Perú)

TI
Tecnología de la Información

TIC
Tecnología de la información y comunicación

ÍNDICE DE CUADROS

ÍNDICE DE GRÁFICOS

ÍNDICE

INTRODUCCIÓN

En la Academia Diplomática del Perú, durante sus años de funcionamiento, se han elaborado tesis sobre problemas internacionales de tipo limítrofe, político, de seguridad y sobre cooperación internacional. En la última década se incluyeron temas relacionados a innovación, cooperación para reducir brechas tecnológicas, y la presente tesis continúa los aportes en materia de ciberdelincuencia y los delitos informáticos como problemas que generan daños al país y que deben ser combatidos a la brevedad posible para reducir riesgos futuros.

Uno de los grandes aportes de la globalización fue la masificación del uso de nuevas tecnologías alrededor del mundo, especialmente las que hacían uso intensivo del Internet. Gracias a la tecnología y los servicios en el ciberespacio, se eliminaron fronteras y conceptos de tiempo al permitir a las personas y empresas una comunicación instantánea desde cualquier lugar y en cualquier momento. A esto se le suma que trajo beneficios para la educación, trabajo, comercio y otros sectores que encontraron en el Internet una herramienta para desarrollarse a un ritmo más rápido.

La ciberdelincuencia es un problema internacional que crece cada día. En los últimos veinte años el mundo ha vivido casos como la paralización de actividades en organizaciones alrededor del mundo mediante software ransomware[1] o robo de datos informáticos para obtención de beneficios. El Perú registró casos de ciberdelitos similares contra empresas, instituciones y personas que generaron considerables pérdidas económicas en los últimos años.

El Perú fue de los primeros países que a inicios de este siglo trató temas de delitos informáticos en su Código Penal incorporando artículos relacionados

[1] El ransomware (también conocido como rogueware o scareware) restringe el acceso a su sistema y exige el pago de un rescate para eliminar la restricción. Los ataques más peligrosos los han causado ransomware como WannaCry, Petya, Cerber, Cryptolocker y Locky. Definición de Avast Software, Inc.

al uso o ingreso de manera indebida de base de datos, sistemas o redes para obtener un beneficio o generar daños. Este esfuerzo tiene jurisdicción y margen de acción nacional, sin tener una respuesta rápida y efectiva cuando los delitos son cometidos desde un punto fuera del territorio peruano.

El Estado peruano está dando importantes pasos en la materia, pero es necesario que con la ayuda de instrumentos internacionales como el Convenio de Budapest sobre la Ciberdelincuencia pueda combatir el mal uso de las Tecnologías de la Información y Comunicación bajo el esquema de esfuerzos y colaboración internacional. Parte de los beneficios de adherirse al Convenio son la cooperación internacional, búsqueda de redes de computadoras e interceptación, facilitación para obtención de información, la investigación y represión del delito para lograr el orden público y mantenimiento de la paz, entre otros.

Un factor importante es el combate de una amenaza común para el mantenimiento de la paz mediante la investigación y la persecución del delito.

La presente tesis tiene como propósito dar a conocer los principales casos de ciberdelitos que sucedieron desde inicio de los 90 y las pérdidas generadas por los mismos; así como: la importancia del Convenio de Budapest sobre la Ciberdelincuencia para los Estados Parte; los desafíos a superar tras una futura adhesión al Convenio y las oportunidades que serán de gran beneficio para la población, empresas e instituciones en el Perú, las cuales son más dependientes del ciberespacio y los servicios que están disponibles. La tesis se divide en tres capítulos, que se detallan a continuación.

El primer capítulo presentará las definiciones de conceptos a ser tratados en la tesis, como delitos informáticos, ciberdelincuencia y todo lo concerniente a los tratados internacionales; se presentarán algunos casos destacados de

ciberdelincuencia en el mundo, y se brindarán datos estadísticos de las pérdidas económicas generadas en el mundo, la región y en el Perú.

El segundo capítulo se enfocará al Convenio de Budapest sobre la ciberdelincuencia, presentando los antecedentes históricos y jurídicos del Convenio; un análisis del mismo enfocado en los delitos establecidos; la presentación de los países signatarios con las principales declaraciones y reservas presentadas al momento del depósito del instrumento de aprobación, ratificación o adhesión; y los avances realizados por los Estados de la región de América Latina y el Caribe para la adhesión al Convenio.

El último capítulo tratará sobre los avances del Perú para la adhesión al Convenio de Budapest sobre la Ciberdelincuencia, incluyendo el contexto sobre el cual el Perú decide adherirse al Convenio; los antecedentes históricos y legales; el proceso de Perfeccionamiento Interno del Tratado; las declaraciones y reservas que presentará el Perú al momento del depósito del instrumento de adhesión; y las oportunidades y desafíos de la adhesión al Convenio para el Ministerio de Relaciones Exteriores y los Ministerios e instituciones que están involucrados.

La principal motivación para la elaboración de la presente tesis de investigación es contribuir a la toma de decisiones en pro de los intereses nacionales relacionados al ciberespacio, y las tecnologías de la información y comunicación en un mundo donde la revolución digital y el Internet abierto para todos no tienen confines nacionales; brindando mejores herramientas al Estado peruano para proteger los derechos relacionados a datos informáticos y la red de las personas naturales y jurídicas del país, haciendo uso del Convenio de Budapest sobre la Ciberdelincuencia para reprimir la delincuencia sin frontera que hace uso de nuevas tecnologías y el ciberespacio.

I. ALCANCES CONCEPTUALES Y CASOS DE CIBERDELINCUENCIA

En el presente capítulo tiene como objetivo tratar las principales definiciones de los conceptos centrales a ser trabajados a lo largo de la presente tesis; los principales hechos acaecidos relacionados a la ciberdelincuencia en países ubicados en diferentes regiones del mundo desde inicios de 1990 hasta la fecha; y las pérdidas generadas, no solo a nivel económico, sino también a nivel social, al perderse oportunidades de inversión con esos recursos perdidos.

En la primera parte del capítulo se presentarán los términos relacionados a los delitos informáticos y ciberdelincuencia que se tratarán alrededor de la tesis, entre los que se encuentran la piratería, el robo de datos confidenciales, el fraude informático, la falsificación de información, la alteración de datos, la destrucción de datos, la privacidad, el ciberespacio, los delitos informáticos y su relación con la ciberdelincuencia, la infraestructura crítica y la prueba electrónica.

Posteriormente se tratan los conceptos relacionados a los tratados internacionales, la adhesión, el perfeccionamiento interno, la ratificación de un tratado, las reservas y las declaraciones a un tratado.

La segunda parte del capítulo presenta casos emblemáticos como el hackeo y robo de cuentas del Banco de San Francisco por parte de un joven programador ubicado en San Petersburgo; el robo de un billón de cuentas de Yahoo por parte de un grupo de hackers; el robo de data sensible a Sony Pictures; el robo de data de JP Morgan Chase & Co para manipular los precios de acciones en el mercado y obtener ganancias y lavarlo al transformarlas en Bitcoins; finalmente se presentan casos relacionados a robos en bancos colombianos y peruanos.

En la última parte del capítulo presenta las pérdidas económicas en diferentes periodos de tiempo, tanto a nivel mundial, regional y en relación al Perú. Dichas pérdidas están proyectadas a nivel mundial para el año 2019 en 2 100 000 millones USD. En la región latinoamericana, las pérdidas económicas son cercanas a los 90 000 millones USD y en el caso peruano, las pérdidas registradas ascendieron el año pasado en aproximadamente 4 782 millones USD.

1.1. Alcances Conceptuales

En la presente sección se presentarán los conceptos que serán utilizados a lo largo de la presente tesis y que ayudarán a un mejor entendimiento de los delitos informáticos presentados en el Convenio de Budapest sobre la Ciberdelincuencia y la legislación peruana.

1.1.1. En relación a los delitos y ciberdelincuencia

La piratería

La piratería es un problema global que afecta a diferentes industrias en términos económicos y de imagen. La definición de la misma evolucionó en el tiempo al igual que su rango de acción y forma de comisión del delito. García, Jeldres, Mardones dan una definición inicial del término piratería y su evolución en el tiempo:

> El término pirata proviene del latín pirata, que significa “el que emprende o el que intenta fortuna, sin embargo, las acciones de estos hombres estaban al margen de cualquier ley. Según la historia, el más antiguo de los piratas fue un griego de nombre Polícrates, famoso por haber creado una gran fortuna con sus robos. (…) Hoy en día el concepto de pirata se relaciona al establecido en sus orígenes, pero adaptado a las condiciones de la sociedad actual. Piratería es usado

> generalmente para describir el crimen deliberado de la copia ilegal a gran escala (García, Jeldres, Mardones, 2007, p. 72).

López incorpora al término piratería, elementos como derecho de autor y lo relaciona con actividades y obras más acordes a la época actual:

> El término “piratería” abarca la reproducción y distribución de copias de obras protegidas por el derecho de autor, así como su transmisión al público o su puesta a disposición en redes de comunicación en línea, sin la autorización de los propietarios legítimos, cuando dicha autorización resulte necesaria legalmente. La piratería afecta a obras de distintos tipos, como la música, la literatura, el cine, los programas informáticos, los videojuegos, los programas y las señales audiovisuales (López, s.f. p. 1).

El robo de datos confidenciales

La División de Seguridad de la Información de la Oficina del Director de Información de Iowa define a los datos confidenciales como información de identificación personal (IIP) que una persona no desea que sean obtenidos sin su consentimiento. Estos datos pueden ser considerados patrimonio tangible o intangible de una persona o institución. Estos datos pueden incluir el número de identificación, el número de teléfono personal o de terceras personas registradas por uno mismo, las cuentas bancarias, las contraseñas de servicios, entre otros (“What is Confidential Data?”, s.f.).

En tal sentido, el robo de datos confidenciales se entiende como un delito contra el patrimonio, por el cual se produce el apoderamiento de información de identificación personal ajena, la cual se obtuvo violentando medidas de seguridad.

El fraude informático

En el Perú, el artículo 8 de la Ley Nº 30096, Ley de Delitos Informáticos; y su modificatoria, Ley 30171, Ley que modifica la Ley 30096, Ley de Delitos Informáticos definen al fraude informático como un delito informático y sus características:

> El que deliberada e ilegítimamente procura para sí o para otro un provecho ilícito en perjuicio de tercero mediante el diseño, introducción, alteración, borrado, supresión, clonación de datos informáticos o cualquier interferencia o manipulación en el funcionamiento de un sistema informático (…) (Ley 30171, 2014)

Esta definición del artículo de la ley tras su modificación en el año 2004 cumple con el concepto de marco legal común con los países miembros del Convenio de Budapest sobre la Ciberdelincuencia, por lo que es considerado en más de cincuenta países.

La falsificación de información

La Enciclopedia Jurídica define la falsificación como la adulteración, corrupción, cambio o imitación para perjudicar a otro u obtener ilícito provecho (“Falsificación”, 2014).

Arias y Aristizábal citan a varios autores, entre los que se encuentran Bollinger, Smith, Bhatt, Speak, Spijkervet, Herder, Davenport y Earl, para definir a la información como datos procesados, organizados o con significado, necesarios para la creación de conocimiento, la cual es valiosa, evaluada, validada y codificada (Arias, Aristizábal, 2011, p. 98).

Por ende, la falsificación de información es la adulteración o imitación de datos procesados con el fin de perjudicar a otro u obtener ilícito provecho.

La alteración de datos

La alteración es la variar, cambiar o hacer diferente algo (“¿Qué es la alteración?”, s.f.)

Un dato es un conjunto discreto, de factores objetivos sobre un hecho real. (…) Los datos describen únicamente una parte de lo que pasa en la realidad y no proporcionan juicios de valor o interpretaciones, y por lo tanto no son orientativos para la acción. La toma de decisiones se basará en datos (IIBI UNAM, s.f.).

Con las definiciones brindadas líneas arriba, se entiende a la alteración de datos como la variación, cambio o la acción de hacer diferente un conjunto de datos, los cuales contienen información almacenada para la toma futura de decisiones.

La destrucción de datos

Se entiende a la destrucción como el acto de arruinar o dañar en forma grave a algo o a alguien para dejarlo arruinado, inservible o dañado (“Concepto de destrucción”, s.f.). En relación con los datos, se infiere que se trata de la acción de dejar inservibles datos que contienen información almacenada.

La privacidad

El concepto de privacidad está relacionado tradicionalmente a las acciones y vida privada de las personas en un ámbito reservado, lo que también es conocido como intimidad. Sarachaga hace uso del concepto tradicional, y lo relaciona al uso las nuevas tecnologías de la información y comunicación, junto a una serie de riesgos propios de ese entorno:

> La privacidad, en su forma tradicional, puede definirse como aquello que una persona lleva a cabo en un ámbito reservado, algo que se mantiene fuera del alcance de otras personas, y puede ser asociado al concepto de intimidad. Sin embargo, actualmente la tecnología está muy presente en nuestras vidas, por lo que el concepto de privacidad obtiene una dimensión mucho mayor de la que tenía en el pasado. Los datos se convierten en el activo más preciado, además de que es sencillo recogerlos, almacenarlos y tratarlos. (…) Las redes sociales, las compras con tarjetas, las llamadas telefónicas y otras muchas actividades que realizamos día a día son fuente de una cantidad inmensa de datos, entre los cuales se encuentran nuestros datos personales. La tecnología a pesar de ser traducirse en herramientas que nos facilitan el día a día automatizando tareas que nunca antes hubiésemos imaginado, conlleva una serie de riesgos, y la pérdida de privacidad es uno de ellos y un tema muy serio a tratar (Sarachaga, 2017).

En la presente década la aparición de nuevos servicios en Internet requiere que parte de nuestra información, archivos y actividades dejen de ser privados para ser utilizados para mejoras de servicio o para ser utilizados por terceros para fines comerciales.

La prueba electrónica

Según Bueno, la prueba electrónica es una prueba presentada de manera informática, la cual depende de un elemento intangible y de un medio físico para su visualización:

> “Cualquier prueba presentada informáticamente y que estaría compuesta por dos elementos: uno material que depende de un hardware, la parte física y visible de la prueba para cualquier usuario de a pie, por ejemplo, la carcasa de un Smartphone o una memoria USB; y por otro lado un elemento intangible que es representado por un software consistente en los metadatos y archivos electrónicos modulados a través de unas interfaces informáticas” (Bueno, 2014, p. 130).

Los manejos de las pruebas electrónicas generan desafíos adicionales a los ya existentes con pruebas físicas, tales como la identificación de alteración

indebida; la obtención, traslado y custodia; o la correcta incorporación de las pruebas electrónicas un el proceso judicial.

El Ciberespacio

Clarke y Knake proponen una definición de ciberespacio que da un acercamiento simple de su funcionamiento:

> El ciberespacio lo conforman todas las redes informáticas del mundo y todo lo que ellas conectan y controlan. No se trata solo de internet. Es importante dejar en claro la diferencia. Internet es una red de redes abierta. Desde cualquier red de internet, podemos comunicarnos con cualquier ordenador conectado con cualquiera otra de las redes de internet. El ciberespacio es Internet más montones de otras redes de ordenadores a las que, se supone, no es posible acceder desde internet. Algunas de esas redes privadas son muy semejantes a internet, pero, al menos teóricamente, se encuentran separadas de ella (Clarke y Knake, 2011, p. 104).

El ciberespacio, por ende, brinda muchas oportunidades para todos sus usuarios y es un medio por el cual los mismos, personas u organizaciones, se pueden conectar para hacer diferentes actividades que serán de beneficio para los mismos. Martínez, Leyva, Félix, Cecenas y Ontiveros citan a Mayans para explicar algunos de los beneficios del ciberespacio, tanto a nivel económico y de accesibilidad:

> (…) El ciberespacio es una dimensión más accesible económicamente que otros canales de difusión e información de utilidad comparable. Esto hace posible que puedan ser millones sus 'habitantes'. (…) El ciberespacio es un entorno conceptualmente accesible y manipulable, donde existen muchas formas de participación y ni siquiera las más complejas y completas son inaccesibles, dado el carácter de lenguaje de su forma de acceder y participar activamente en él (Martínez, Leyva, Félix, Cecenas, Ontiveros, 2014, p. 49).

Los delitos Informáticos

Los delitos informáticos han sido mencionados desde la década de los 60 y su concepto ha evolucionado en el tiempo. En esa misma década se consideraba a los delitos informáticos como daños físicos contra infraestructura informática, en la década de los 70 se empezó a utilizar de manera ilícita los sistemas informáticos. Una década después comenzaron los delitos contra infraestructuras críticas, piratería y delitos de patentes. En este periodo de tiempo Callegari definía los delitos informáticos como aquellos que se dan con la ayuda de la informática o de técnicas anexas (Callegari, 1985, p. 115). Un ejemplo claro de la época era la piratería de software y archivos multimedia, que se incrementarían exponencialmente en las dos siguientes décadas. Con la llegada del Internet a los hogares a inicios de la década de los 90 los delincuentes informáticos tenían un nuevo medio y herramientas para realizar sus actividades.

Una definición que enmarca los temas presentados previamente es el que brinda Villavicencio, quien alega que:

> Los delitos informáticos se vinculan con la idea de la comisión del crimen a través del empleo de la computadora, internet, etcétera; sin embargo, esta forma de criminalidad no solo se comete a través de estos medios, pues éstos solo son instrumentos que facilitan, pero no determinan la comisión de estos delitos. Esta denominación es poco usada en las legislaciones penales; no obstante, bajo ella se describe una nueva forma de criminalidad desarrollada a partir del elevado uso de la tecnología informática (Villavicencio, 2014, p. 286).

En base a las definiciones presentadas previamente, se define a los delitos informáticos no como nuevas conductas ilícitas, sino como nuevas formas como se desarrollan los delitos mediante el uso de medios informáticos conectados a Internet o de manera física teniendo acceso a un dispositivo con algún puerto que permita una conexión al sistema y a los archivos que están contenidos.

El siguiente cuadro presenta los principales delitos informáticos.

Cuadro Nº 1: Principales delitos informáticos

Categoría de Delito	Tipo de Delito
Delitos contra la intimidad	Almacenamiento, modificación, revelación o difusión ilegal de datos personales.
Delitos relativos al contenido	Difusión, especialmente por Internet, de pornografía, y en especial de pornografía infantil, declaraciones racistas e información que incita a la violencia.
Delitos económicos, acceso no autorizado y sabotaje	La piratería, el sabotaje informático y la distribución de virus, el espionaje informático, y la falsificación y el fraude informáticos.
Delitos contra la propiedad intelectual	Delitos contra la protección jurídica de programas y la protección jurídica de las bases de datos, los derechos de autor y derechos afines.

Elaboración: Propia
Fuente: Ing. Walter Edison Alanya Flores (Colegio de Ingenieros del Perú de Tacna)

Ciberdelincuencia

A la fecha no existe una definición consensuada del término ciberdelincuencia, diferentes autores presentan su definición teniendo como elemento central el uso de dispositivos informáticos y una red para conectarse a otros dispositivos.

La Unión Internacional de Telecomunicaciones (ITU) en su informe de Comprensión de la ciberdelincuencia: Fenómenos, dificultades y respuesta jurídica, del año 2014, brinda dos definiciones de ciberdelincuencia basados en los conceptos trabajados en el taller que tuvo lugar con ocasión del 10º Congreso de las Naciones Unidas sobre Prevención del Delito y Tratamiento del Delincuente:

> *Ciberdelincuencia en sentido estricto (delito informático) comprende cualquier comportamiento ilícito realizado mediante operaciones*

> *electrónicas que atentan contra la seguridad de sistemas informáticos y de los datos que éstos procesan. En sentido general, ciberdelincuencia (delitos relacionados con las computadoras) comprende cualquier comportamiento ilícito cometido por medio de un sistema informático o una red de computadores, o relacionado con éstos, incluidos delitos tales como la posesión ilícita y la puesta a disposición o distribución de información mediante sistemas informáticos o redes de computadores* (ITU, 2014, p. 11).

Cabe resaltar que algunos años atrás, Hale trató de dar una definición más precisa incluyendo los objetivos o intenciones, pero ese concepto puede excluir delitos que pueden ser considerados ciberdelincuencia en ciertos acuerdos internacionales, tales como la Legislación Modelo de la Commonwealth sobre la delincuencia informática y relacionada con los computadores o el Convenio del Consejo de Europa sobre la Ciberdelincuencia (ITU, 2014, p. 11).

Mehan brinda un concepto del término ciberdelincuencia, el cual considera:

> Todas las formas de actividad delictiva perpetradas utilizando tecnología de la información e Internet. (...) El ciberdelito no es más que actividades delictivas tradicionales, como el robo y el fraude, que se lleva a cabo utilizando las tecnologías digitales más avanzadas y que aprovecha la creciente dependencia de la tecnología de la información. Esta dependencia es un factor debilitante que se ha incrementado exponencialmente con la abundancia de sistemas de información interconectados, el desarrollo de la computación en la nube, la virtualización, los dispositivos móviles y los sitios de redes sociales (Mehan, 2014, p. 19-20).

Este concepto incluye las principales herramientas y medios para poder realizar las actividades delictivas, y, sobre todo, se hace mención de la convergencia que se está viviendo en la actualidad y que considera los dispositivos más utilizados por la población mundial (computadoras, laptops, celulares, tabletas, entre otros).

Al igual que los delitos tradicionales, los ciberdelitos también han evolucionado y su crecimiento está relacionándose al crecimiento en la cantidad de usuarios que usan servicios en la red. Morgan detalla esta evolución de la siguiente manera:

> Al igual que el crimen callejero, que históricamente creció en relación con el crecimiento de la población, estamos presenciando una evolución similar de la ciberdelincuencia. No se trata solo de armamento más sofisticado, se trata tanto del creciente número de objetivos humanos y digitales (Morgan, 2017, p. 4).

El objetivo fundamental de los ciberdelincuentes es maximizar su rentabilidad financiera a la vez que minimizan su riesgo. Un objetivo secundario podría ser el deseo de obtener poder a través del control de información y / o fuentes de información (Mehan, 2014, p. 20).

La relación entre Delitos Informáticos y Ciberdelincuencia

Los términos presentados previamente tienen una estrecha relación, la cual imposibilita el excluir un concepto del otro. No se puede hablar de delitos informáticos sin considerar a la ciberdelincuencia, la cual se diferencia de la primera al tener que utilizar una red para cometer el delito. Y de igual manera no se puede hablar de ciberdelincuencia sin considerar la ciberseguridad, elemento que tanto el Estado, empresas y sociedad civil deben implementar para reducir los riesgos de ser víctimas de ciberdelitos.

Sobre la última relación, la Asamblea General de las Naciones Unidas en el año 2010, mediante la Resolución 64/211 “Creación de una Cultura Global de Ciberseguridad y Análisis de los Esfuerzos Nacionales para Proteger las Infraestructuras de Información Críticas” recomienda incluir en el marco legal de los Estados miembros vía artículo 13 de los anexos, los temas relacionados a ciberdelincuencia en sus políticas de ciberseguridad (ONU, 2010, p. 1-5).

El informe de la ITU del 2016 destaca que el término “ciberdelincuencia” es más restrictivo que el de delito informático, ya que el primero requiere del uso de una red informática y los delitos informáticos en cambio consideran también los delitos a sistemas autónomos sin necesidad de hacer uso de una red para cometer el acto, en otras palabras, con instrumentos tecnológicos físicos se puede realizar el delito de sustracción, modificación o eliminación de data o de todo el sistema intervenido. (ITU, 2014, p. 11).

La infraestructura Crítica

Relacionada y cada vez más dependiente del ciberespacio, una infraestructura crítica puede ser definida como: una infraestructura que resulta esencial para la seguridad económica, el fluido funcionamiento del gobierno en todos sus niveles, y la sociedad en su conjunto (Thill, 2010, p. 10).

Sánchez, propone distribuir en diez categorías a las infraestructuras críticas disponibles a la fecha:

> Son infraestructuras críticas las siguientes: Administración (servicios básicos, instalaciones, redes de información, y principales activos y monumentos del patrimonio nacional); Instalaciones del Espacio; Industria Química y Nuclear (producción, almacenamiento y transporte de mercancías peligrosas, materiales químicos, biológicos, radiológicos, etc.); Agua (embalses, almacenamiento, tratamiento y redes); Centrales y Redes de energía (producción y distribución); Tecnologías de la Información y las Comunicaciones (TIC); Salud (sector e infraestructura sanitaria); Transportes (aeropuertos, puertos, instalaciones intermodales, ferrocarriles y redes de transporte público, sistemas de control del tráfico, etc.); Alimentación (producción, almacenamiento y distribución); y Sistema Financiero y Tributario (entidades bancarias, información, valores e inversiones) (Sánchez, 2011).

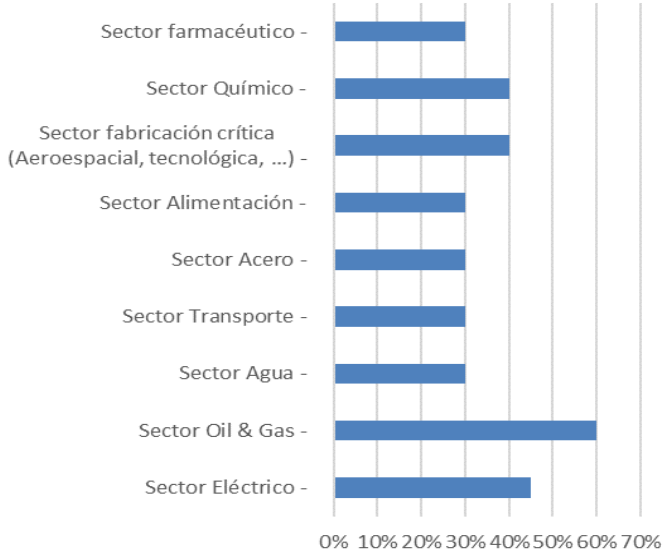
Estas funcionan y son monitoreados mediante el uso de sistemas basados en las tecnologías de la información y comunicación. Si bien la adopción de nuevas tecnologías digitales permite una gestión más eficiente de las

infraestructuras críticas en términos de escala, distancia y tiempo, también introduce nuevas vulnerabilidades que hacen que la protección de las infraestructuras de información críticas sea una tarea importante y desafiante (OEA, 2018, p. 15). Esto debido a personas u organizaciones delictivas que buscan obtener información confidencial, desestabilizar los sistemas o generar daños físicos a infraestructuras.

Por tanto, las infraestructuras críticas tienen una importancia grande para la sociedad en general que cada día es más dependiente de los servicios que estas brindan. El fallo en una de las infraestructuras podrá repercutir en otras, las cuales en algunos casos están relacionadas y dará a conocer deficiencias en términos de seguridad y respuesta ante una crisis.

En la categoría de Alimentos podemos encontrar a las organizaciones industriales, las cuales brindan productos y servicios para la vida diaria y también son fuente de trabajo para la población, pero, sobre todo, tienen una gran dependencia de las infraestructuras críticas. El Centro de Ciberseguridad Industrial elaboró un estudio refleja el nivel de sensibilidad de las organizaciones industriales del Perú relacionadas a las infraestructuras críticas como se puede ver en el siguiente gráfico (CCI, 2017).

Gráfico Nº 1: Nivel de sensibilidad de las organizaciones industriales del Perú (2017)



Fuente: Centro de Ciberseguridad Industrial
Elaboración: Centro de Ciberseguridad Industrial

La misma institución en la sección de "Detalle País" de su sitio web menciona que el Perú cuenta con diversos organismos públicos nacionales que velan por generar un marco legal adecuado que garantice la progresiva incorporación de la ciberseguridad industrial en las estructuras de las empresas con presencia nacional (principalmente infraestructuras críticas), entre las principales cabe destacar la Secretaría de Gobierno Digital (SEGDI)[2] y la Coordinación de Emergencias en Redes Teleinformáticas (PeCERT). También describe el nivel de sensibilidad de las organizaciones industriales del Perú de acuerdo a los siguientes porcentajes (CCI, 2017)

La Sociedad de la Información y del Conocimiento

Según Torres, la Sociedad de la Información tiene como eje central el conocimiento teórico y advierte que los servicios basados en el conocimiento se convertirán en la estructura central de la nueva economía, donde las

[2] En el detalle país se menciona aún a la Oficina Nacional de Gobierno Electrónico e Informática (ONGEI)

tecnologías de la comunicación tienen un factor clave de aceleración de la globalización económica. En cambio, la Sociedad del Conocimiento busca incorporar una concepción más integral, no solamente ligado a lo económico y captura mejor la complejidad y dinamismo de los cambios que se están llevando. Busca empoderar y desarrollar todos los sectores de la sociedad (Torres, 2005, p. 1-2)

1.1.2. En relación a los tratados

Los tratados internacionales

Novak y García-Corrochano dan a conocer la evolución de los tratados internacionales su importancia en el derecho internacional público a lo largo del tiempo desde hace poco más de 300 años:

> Los tratados internacionales se han convertido progresivamente, en la fuente más recurrida del derecho internacional contemporáneo. Su incorporación y posterior desarrollo en esta disciplina fue fruto del intensivo proceso codificador que se inicia a fines del siglo XVIII, el mismo que tuvo como propósito ordenar sistemáticamente las normas consuetudinarias existentes, modificar algunas de ellas y elaborar reglas nuevas, con un criterio jurídico adecuado (Novak, García-Corrochano, 2003, p. 130).

Si bien existen diferentes definiciones de tratados, para la presente tesis se hará uso del concepto brindado por el Ministerio de Relaciones Exteriores en la Directiva N° 002-DGT/RE-2013 “Lineamientos Generales sobre la suscripción, perfeccionamiento y registro de los Tratados”, la cual estaba basada en el concepto de tratados brindado por la Convención de Viena sobre el Derecho de los Tratados de 1969:

> Acuerdo internacional celebrado por escrito entre Estados, o entre Estados y Organizaciones Internacionales, o entre Estados y otros Sujetos de Derecho Internacional con capacidad para ello, regido por el Derecho Internacional, ya que conste en un documento único o en

> dos o más instrumentos conexos y cualquiera sea su denominación particular. Puede ser bilateral, Plurilateral o Multilateral.
> Los tratados son suscritos por el Presidente de la República, el Ministro de Relaciones Exteriores o cualquier funcionario público que haya sido facultado para ello a través de Plenos Poderes (MRE, 2013a, p. 2-3).

Según Novak y García-Corrochano, los tratados se pueden clasificar en base a diferentes criterios, los más usuales son: en cuanto al número de Estados Parte, en cuanto la posibilidad de acceso, en cuanto a su forma de celebración, en cuanto a su contenido, en cuanto a la materia objeto del tratado. Y los mismos tienen un ámbito de aplicación que puede ser temporal o espacial (Novak, García-Corrochano, 2003, p. 149-160).

El Perú es un Estado Parte de a la Convención de Viena de 1969 sobre el Derecho de los Tratados desde momento de su ratificación el 14 de septiembre del año 2000. Con dicho acto hizo constancia internacional de su consentimiento a obligarse al instrumento y sus pautas para la firma de tratados internacionales.

Según procedimientos de dicho tratado, posteriormente se procedió a notificar a los demás Estados Parte las reservas presentadas por el Estado peruano. Las mismas estaban relacionadas la aplicación de los artículos 11 (“Formas de manifestación del consentimiento en obligarse por un tratado”), 12 (“Consentimiento en obligarse por un tratado manifestado mediante la firma”) y 25 (“Aplicación provisional”) de la Convención, los cuales en el Perú están sujetos a un proceso dispuesto por la Constitución Política de 1993 que incluye la firma, aprobación, ratificación, adhesión y entrada en vigor del instrumento internacional (ONU, s.f.).

De igual manera, un dato de interés sobre el proceso de ratificación y reservas seguido por el Estado peruano, se encuentra la objeción por parte de Austria, el 14 de noviembre del año 2001, por las reservas presentadas por el Perú. Austria alegó que según el artículo 20, párrafo 5 del Convenio, los doce meses

para hacer objeciones por parte de otros Estados Parte concluyó previo a la comunicación de Austria a la Secretaría General, por lo que considera que la objeción queda sin efecto legal, debido a la existencia de una aceptación tácita.

La adhesión a un tratado

Para las situaciones donde un Estado no participó en la creación del tratado, pero se le permite formar parte del mismo de manera ulterior, por lo que existe la opción de la adhesión. La Organización de las Naciones Unidas, en base a los artículos 2.1.b, y 15 de la Convención de Viena sobre el Derecho de los Tratados de 1969, define un concepto de adhesión:

> La "adhesión" es el acto por el cual un Estado acepta la oferta o la posibilidad de formar parte de un tratado ya negociado y firmado por otros Estados. Tiene los mismos efectos jurídicos que la ratificación. En general, la adhesión se produce una vez que el tratado ha entrado en vigor. (ONU, 2018).

El perfeccionamiento interno de un tratado

Se entiende por perfeccionamiento interno a: los actos dispuestos por la legislación interna destinados a la aprobación y ratificación de los acuerdos internacionales suscritos por el Estado peruano, y su posterior incorporación al Derecho nacional (MRE, 2013a, p. 3).

La ley peruana N°29158, Ley Orgánica del Poder Ejecutivo en su artículo 8.1.i establece que el Presidente de la República del Perú en su calidad de Jefe de Estado tiene la función de celebrar y ratificar tratados, los cuales en base al artículo 5, párrafos 6 y 18 de la Ley N° 29357 son negociados y suscritos por el Ministerio de Relaciones Exteriores como entidad rectora en coordinación con los sectores correspondientes, por contar tanto el Presidente como el Ministro de Relaciones exteriores con plenos poderes.

Como menciona el punto 6.2 de la Directiva N° 002-DGT/RE-2013, el MRE deberá realizar solicitudes previas a los sectores e instituciones vinculados con la materia del tratado para ser absueltas a la brevedad posible, lo que favorecerá a la negociación, firma y perfeccionamiento interno. Si no se hizo la consulta previa a la suscripción del tratado, la DGT podrá solicitarla posteriormente en el momento de su perfeccionamiento y definirá su vía para este procedimiento, si es simplificada o agravada.

La Constitución Política del Perú define la vía de perfeccionamiento en los artículos 56 y 57 del Capítulo II “De los tratados” como se detallan a continuación.

> CONCORDANCIA: Ley N° 26647 (Normas que regulan actos relativos al perfeccionamiento nacional de los Tratados celebrados por el Estado Peruano).
>
> Artículo 56.- Aprobación de tratados
> Los tratados deben ser aprobados por el Congreso antes de su ratificación por el Presidente de la República, siempre que versen sobre las siguientes materias:
>
> 1. Derechos Humanos.
> 2. Soberanía, dominio o integridad del Estado.
> 3. Defensa Nacional.
> 4.Obligaciones financieras del Estado.
>
> También deben ser aprobados por el Congreso los tratados que crean, modifican o suprimen tributos; los que exigen modificación o derogación de alguna ley y los que requieren medidas legislativas para su ejecución (Congreso, 1993, p. 18).

Esto es lo que se conoce como vía agravada.

En contraposición, la vía simplificada se encuentra en el artículo 57 de la Constitución (Tratados Ejecutivos), la que señala:

> Artículo 57.- Tratados Ejecutivos
> El Presidente de la República puede celebrar o ratificar tratados o adherir a éstos sin el requisito de la aprobación previa del Congreso en materias no contempladas en el artículo precedente. En todos esos casos, debe dar cuenta al Congreso.
>
> Cuando el tratado afecte disposiciones constitucionales debe ser aprobado por el mismo procedimiento que rige la reforma de la Constitución, antes de ser ratificado por el Presidente de la República.
>
> La denuncia de los tratados es potestad del Presidente de la República, con cargo de dar cuenta al Congreso. En el caso de los tratados sujetos a aprobación del Congreso, la denuncia requiere aprobación previa de éste (Congreso, 1993, p. 18).

El artículo 4 (“Alcances del concepto de las normas legales”) del Reglamento que establece disposiciones relativas a la publicidad, publicación de proyectos normativos y difusión de normas legales de carácter general, emitido por Decreto Supremo N° 001-2009-JUS, dicta que los tratados deben ser publicados en el Diario Oficial El Peruano.

La atribución de aprobar tratados por parte del Congreso de la República se establece en el artículo 102 de la Constitución Política del Perú de 1993, y el cumplir y hacer cumplir los tratados es una atribución otorgada al Presidente de la República en el artículo 118 de la misma Constitución.

En el caso de los Plenos Poderes, el Decreto Supremo N° 031-2007-RE establece que cualquier funcionario de la Administración Pública puede suscribir un tratado si cuenta con los Plenos Poderes que serán otorgados por el Ministerio de Relaciones Exteriores mediante Resolución Suprema, a través de un diploma que la acompaña. Para esto, se deberá enviar una solicitud al viceministro de Relaciones Exteriores que lo derivará a la Dirección General

de Tratados. Cabe señalar que ni el Presidente de la República, ni el Ministro de Relaciones Exteriores necesitan Plenos Poderes.

El reglamento de Organización y Funciones del Ministerio de Relaciones Exteriores del Perú, aprobado por Decreto Supremo N° 135-2010-RE, en su artículo 128 designa a la Dirección General de Tratados como: "responsable de dictar las normas y lineamientos técnicos para la adecuada suscripción, perfeccionamiento interno y registro de los tratados y demás instrumentos internacionales que suscriba el Estado peruano" (MRE, 2010). De igual forma, el artículo 128 del mismo D.S. establece 16 funciones específicas a la DGT para lograr los objetivos encomendados.

Gamero detalla la labor más compleja que debe realizar el Ministerio de Relaciones Exteriores durante el proceso:

> El Ministerio de Relaciones Exteriores lleva adelante este procedimiento. La labor principal y la más compleja consiste en la calificación del tratado, que consiste en la determinación de la vía que debe seguirse, vale decir, si el tratado requiere o no la aprobación previa del Congreso. Para esta tarea resulta indispensable contar las opiniones técnicas favorables de las entidades del Sector Público concernidas en la temática del instrumento internacional (Gamero, 2012).

La ratificación de un tratado

Organización de las Naciones Unidas, en base a los artículos 2.1.b, 14.1 y 16 de la Convención de Viena sobre el Derecho de los Tratados de 1969, define un concepto de ratificación de tratados desde una perspectiva general y para los casos de tratados bilaterales y multilaterales:

> La "ratificación" designa el acto internacional mediante el cual un Estado indica su consentimiento en obligarse por un tratado, siempre que las partes la hayan acordado como la manera de expresar su consentimiento. En el caso de tratados bilaterales, la ratificación se

> efectúa por lo general mediante el canje de los instrumentos requeridos. En el caso de tratados multilaterales, el procedimiento normal consiste en que el depositario recoja las ratificaciones de todos los Estados y mantenga a todas las partes al corriente de la situación. La necesidad de firma sujeta a ratificación concede a los Estados el tiempo necesario para lograr la aprobación del tratado en el plano nacional, y para adoptar la legislación necesaria para la aplicación interna del tratado (ONU, 2018).

Las reservas a un tratado

La Convención de Viena sobre el Derecho de los Tratados de 1969 define el término “reserva” en un tratado internacional:

> (…) una declaración unilateral, cualquiera que sea su enunciado o denominación, hecha por un Estado al firmar, ratificar, aceptar o aprobar un tratado o al adherirse a él, con objeto de excluir o modificar los efectos jurídicos de ciertas disposiciones del tratado en su aplicación a ese Estado (ONU, 1969, p. 3).

Garnica cita a Polakiewicz, quien considera que las reservas buscan:

> Facilitar la participación de más partes en los tratados internacionales. (…) al hacer una reserva se excluyen o modifican términos del tratado o el efecto legal de algunas cláusulas en cuanto a su aplicación en sus respectivos países u organizaciones. En muchos casos el estado que se reserva busca limitar sus obligaciones conforme al tratado (Garnica, 2011, p. 2).

En base a la definición y el aporte de Polakiewicz, se establece que las reservas son un medio de facilitación para la futura adhesión de un Estado al tratado, entendiendo que existirán restricciones que el mismo instrumento definirá en su texto.

Las declaraciones a un tratado

A diferencia de las reservas, las declaraciones no están reguladas por el Convención de Viena sobre el Derecho de los Tratados de 1969. Según Novak y García-Corrochano: las declaraciones son manifestaciones de los Estados por las cuales asumen obligaciones sin recibir nada a cambio (Novak, García-Corrochano, 2016, p. 240).

Bajo esta definición, podemos entender que una reserva es una declaración unilateral, pero una declaración no es una reserva, ya que no limita sus obligaciones convencionales.

Un concepto complementario a considerar es el de "declaración interpretativa", el cual es definida por la Comisión de Derecho Internacional en su anuario de 1999, como:

> (…) Una declaración unilateral, cualquiera que sea su enunciado o denominación, hecha por un Estado o por una organización internacional con el objeto de precisar o aclarar el sentido o el alcance que ese Estado o esa organización internacional atribuye al tratado o a algunas de sus disposiciones (CDI, 1999, p. 98).

Las declaraciones interpretativas pueden establecerse por los sujetos de Derecho Internacional de manera indiferente si existe o no una restricción para hacer reservas al momento de adherirse a un tratado. Aunque usualmente se dan ante la restricción de reservas como forma de expresar el sentir de una Parte, según la CCI también pueden darse declaraciones que tienen por objeto cumplir una obligación por medios equivalentes:

> Una declaración unilateral formulada por un Estado o por una organización internacional en el momento en que ese Estado o esa organización expresa su consentimiento en obligarse por un tratado, con el objeto de cumplir una obligación prevista en el tratado de una

manera diferente pero equivalente a la impuesta por el tratado, constituye una reserva (CDI, 1999, p. 98).

1.2. Principales casos de ciberdelincuencia a nivel internacional

Desde la masificación del internet a inicios de la década de los 90, la cantidad de ciberdelitos ha crecido, no sólo numéricamente, sino también por el daño degenerado por los mismos. Estos ocurren en diferentes partes del mundo y abarcan diferentes sectores, tanto públicos como privados, tal como se menciona en la introducción como producto de una sociedad globalizada en la que los instrumentos tecnológicos son más frecuentes en su uso y han cambiado diversos conceptos, que se ven reflejados en comunicación en tiempo real sin importar dónde se está ubicado físicamente.

En ese sentido, se estima que es importante que la presente sección de a conocer algunos casos importantes de ciberdelincuencia que tuvieron repercusión a nivel internacional.

1. **El hackeo y robo a cuentas del Banco de San Francisco en Estados Unidos (1994)**

Uno de los casos más importantes a inicios de la nueva era virtual del ciberdelito fue el hackeo del Banco de San Francisco en 1994 por parte de un joven programador de computadoras en San Petersburgo-Rusia. El caso sale a la luz cuando varios clientes corporativos del banco se percataron que un total de 400 000 USD no se encontraban en sus cuentas. Tras solicitar ayuda al FBI, se detectó transferencias al extranjero de más de 10 millones USD provenientes de las cuentas antes mencionadas. Después de capturar a los dueños de las cuentas se identificó al líder de la banda delictiva y mediante la cooperación entre Estados Unidos y Rusia se procedió a recopilar las pruebas necesarias y a su captura vía extradición desde Reino Unido. Cabe resaltar

que no todo el dinero fue recuperado, generando daños financieros al banco y sus aseguradoras (FBI, 2014).

2. **Un billón de cuentas robadas de Yahoo (2013)**

En el año 2013 se sustrajo información relacionada a nombres, números de teléfono, claves y direcciones de email de un billón de usuario de Yahoo. tres años después, en 2016, hackers volverían a comprometer las cuentas de aproximadamente 500 millones de usuarios. En ambos casos según lo declarado por Yahoo, no se llegaron a sustraer detalles bancarios de sus usuarios, pero la imagen del proveedor de servicios en Internet recibió un gran daño (The Sun, 2017).

3. **El Robo de 100 terabytes de data sensible a Sony Pictures (2014)**

Poco antes de estrenar la película “La Entrevista” en la que se hacía una parodia sobre un futuro intento de asesinato del presidente norcoreano Kim Jong-un, el grupo de ciberdelincuentes Guardianes de la Paz robaron 100 terabytes de data sensible de la compañía. Agencias del gobierno de Estados Unidos aseguran que Corea del Norte autorizó el ciberataque para prevenir que la película fuese proyectada en cines. (The Sun, 2017)

4. **JP Morgan Chase & Co blanco de un conglomerado de hackers (2015)**

Un trío de hackers que se cree operaron desde Israel durante casi una década, robaron en el año 2015 datos personales de empresas y del principal banco de Estados Unidos, JP Morgan Chase & Co. Según declaraciones de los hackers en mención, se considera dicho robo como uno de los mayores robos financieros de la historia. El grupo sustrajo información de ochenta y tres millones de clientes del banco, y reportes de rendimiento con los que

manipularon los precios de acciones para generar ganancias y lavar el dinero transformándolas en Bitcoins que transfirieron a 75 cuentas en diferentes partes del mundo (The Sun, 2017).

5. **El Servicio Nacional de Salud de Reino Unido es hackeado utilizando el virus WannaCry (2015)**

A mediados del 2017 las computadoras del Servicio Nacional de Salud fueron infectadas con el virus WannaCry -vía un archivo adjunto enviado por correo electrónico- y completamente deshabilitadas por una semana, forzando a los hospitales y médicos a trabajar desconectados del sistema, y mostrando uno de los mayores huecos de ciberseguridad del sistema de salud de Reino Unido. El Servicio Nacional de Salud identificó 6 912 computadoras infectadas, aunque se estima que realmente fueron 19 000 aproximadamente. El monto demandado por los hackers para el rescate de cada computadora era de £230 (US$300). El daño no fue solo económico por los recursos inmovilizados, si no también afectó la salud de las personas. Se calcula que 139 personas potencialmente con cáncer no pudieron ser atendidos y no se tiene registro de todas las atenciones canceladas en esas fechas (BBC, 2017).

6. **El Robo a un reconocido banco en Colombia (2017)**

Un reconocido banco (la fiscalía no brindó el nombre del mismo por temas de imagen) sufrió en marzo de 2017 el robo de 700 millones de dólares americanos por medio de varias maniobras fraudulentas. Un grupo criminal utilizó un dispositivo USB con un malware para infectar los sistemas de la entidad bancaria y así vulnerar su seguridad informática. Gracias a esto se realizaron transacciones y desvíos de dinero a veinticuatro cuentas del banco. La investigación del caso por parte de la Fiscalía General de la Nación tomó aproximadamente seis meses y se pudo identificar la estructura de la organización criminal y se capturó a veintidós personas, entre los que se

encontraba una administradora de una sucursal del banco afectado. En este caso se logró una captura gracias a que el caso y los delincuentes se encontraban en el mismo territorio y el Estado podía tomar medidas penales contra los mismos (Kienyke, 2017).

7. Bancos peruanos asumirán pérdidas de clientes ante ciberataques (2018)

El 17 de agosto de 2018 a las 3:00 a. m. se registró un ciberataque realizado por un grupo de hackers a las principales entidades financieras del Perú. Para cometer el delito hicieron uso de suplantación de usuarios con el uso de los malware Samas y Dark Tequila, con los que penetraron de los sistemas bancarios. Ni bien se descubrió el ataque, se suspendió temporalmente algunos servicios para proteger el dinero de los clientes de los bancos, lo que generó problemas en algunas operaciones con tarjetas y en cajeros automáticos. En la noche del mismo día, la Asociación de Bancos del Perú informó que los intentos fueron repelidos con éxito, pero se reconoce que debió ocurrir robos a algunas cuentas, pérdidas que serán asumidas por los bancos (RPP, 2018).

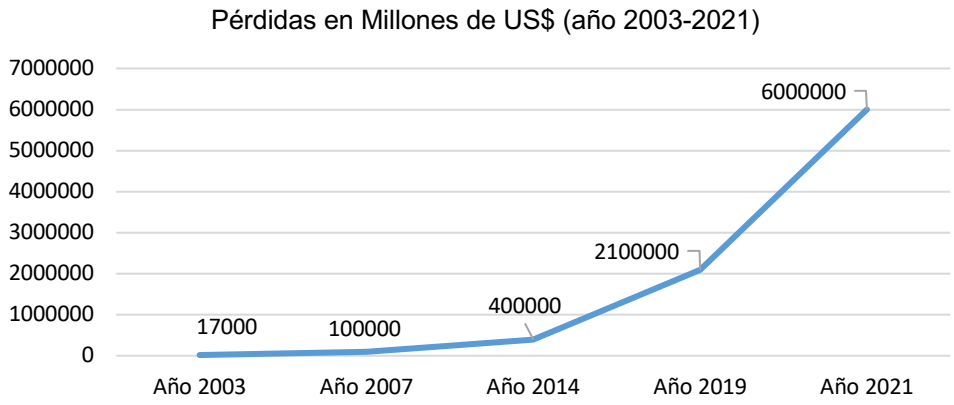
1.3. Pérdidas económicas generadas por la ciberdelincuencia

La ciberdelincuencia ha generado grandes pérdidas a nivel global, lo que genera un incremento adicional en seguridad de la información para tratar de impedir nuevos casos. Un factor importante a considerar es la falta de cultura para comunicar ciberdelitos ocurridos, llevando a la creación de estadísticas presentadas en informes que no son una imagen 100% real de todas las pérdidas para las personas, empresas e instituciones.

1.3.1. Las pérdidas generadas alrededor del mundo

El informe de la ITU del año 2014 ofreció datos estadísticos sobre las pérdidas financieros estimadas causadas por la ciberdelincuencia en todo el mundo. Solo durante el 2003 se registraron pérdidas por 17 000 millones USD, monto que aumentó en más de 400% llegando a 100 000 millones USD en 2007, mantuvo el crecimiento cuadruplicando los resultados previos hasta 400 000 millones USD en el año 2014 y se proyecta para el año 2019 pérdidas por 2 100 000 millones USD (Morgan, 2016a) y para 2021, perjuicios por 6 000 000 millones USD (Morgan, 2016b, p. 3).

Gráfico Nº 2: Pérdidas en Millones de USD, periodo 2003-2021



Fuente: ITU
Elaboración: Propia

Morgan en el Reporte de Ciberdelincuencia (Cybercrime Report) 2017 de Cybersecurity Ventures brinda datos sobre los costos relacionados a los ciberdelitos:

> Los costos de los ciberdelitos incluyen daño y destrucción de datos, dinero robado, pérdida de productividad, robo de propiedad intelectual, robo de datos personales y financieros, malversación de fondos, fraude, interrupción posterior al ataque en el curso normal de los negocios, investigación forense, restauración y eliminación de datos y sistemas intervenidos, y daño de reputación. (…) Los ciberdelitos están

> creando un daño sin precedentes a ambas, empresas privadas y públicas. (…) El gasto mundial de seguridad de la información crecerá 7% hasta llegar a los 86 400 millones USD en 2017 y subirá hasta 93 000 millones en 2018 (Morgan, 2017 p. 3-6).

1.3.2. Las pérdidas generadas en la región latinoamericana

Según declaraciones de Moreno, presidente del BID, en el informe de Ciberseguridad 2016 de la OEA y el BID, los daños por la ciberdelincuencia (mencionado en su declaración como cibercrimen) en el año 2016 son mayores a los ingresos por donaciones para el desarrollo internacional y que el dinero perdido podría ser utilizado en otras actividades de utilidad para la región:

> Según algunos cálculos, el cibercrimen le cuesta al mundo hasta US$575 000 millones al año, lo que representa 0,5% del PIB global. Eso es casi cuatro veces más que el monto anual de las donaciones para el desarrollo internacional. En América Latina y el Caribe, este tipo de delitos nos cuestan alrededor de US$90 000 millones al año. Con esos recursos podríamos cuadruplicar el número de investigadores científicos en nuestra región (BID, 2016 p. IX).

La consultora Deloitte en su encuesta 2016 sobre Tendencias de Cyber Riesgos y Seguridad de la Información en Latinoamérica informó que 4 de cada 10 organizaciones sufrieron una brecha de seguridad en los últimos 24 meses y menos del 20% de las mismas cuentan con un centro de operaciones de seguridad (Deloitte, 2016, p. 4). Dentro de ese grupo se encuentran las entidades financieras, las cuales, según cifras conservadoras, sitúan en casi mil millones de dólares americanos anuales las pérdidas de dicho sector por deficiencias relacionadas con la ciberseguridad. Sin embargo, en muchos países de la región, el concepto de ciberdelincuencia y su combate siguen estando ausentes de las normativas nacionales, lo que dificulta un marco legal para su erradicación (Trettenero, 2017).

Los ciberdelincuentes ven a Latinoamérica como un lugar para realizar sus delitos con menor riesgo a ser descubiertos o que se pueda hacer algo en su contra debido a la ineficiencia del marco legal de varios países de la región. El tema fue tratado en el Evento CI@b 2017 que reúne a los principales bancos de la región y una de las exposiciones detalla ese problema:

> Estos delincuentes han ampliado el negocio a América Latina porque ven que las infraestructuras son deficientes o inexistentes y las entidades normalmente actúan de manera reactiva, con lo cual los esfuerzos preventivos son escasos. Además, existe una gran capacidad de inventiva y creatividad (en el sentido negativo) que provoca mucho daño al cliente de banca", explica un experto de una firma de investigación (Trettenero, 2017).

1.3.3. Las pérdidas generadas en el Perú

Para el cierre del año 2017 se proyectó pérdidas generadas por 4 782 millones de dólares americanos, siendo el séptimo país de la región más afectado por la ciberdelincuencia (Gestión, 2017). Los principales delitos se realizan aprovechando las brechas existentes en varios sectores, la falta de medidas e inversión en seguridad y la falta de cultura de seguridad por las mismas instituciones, colaboradores y población en general.

El dato proyectado no refleja la realidad de los daños generados en el país, muchos de los afectados no comunican el hecho para su respectivo registro oficial y no se pueden elaborar estadísticas más fidedignas y tener una visión más realista del contexto en el que vive el Perú.

2. EL CONVENIO DE BUDAPEST SOBRE LA CIBERDELINCUENCIA

El segundo capítulo de la tesis tiene como principales objetivos, haciendo uso de los conceptos presentados en el capítulo anterior, el describir y analizar el Convenio de Budapest sobre la Ciberdelincuencia, para así dar a conocer los elementos de importancia que servirán de apoyo a los Estados miembros del Convenio; y presentar los avances hasta la fecha de otros Estados de América Latina y el Caribe, los cuales están en la misma región del Estado peruano.

Este capítulo estará dividido en dos partes. La primera correspondiente al Convenio de Budapest sobre la Ciberdelincuencia, en la que se analizará el instrumento y sus cuarenta y ocho artículos, dando énfasis en los nueve delitos presentados en la sección de Derecho Penal Sustantivo del Convenio; una breve descripción de Estados Parte, resaltando la participación de Estados de la región; y un análisis de las reservas y/o declaraciones presentadas por cada Estado al momento del depósito del instrumento de aprobación, ratificación o adhesión.

Finalmente, la segunda parte del capítulo tratará los avances de la región de América Latina y el Caribe en materia legislativa, y en su proceso adhesión al Convenio de Budapest sobre la Ciberdelincuencia, presentando la situación actual de los países vecinos del Perú.

2.1. El Convenio de Budapest sobre la Ciberdelincuencia

El Convenio de Budapest sobre la Ciberdelincuencia es un tratado multilateral de naturaleza jurídica derivada del Derecho Internacional, el cual permite a los Estados Partes a obligarse al mismo vía el consentimiento para el logro de un objetivo específico.

Es considerado el primer tratado internacional sobre delitos cometidos a través de internet y otros sistemas informáticos, el cual busca brindar herramientas de derecho penal sustantivo y procesal, así como mejorar capacidades de cada Estado Parte mediante cooperación internacional en tiempo real para la lucha contra la ciberdelincuencia.

La adhesión al Convenio no generará mayor costo a los Estados Parte fuera de la adecuación de la legislación interna de ser necesario y los trámites a seguir según procedimientos del Convenio, pero a cambio, como se mencionó en el párrafo anterior, contarán con una herramienta para combatir delitos cometidos con el uso de dispositivos informáticos. La entrada en vigor para los Estados Parte se realizará según lo establecido por el instrumento.

En relación a la cooperación internacional, los Estados decidirán los recursos a destinar para la lucha contra la ciberdelincuencia en base a sus posibilidades y de igual manera podrán aprovechar las modalidades de cooperación disponibles dentro del Convenio.

2.1.1. El contexto para su creación

La difusión masiva del Internet, y la aparición de dispositivos electrónicos y sistemas operativos pensados para todo público a inicios de la década de los noventa permitieron a las poblaciones de todo el mundo el conocer y explotar un nuevo mundo de posibilidades. Esto vino acompañado de un rápido desarrollo en el campo de las tecnologías de la información y comunicación que cada día estaban introduciéndose en todos los sectores de la sociedad moderna generando cambios importantes en la economía y la sociedad, y creando mayor dependencia a sus usuarios por la velocidad, facilidades y otros beneficios que las mismas brindaban.

El internet y el ciberespacio lograron interconectar países, sus poblaciones, dispositivos y sistemas; lo que permitió tener realmente un mundo globalizado. Las nuevas tecnologías traspasaron las fronteras y el tiempo, haciendo innecesario estar en una ubicación geográfica específica, el esperar horas o días para hacer operaciones comerciales o enterarse de eventos en el mundo. La comunicación también se había vuelto instantánea, y la noción de horarios y tiempo desaparecía en el nuevo entorno del ciberespacio.

En este nuevo contexto, cualquier persona con un dispositivo adecuado y conexión a Internet era capaz de tener acceso a servicios en el ciberespacio o a redes privadas o públicas alrededor del mundo sin importar desde qué punto del planeta se encuentre. Por un lado, esta situación rompía los conceptos de fronteras para dar libertad a la población mundial, pero, por otro lado, generaba una incertidumbre por el mal uso de las nuevas herramientas disponibles en el ciberespacio, la cual no podía ser controlada con facilidad debido a la nueva naturaleza transfronteriza que adquirían las redes de la información (COE, 2001b, p. 1).

La aparición de virus alrededor del mundo y la evolución de la comisión de delitos tradicionales que incrementaban su alcance de daño mediante el uso de nuevas tecnologías, fueron nuevos retos que los Estados empezaron a tomar con mayor preocupación. Los delincuentes ya no debían estar en el Estado donde se realizaban los delitos, es por eso que era necesario crear instrumentos jurídicos internacionales que ayuden a afrontar este nuevo desafío, sobre todo para el bienestar y protección de las poblaciones y sus derechos humanos en la nueva era de la Sociedad de la Información, la cual hace uso intensivo de la tecnología y comunicación para el desarrollo de las personas.

2.1.2. Antecedentes del Convenio

En noviembre de 1996 el Comité de Europeo para los Problemas Criminales (CDPC) vía decisión número CDPC/103/211196 establece un “Comité de Expertos Encargados de Delitos Informáticos” para examinar revisar las recomendaciones 89 y 95 sobre procedimiento penal vinculado a la tecnología de la información y elaborar un borrador de instrumento jurídicamente vinculante.

El 4 de febrero de 1997 mediante decisión número CM/Del/Dec(97)583 se establece en el Consejo de Europa el “Comité de Expertos en la Delincuencia en el Ciberespacio (PC-CY)” para elaborar un instrumento jurídicamente vinculante que trate el problema de los delitos cometidos por medios electrónicos.

El nuevo comité se encargó de elaborar un borrador del instrumento entre abril de 1997 y diciembre del año 2000 con recomendaciones de expertos y la participación de Estados miembros y no miembros del Consejo de Europa. En

abril del 2000 se desclasificó y publicó el proyecto de Convenio que seguiría siendo modificado en los siguientes meses.

En la sesión plenaria 50 del CDPC de junio de 2001 se aprobó el proyecto de Convenio y en la sesión 109 del Consejo de Europa de noviembre de 2001 se aprobó el tratado No. 185 del Consejo de Europa o Convenio de Budapest sobre la Ciberdelincuencia. A partir de ese momento el instrumento quedaba abierto para la firma de los Estados que participaron en su elaboración.

Casi tres años después, con la expresión de consentimiento y entrega de los instrumentos de ratificación, aceptación o aprobación depositados en poder del Secretario General (artículo 36.2) de por lo menos cinco Estados, los cuales deben incluir a tres estados miembros del Consejo de Europa (Albania, Croacia, Estonia, Hungría y Lituania) para su entrada en vigencia; y habiendo expirado el plazo estipulado de tres meses de la expresión del consentimiento de los Estados para quedar vinculados por el Convenio (artículo 36.3); entra en vigor a nivel internacional el 1 de julio de 2004 el Convenio de Budapest sobre la Ciberdelincuencia.

Con este acto, el Convenio mencionado previamente pasa a ser el primer tratado internacional sobre delitos cometidos a través de internet y otras redes informáticas relacionados a derechos de autor, fraude informático, pornografía infantil y violaciones de seguridad en la red. Mientras brinda herramientas de derecho y cooperación judicial a las partes para la protección de sus poblaciones en relación a los ciberdelitos.

2.1.3. Los objetivos del Convenio

El principal objetivo del Convenio de Budapest sobre la Ciberdelincuencia es: aplicar una política penal común con objeto de proteger a la sociedad frente a la ciberdelincuencia, en particular mediante la adopción de una legislación adecuada y la mejora de la cooperación internacional (COE, 2001a, p.1).

Con el logro del objetivo, se busca incrementar las capacidades y eficiencia en la investigación, persecución y proceso penal; así como permitir la obtención de pruebas electrónicas de los delitos cometidos para los Estados Parte mediante la cooperación internacional en tiempo real.

2.1.4. La estructura del Convenio

El Convenio contiene un Preámbulo y un total de cuarenta y ocho artículos distribuidos en cuatro capítulos:

- Capítulo I: Terminología,
- Capítulo II: Medidas que deben adoptarse a nivel nacional,
- Capítulo III: Cooperación Internacional y
- Capítulo IV: Cláusulas finales, con sus correspondientes secciones y títulos.

Posteriormente, el 28 de enero de 2003, se adicionó un Prólogo que entraba en vigor el 1 de marzo de 2006, donde se penalizaba los actos racistas y xenófobos cometidos mediante medios informáticos. Dicho Prólogo no se considera para que los Estados puedan realizar los procedimientos de adhesión o ratificación del Convenio.

2.2. El análisis del Convenio

Para el presente análisis se hará uso del Convenio de Budapest sobre la Ciberdelincuencia como base, dando énfasis en los delitos informáticos dentro de la sección de Derecho Penal Sustantivo, en los que se dará una explicación de la naturaleza de los mismos, los elementos que se consideraron en su elaboración y algunos casos a modo de ejemplo para ver la propicia aplicación o no aplicación de los mismos artículos por parte de los Estados Parte del Convenio.

Preámbulo

En el Preámbulo se reconoce el interés de intensificar la cooperación entre los Estados Parte del Convenio (párr. 3); la necesidad de aplicar una política penal común para proteger a la sociedad frente a la ciberdelincuencia, adoptando una legislación adecuada, y mejorando la cooperación internacional en términos de reforzamiento y velocidad (párr. 4 y 8); y la necesidad de cooperación entre los Estados y el sector privado, así como proteger los intereses en la utilización y desarrollo de las tecnologías de la información (párr. 7).

Menciona la importancia del Convenio para prevenir actos delictivos que pongan en peligro la confidencialidad, integridad, y disponibilidad de los sistemas y datos informáticos; dar poderes para luchar contra los mismos a nivel nacional e internacional; y brindar disposiciones que permitan una cooperación internacional rápida y fiable (párr. 9).

También presenta la necesidad de garantizar el debido equilibrio entre los intereses de acción penal y el respeto por los derechos humanos fundamentales consagrados en diferentes tratados internacionales en el marco del Consejo de Europa y la Organización de Naciones Unidas; y

completar con el Convenio de Budapest otros convenios internacionales relacionados a la protección de datos personales, derechos del niño o cooperación en materia penal (párr. 10 al 13).

Finalmente, busca recordar las iniciativas para mejorar el entendimiento y cooperación internacional de las Naciones Unidas, la OCDE, Unión Europea, el G8 sobre la materia; las recomendaciones el Comité de Ministros de Justicia europeos; y el tener en cuenta el plan de acción adoptado por los Jefes de Estado y de Gobierno del Consejo de Europa para encontrar respuestas comunes ante el desarrollo de nuevas TICs (párr. 14 al 17).

Capítulo I – Terminología

El objetivo del primer capítulo es dar a conocer conceptos que los Estados Parte deberán considerar para implementar en su derecho interno. Esto va de la mano con el espíritu del Convenio de buscar un marco legal común, pero no necesariamente igual para todos los casos, debido a las particularidades de cada Estado.

El capítulo I cuenta con un único artículo sobre definiciones, cuatro incisos y dos sub incisos correspondientes al inciso “c”.

Artículo 1 – Definiciones. Brinda conceptos de “sistema informático” (inciso a); “datos informáticos” (inciso b); “proveedor de servicios” (inciso c, sub incisos i. y ii.); y “datos relativos al tráfico” (inciso d).

Capítulo II – Medidas que deberán adoptarse a nivel nacional

El objetivo del segundo capítulo es desarrollar normas de derecho sustantivo relacionado a los delitos realizados mediante o con el uso de sistemas informáticos, los cuales están relacionados a los actos de piratería o robo de

datos confidenciales, fraude, falsificación de información, alteración, destrucción, pornografía infantil, propiedad intelectual, entre otros. De igual manera trata normas de derecho procesal y la jurisdicción correspondiente.

El capítulo II cuenta con tres secciones que tratan temas de: Derecho penal sustantivo, con cinco títulos que agrupan los artículos 2 al 13; Derecho procesal, también con cinco títulos que agrupan los artículos 14 al 21; y Jurisdicción con el artículo 22.

Sección 1 – Derecho penal sustantivo

Esta sección cuenta con cinco títulos y trece artículos, los cuales tienen como finalidad lograr que los Estados Parte establezcan normas mínimas comunes en su derecho interno para nueve delitos deliberados e ilegítimos contenidos en los primeros cuatro títulos de la sección; y adoptar medidas necesarias para garantizar la exigencia de responsabilidades y sanciones, como se menciona en el quinto título de la misma sección.

Se hará un análisis de los nueve delitos informáticos a tipificar por cada Estado Parte en su derecho interno, los cuales se encuentran agrupados en los cuatro títulos de esta sección.

Título 1 – Delitos contra la confidencialidad, la integridad y la disponibilidad de datos y sistemas informáticos

Los artículos del primer título hacen referencia delitos penales, diferenciándolos de actividades comerciales o de seguridad trabajadas por entidades públicas o privadas.

Artículo 2 - Acceso ilícito

> Cada parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno el acceso deliberado e ilegítimo a todo o parte de un sistema informático. Las Partes podrán exigir que el delito se cometa infringiendo delictiva, o en relación con un sistema informático conectado a otro sistema informático.

Cabe resaltar que no se puede considerar como ilegítimos para la obtención de datos el uso de cookies en sitios web, los programas de recolección de datos de anónimos o de experiencia de usuario, debido a que son anunciados al momento del primer uso de las mismas; y sirven para beneficio del usuario y editor al brindar información, mejorando la experiencia de navegación y edición o publicación de contenidos.

De igual manera, el acceso a todo o parte de un sistema sin intención delictiva es una práctica común en varios países para encontrar errores o deficiencias de programación y mejorar el producto final. Empresas que desarrollan software como Google o Apple premian a las personas o empresas que ayudan a mejorar las medidas de seguridad de sus aplicaciones (Applesfera, 2016).

Otro ejemplo es el de Google con su programa de seguridad Project Zero sin costo para terceros, con el cual buscan errores de programación de sistemas operativos de otras empresas donde ellos publican su software para advertirles y solicitar que corrijan el mismo vía parches (Google, s.f.).

Artículo 3 - Interceptación ilícita:

> Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno la interceptación deliberada e ilegítima por medios de técnicos de datos informáticos en transmisiones no públicas dirigidas a un sistema

informático, originadas en un sistema informático o efectuadas dentro del mismo, incluidas las emisiones electromagnéticas provenientes de un sistema informático que transporte dichos elementos informáticos. Las Partes podrán exigir que el delito se cometa con intención delictiva o en su relación con un sistema informático conectado a otro sistema informático.

Las interceptaciones en transmisiones no públicas no deberían ser penalizadas si hay una ley interna que lo permita, siempre y cuando estén relacionadas a temas de seguridad nacional.

Artículo 4 - Ataques a la integridad de los datos

1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno todo acto deliberado e ilegitimo que dañe, borre, deteriore, altere o suprima datos informáticos.

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

El artículo busca brindar a los datos informáticos una protección similar a los objetos físicos ante daños que se les pueda generar. La modificación de datos relativos al tráfico para facilitar comunicaciones anónimas o para garantizar la seguridad de las comunicaciones está permitida, a menos que se use para ocultar la identidad del delincuente cuando realiza un acto deliberado e ilegítimo.

Artículo 5 - Ataques a la integridad del sistema

Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno la obstaculización grave, deliberada e ilegítima del funcionamiento de un sistema informático mediante la introducción, transmisión, daño, borrado, deterioro, alteración o supresión de datos informáticos.

Este artículo se desarrolló basándose en la recomendación 89 del procedimiento penal vinculado a la tecnología de la información del Consejo de Europa que define los ataques mencionados como sabotaje informático.

Artículo 6 - Abuso de los dispositivos:

1. 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 ilegítima de los siguientes actos:

   a. La producción, venta, obtención para su utilización, importación, difusión u otra forma de puesta a disposición de:

      i. cualquier dispositivo, incluido un programa informático, concebido o adaptado principalmente para comisión de cualquiera de los delitos previstos en los artículos 2 al 5del presente Convenio;
      ii. una contraseña, código de acceso o datos informáticos similares que permitan acceder a todo o parte de un sistema informático,

      Con la intención de que sean utilizados para cometer cualquiera de los delitos contemplados en los artículos 2 a 5; y

   b. La posesión de alguno de los elementos mencionados previamente para intentar cometer un delito del art. 2 al 5.

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 disposición mencionada en el párrafo 1 del presente artículo no tenga por objeto la comisión de uno de los delitos previstos de conformidad con los artículos 2 a 5 del presente Convenio, como en el caso de las pruebas autorizadas o de la protección de un sistema informático.

3. Las Partes podrán reservarse el derecho a no aplicar el párrafo 1 del presente artículo, siempre que dicha reserva no afecte a la venta, distribución o cualesquiera otras formas de puesta a disposición de los elementos mencionados en el inciso 1 a) ii) del presente artículo.

El artículo trata de resaltar que, sin importar el dispositivo, su diseño, fabricación o uso, lo que genera responsabilidad es el elemento subjetivo (cometer el acto). En caso se trate de dispositivos para comprobar la fiabilidad

de productos de tecnología de la información, el uso de los mismos no genera responsabilidad.

Título 2 – Delitos informáticos

Los artículos del segundo título hacen referencia a los principales delitos cometidos mediante medios informáticos que los Estados deberán adoptar en su legislación tipificándolos en su derecho interno como delitos. Se presentan los delitos de falsificación informática y fraude informático.

Artículo 7 - Falsificación informática

> Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno la introducción, alteración, borrado o supresión deliberada e ilegítima de datos informáticos que genere datos no auténticos con la intención de que sean tomados o utilizados a efectos legales como auténticos, con independencia de que los datos sean legibles o inteligibles directamente. Las Partes podrán exigir que exista una intención dolosa o delictiva similar para que se considere que existe responsabilidad penal.

El fin del séptimo artículo es establecer un delito paralelo que combine la falsificación tradicional de documentos tangibles con medios informáticos para generar la correspondiente responsabilidad penal.

Artículo 8 - Fraude informático

> Las Partes adoptarán las medidas legislativas o de otro tipo que resulten necesarias para tipificar como delito en su derecho interno los actos deliberados e ilegítimos que causen perjuicio patrimonial a otra persona mediante:
>
> a. la introducción, alteración, borrado o supresión de datos informáticos;
> b. cualquier interferencia en el funcionamiento de un sistema informático;

Con la intención, dolosa o delictiva, de obtener de forma ilegítima un beneficio económico para uno mismo o para otra persona.

El artículo busca resaltar la importancia de la manipulación de datos para aprovechar recursos económicos o financieros, el cual ha crecido en los últimos años debido al incremento de interconexión de sistemas y el uso de nuevas tecnologías, las cuales contener tener huecos de seguridad en su programación.

Título 3 – Delitos relacionados con el contenido

El artículo del tercer título hace referencia a los principales delitos relacionados a la pornografía infantil y los actos que generan responsabilidad penal.

Artículo 9 - Delitos relacionados con la pornografía infantil

1. 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 ilegítima de los siguientes actos:
a. la producción de pornografía infantil con la intención de difundirlas a través de un sistema informático;
b. la oferta o la puesta a disposición de pornografía infantil a través de un sistema informático;
c. la difusión o la transmisión de pornografía infantil a través de un sistema informático;
d. la adquisición, para uno mismo o para otros, de pornografía infantil a través de un sistema informático;
e. la posesión de pornografía infantil en un sistema informático o en un dispositivo de almacenamiento de datos informáticos.

2. A los efectos del párrafo 1 anterior, se entenderá por ‹‹pornografía infantil›› todo material pornográfico que contenga la representación visual de:

a. Un menor adoptando un comportamiento sexualmente explícito;
b. Una persona que parezca un menor adoptando un comportamiento sexualmente explícito;

c. Imágenes realistas que representen a un menor adoptando un comportamiento sexualmente explícito.

3. A los efectos del párrafo 2 anterior, se entenderá por ‹‹menor›› toda persona menor de 18 años. Las Partes podrán, no obstante, exigir un límite de edad inferior, que deberá ser como mínimo de 16 años.

4. Las Partes podrán reservarse el derecho a no aplicar, en todo o en parte, los apartados d) y e) del párrafo 1 y los apartados b) y c) del párrafo 2.

El artículo busca reforzar las medidas de protección ante explotación sexual de menores de edad incluyendo el uso de sistemas informáticos en la realización del delito. También con este artículo se evidencia el compromiso adoptado en la Convención de Naciones Unidas sobre los Derechos del Niño e iniciativas europeas.

Finalmente se resalta el hecho que poner material de pornografía infantil a disposición de terceros existiendo o no una compensación económica ya genera responsabilidad penal, y el comportamiento sexualmente explícito que puede ser realizado por un menor de edad o alguien que simule serlo, que puede incluir el mostrar partes o acciones.

Título 4 – Delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines

El único artículo del cuarto título hace referencia a las infracciones de los derechos de propiedad intelectual en base a actas, tratados y convenciones sobre los cuales los Estados ya se encuentran previamente obligados.

Artículo 10 - Delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines

1. Los Estados firmantes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para prever como infracción penal, conforme a su derecho interno, los atentados a la propiedad intelectual definida por la legislación de cada Estado, conforme a las obligaciones que haya asumido por aplicación de la Convención Universal sobre los Derechos de Autor, revisada en París el 24 de julio de 1971, del Convenio de Berna para la protección de obras literarias y artísticas, del Acuerdo sobre los aspectos de los derechos de propiedad intelectual relacionados con el comercio y del Tratado de la OMPI sobre Derecho de Autor, a excepción de cualquier derecho moral conferido por dichas Convenciones, cuando tales actos sean cometidos deliberadamente, a escala comercial y a través de un sistema informático.

2. Los Estados firmantes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para prever como infracción penal, conforme a su derecho interno, los atentados a los derechos afines definidos por la legislación de cada Estado, conforme a las obligaciones que haya asumido por aplicación de la Convención Internacional sobre la Protección de los Artistas Intérpretes o Ejecutantes, los Productores de Fonogramas y los Organismos de Radiodifusión, hecha en Roma (Convención de Roma), del Acuerdo sobre los aspectos de los derechos de propiedad intelectual relacionados con el comercio y del Tratado de la OMPI sobre interpretación o ejecución y fonogramas, a excepción de cualquier derecho moral conferido por dichas Convenciones, cuando tales actos sean cometidos deliberadamente, a escala comercial y a través de un sistema informático.

3. Los Estados podrán, de concurrir determinadas circunstancias, reservarse el derecho de no imponer responsabilidad penal en aplicación de los párrafos 1 y 2 del presente artículo, siempre que se disponga de otros recursos eficaces para su represión y que dicha reserva no comporte infracción de las obligaciones internacionales que incumban al Estado por aplicación de los instrumentos internacionales mencionados en los párrafos 1 y 2 del presente artículo.

Las infracciones a los derechos de propiedad intelectual son algunos de los delitos más comunes cometidos por Internet. Estas están relacionadas a

obras protegidas de autores como libros, contenido audiovisual, data, sistemas informáticos, software, entre otros.

Los Estados Parte deberán tipificar en su derecho interno las infracciones mencionadas en el artículo, pero las sanciones que establezcan las partes podrán diferir ligeramente, ya que el Convenio no limita ese aspecto, entendiendo también que deben estar alineadas a los compromisos internacionales ya adquiridos por los mismos. El artículo hace mención de algunos compromisos como los adquiridos por la Convención Universal sobre los Derechos de Autor, Tratado de la OMPI sobre Derecho de Autor, Convención de Roma, entre otros.

Título 5 – Otras formas de responsabilidad y sanción

Los artículos 11 al 13 que conforman el quinto título buscan que los Estados parte adopten las medidas legislativas y de otro tipo para tipificar como delito en su derecho interno la complicidad deliberada para los delitos previstos en los artículos 2 al 10; y toda tentativa deliberada de cometer alguno de los delitos previstos de los artículos 3, 5, 7, 8 9.1.a) y 9.1.c). En el último caso los Estados Parte podrán hacer reservas en todo o parte del párrafo 2 (art. 11).

Adicionalmente se podrá exigir responsabilidad de las personas jurídicas por los delitos previstos en la Convención por una persona física que ejerce funciones directivas, ya sea por sus actos o por permitir la comisión de un delito; y la imposición de sanciones efectivas, proporcionadas y disuasorias, incluidas penas privativas de libertas para los delitos de los artículos 2 a 11, así como medidas penales o no penales efectivas, incluidas las sanciones pecuniarias.

Para la complicidad deliberada es necesario que exista conocimiento del delito y cómo se llevará a cabo. No se puede relacionar, por ejemplo, con el uso de

proveedores de servicios, por ejemplo, de telefonía móvil, ya que el último no sabía que se realizaría el delito vía su canal de trabajo.

Sobre la tentativa deliberada se puede relacionar al ofrecimiento de software ilegal, pornografía infantil, un futuro acto fraudulento, entre otros. Finalmente, las sanciones pueden variar dependiendo de la gravedad del delito y las normas internas de cada Estado Parte.

Sección 2 – Derecho procesal

Esta sección cuenta con cinco títulos y ocho artículos, los cuales tienen como finalidad lograr que los Estados Parte establezcan medidas procesales para los delitos de la sección 1 u otros delitos delito que se puedan realizar mediante un sistema informático, así como para la obtención de pruebas electrónicas relativas a un delito penal.
Se brindan disposiciones comunes para la adopción de medidas legislativas o de otro tipo para el establecimiento o aplicación de poderes y procedimientos para efectos de investigación o de procedimientos penales específicos para delitos mencionados en los artículos 2 a 11 u otros cometidos por medio de un sistema informático y la obtención de pruebas electrónicas de cualquier delito. Se podrá presentar reservas si se cumplen las condiciones establecidas en el mismo artículo.

De igual manera la instauración, ejecución y aplicación de los poderes y procedimientos mencionados previamente deben someterse a las salvaguardias previstas en el derecho interno de cada Parte, garantizando la protección adecuada de los derechos humanos y de las libertades asumidas en diferentes instrumentos internacionales por cada Parte, incluyendo una supervisión judicial u otra forma de supervisión independiente.

El Convenio también establece las medidas para conservación total o parcial rápida de datos electrónicos y datos de tráfico almacenados por medio de un sistema informático cuando se crea que podrían ser susceptibles de pérdida o modificación. Estas medidas buscan obligar a conservar y proteger los datos durante el tiempo necesario, hasta un máximo de 90 días para que las autoridades competentes puedan obtener su revelación, lo que ayudará a identificar a los proveedores de servicios, así como la vía por la que se transmitió la comunicación relacionada al delito.

Los proveedores de servicios, los cuales pueden ser de hospedaje o de Internet tienen políticas de conservación de datos (usualmente 30 días), con este artículo, el plazo se podrá ampliar a un triple de ese periodo tanto para ellos, como a terceros encargados de la conservación de los datos solicitados. Adicionalmente, se les podrá obligar a mantener en secreto la ejecución de los procedimientos según el derecho interno de cada Estado.

Las medidas de los artículos del título 2 solo aplican a datos informáticos ya existentes y almacenados, de tratarse de datos futuros, deberá aplicarse las medidas del título 5 del capítulo II; y se utiliza la palabra conservación y no retención, porque el primero se entiende por almacenaje de manera segura.

Las partes deben facultar a sus autoridades competentes para ordenar la comunicación de determinados datos informáticos bajo poder o control de una persona o un proveedor. De igual manera se les debe dar facilidades para confiscar, realizar y conservar copias, preservar integridad de los datos almacenados y hacer inaccesibles o suprimir los datos informáticos del sistema informático consultado.

Asimismo, en los artículos del título 5, se dan los lineamientos que las Partes deben seguir para la obtención en tiempo real de datos relativos al tráfico y la interceptación de datos relativos al contenido.

Capítulo III – Cooperación Internacional

El objetivo del tercer capítulo es establecer disposiciones para facilitar y estandarizar las acciones relacionadas a la cooperación internacional entre los Estados Parte del Convenio. Estas acciones incluyen la extradición; la conservación rápida, acceso, obtención e interceptación de datos informáticos almacenados, así como el asegurar medidas para una asistencia inmediata en cualquier momento.

El capítulo III cuenta con dos secciones, la primera sobre Principios Generales con cuatro títulos que agrupan los artículos 23 al 28; y Disposiciones Específicas con tres títulos que agrupan los artículos 19 al 35.

Sección 1 – Principios generales

La primera sección del capítulo III presenta los principios generales relativos a la cooperación internacional, la extradición, la asistencia mutua y los procedimientos a seguir por los Estados Parte para la asistencia mutua en caso de ausencia de acuerdos internacionales aplicables.

Se establece que los Estados Parte deben cooperar entre sí en las investigaciones o procedimientos relativos a los delitos presentados en el Convenio.

En relación a la extradición, podrá aplicarse cuando se cometa por lo menos uno de los delitos de los artículos 2 al 11, siempre y cuando las legislaciones de ambos Estados Parte castiguen el delito con un plazo no menor de un año o como establezca un tratado previo entre las Partes. Para una correcta labor, será necesario notificar el nombre y dirección de la autoridad responsable del envío o recepción de demandas de extradición. Para casos particulares se puede denegar la extradición según lo estipulado por el Convenio.

Se regularán las disposiciones que rigen la asistencia mutua entre los Estados Parte en relación a los delitos señalados en el Convenio. Las Partes deben prestar toda la ayuda mutua posible después de recibir por canal convencional o por medio rápido en caso de urgencia para obtener pruebas en formato electrónico de un delito. Se podrá exigir la existencia de doble tipificación penal para condicionar la asistencia mutua.

En base al derecho interno de cada Estado Parte, se podrá comunicar información obtenida de propias investigaciones a otra Parte. Dicha información puede ser solicitada que sea trabajada de manera confidencial o bajo ciertas condiciones.

En los casos de ausencia de acuerdos internacionales aplicables, se aplicarán las disposiciones que el artículo 27 establece. En caso exista algún tratado previo, si las Partes están de acuerdo, podrán decidir aplicar parte o la totalidad de las disposiciones previstas por el mencionado artículo.

Ante la ausencia de un tratado previo, para los casos de solicitudes de confidencialidad y restricciones de uso, se aplicarán las disposiciones que el artículo 28 establece.

Sección 2 – Disposiciones específicas

La segunda sección del capítulo III establece las previsiones específicas sobre modalidades que los Estados Parte pueden adoptar para la asistencia mutua y la designación de un grupo para garantizar la asistencia inmediata en la investigación de los delitos

Las medidas previsionales en materia de conservación y revelación rápida de datos informáticos almacenados, la facultad de reservarse el derecho a denegar la solicitud por exigencia de doble tipificación, y la denegación de

revelación rápida en casos específicos, se encuentran detalladas en los artículos 29 y 30 para ser aplicados por los Estados Parte.

De igual manera, en los capítulos contenidos en el título 2 de la sección 2 del capítulo, se contemplan las acciones y procedimientos a tomar para la asistencia mutua en relación con el acceso a datos almacenados; el acceso transfronterizo a datos almacenados, con consentimiento o cuando sean accesibles al público; la asistencia mutua para la obtención en tiempo real de datos relativos al tráfico; y la asistencia mutua en relación con la interceptación de datos relativos al contenido.

Finalmente se establece que cada Estado Parte debe designar un grupo formado y equipado de contacto localizable las 24 horas del día, los 7 días de la semana, para garantizar asistencia inmediata en la investigación de los delitos mencionados en el Convenio. La asistencia se realizará mediante asesoría técnica, conservación de datos, obtención de pruebas, y de suministro de información de carácter jurídico y localización de sospechosos.

Capítulo IV – Cláusulas finales

El presente capítulo se encuentra conformado por los artículos 36 al 48 y brinda los detalles para la firma y entrada en vigor del Convenio; el procedimiento para la adhesión de terceros Estados; la aplicación territorial; los efectos del Convenio; las indicaciones para las declaraciones y reservas; las enmiendas, la solución de controversias; las consultas entre las partes; las denuncias; las notificaciones; y otros detalles o forma de aplicación.

Se menciona que el Convenio está abierto a firma, ratificación, aceptación o aprobación de los Estados miembros y no miembros del Consejo de Europa que participaron en su elaboración. El mismo entrará en vigor el primer día del mes siguiente a la expiración de un plazo de tres meses desde la fecha en

que cinco Estados, de los cuales por lo menos tres deben ser del Consejo de Europa, expresen su consentimiento para quedar vinculados por el Convenio. Para los demás Estados signatarios que expresen ulteriormente su consentimiento para quedar vinculados por el Convenio, la entrada en vigor será el mismo plazo contado desde la expresión del consentimiento (art. 36).

El Convenio está abierto a futuras adhesiones por parte de Estados que no participaron en su elaboración, vía invitación del Comité de Ministros del Consejo de Europa y previo consentimiento unánime de los Estados contratantes del Convenio. El plazo de entrada en vigor para estos casos será el mismo del de los miembros que participaron en su elaboración, con la diferencia que se contará desde el momento del depósito del instrumento de adhesión al Secretario General del Consejo de Europa (art. 37). Este último artículo da pie a una mejor cooperación internacional como se menciona en el preámbulo del Convenio, haciendo que se respeten las restricciones que el mismo impone para que los Estados Parte puedan analizar si las solicitudes de adhesión son propicias o no.

Al momento del depósito del instrumento de ratificación, aceptación o adhesión, los Estados podrán designar los territorios donde aplicará el Convenio. Si desean hacer extensivo la aplicación a nuevos territorios propios, deberán enviar una declaración dirigida al Secretario General del Consejo de Europa. El plazo de entrada en vigor será el mismo al del consentimiento original contado desde la fecha en que el Secretario General haya recibido la declaración. De igual manera se puede retirar la declaración y surtirá efecto en el mismo plazo de tiempo desde el momento en que el Secretario General haya recibido la declaración (art. 38). Este artículo será de suma utilidad para aquellos Estados con territorios en conflicto o en los cuales tenga problemas para hacer totalmente efectivo el orden interno.

Se resalta el objetivo de completar tratados con herramientas para la persecución del delito o acuerdos multilaterales o bilaterales como el Convenio Europeo de Extradición, y el Convenio Europeo de Asistencia Judicial en Materia Penal y su protocolo adicional. Igualmente se reconoce otros tratados previos entre las Partes sobre la materia, las cuales pueden regular sus relaciones y la aplicación de medidas entre los mismos, siempre y cuando no sean incompatibles con el objeto y principios del presente Convenio o afecte otros derechos, restricciones, obligaciones y responsabilidades de cada Parte (art. 39).

Al momento de la firma o depósito del instrumento de ratificación, aceptación, aprobación o adhesión, mediante declaración por escrito dirigida al Secretario General del Consejo de Europa, un Estado puede confirmar que se acoge a la facultad de exigir uno o más elementos de los artículos 2, 3, 6.1.b), 7, 9.3 y 27.9.e) (art. 40). La legislación interna de cada Estado puede diferir del tratado al exigir parte o todos los requisitos de algunos artículos, por eso se habilita la opción de declaraciones.

Para el caso de Estados federales, se habilita la opción de reservarse el derecho de cumplir las obligaciones del Capítulo II debido a la relación de su gobierno central y los estados que la constituyen u otras entidades territoriales análogas. Adicionalmente se dan indicaciones de la formulación de la reserva y las disposiciones cuya aplicación sea competencia legislativa de cada uno de los estados constituyentes u otras entidades territoriales análogas (art.41). El Convenio brinda facilidades para las Partes, entendiendo que no todos los Estados cuentan con la misma organización de Estado o constituciones similares.

Al igual que las declaraciones, al momento de la firma o depósito del instrumento de ratificación, aceptación, aprobación o adhesión, mediante una notificación por escrito dirigida al Secretario General del Consejo de Europa,

un Estado puede confirmar que se acoge a una o varias reservas de algunos artículos del Convenio detallados (art.42). Esta habilitación de reservas permite que más Estados puedan adherirse al Convenio y puedan seguir siendo coherentes con su legislación interna, la cual puede tener disposiciones similares, pero no iguales al del Convenio.

Si un Estado desea retirar su reserva de manera parcial o total, puede hacerlo vía notificación por escrito al Secretario General del Consejo de Europa. El retiro surtirá efecto al momento de recibida la notificación o la fecha que la misma establezca, tratando que sea lo más pronto posible. El Secretario General podrá solicitar periódicamente a las Partes que hayan formulado reservas, información sobre perspectivas de su retiro (art. 43).

Las propuestas de enmienda estarán permitidas, las cuales deben ser comunicadas por el Secretario General del Consejo de Europa a las Partes y a los invitados a adherirse. Las propuestas de enmiendas serán comunicadas al Comité Europeo para Problemas Criminales, quien someterá su opinión al Comité de Ministros. Este último examinará la propuesta considerando a todas las partes y de aceptarse la adopción, se remitirá a las partes para su aceptación. La entrada en vigor será de treinta días después de que todas las partes hayan informado al Secretario General su aceptación (art. 44). Con este artículo se busca dar a conocer que el Convenio brinda las facilidades para hacer modificaciones al mismo, debido al constante cambio de los delitos y los procedimientos a seguir. De igual forma muestra que considera la opinión de todas las partes para hacer más democrática la aplicación de la enmienda.

El Convenio permite, en caso de controversias sobre interpretación o aplicación, que las Partes puedan solucionar las mismas mediante negociación u otro medio pacífico, entre las que se encuentran tres soluciones (art. 45). Se resalta el hecho de no limitar las opciones disponibles, dando libertad de elección y el acuerdo mutuo.

Las Partes se consultarán periódicamente para identificar problemas en la utilización y aplicación del Convenio, las repercusiones de las declaraciones y reservas, novedades en el ámbito de la delincuencia informática y obtención de pruebas en formato electrónico, y el estudio de la posibilidad de ampliar o enmendar el Convenio. Todo esto informando periódicamente al CDPC, quien podrá tomar medidas para ayudar a las Partes en sus esfuerzos por ampliar o enmendar el Convenio. El Secretario General también podrá asistir a las Partes (art. 46).

Las Partes podrán tener asistencia por los efectos que se generarán cuando aplican los artículos 40 y 42. Estas consultas correrán a cargo de las Partes interesadas y brinda un importante soporte para el cumplimiento del Convenio y una mejora a futuro, dando a entender que el mismo deberá estar actualizado para adecuarse a los nuevos cambios en un mundo globalizado y donde la ciberdelincuencia evoluciona a pasos agigantados.

Las Partes podrán denunciar el Convenio en cualquier momento mediante una notificación al Secretario General, surtiendo efecto el primer día del mes siguiente a la expiración de un plazo de 3 meses desde que el Secretario General reciba la notificación (art. 47).

El Secretario General notificará a los Estados miembros y no miembros del Consejo de Europa, Estados adheridos y los invitados a adherirse sobre cualquier firma, cualquier depósito de instrumento, fechas de entrada en vigor, declaraciones, reservas y cualquier otro acto, notificación o comunicación en relación al Convenio (art. 48). Demostrando la importancia de la actividad realizada por el Secretario General para la correcta y oportuna transmisión de información a las Partes, y el respeto al principio de transparencia en el marco del Convenio.

2.3. Los Estados Parte

El Convenio de Budapest sobre la Ciberdelincuencia cuenta con sesenta y un Estados Parte, los cuales están distribuidos en cuarenta y tres Estados miembros de la Comunidad Europea y dieciocho Estados no miembros de la misma comunidad, provenientes de todos los continentes.

Cuadro Nº 2: Los Estados miembros del Consejo de Europa

Los Estados miembros del Consejo de Europa			
Albania	Dinamarca	Lituania	Rumania
Alemania	Estonia	Luxemburgo	Serbia
Andorra	Finlandia	Malta	República Eslovaca
Armenia	Francia	Mónaco	Eslovenia
Austria	Georgia	Montenegro	España
Azerbaiyán	Grecia	Países Bajos	Suiza
Bélgica	Hungría	Noruega	República de Macedonia
Bosnia y Herzegovina	Islandia	Polonia	Turquía
Bulgaria	Italia	Portugal	Ucrania
Croacia	Letonia	República Checa	Reino Unido
Chipre	Liechtenstein	República de Moldavia	

Fuente: Consejo de Europa
Elaboración: Propia
Fecha de revisión: 11/09/2018

Cuadro Nº 3: Los Estados no miembros del Consejo de Europa

Los Estados no miembros del Consejo de Europa			
Argentina	Costa Rica	Marruecos	Sri Lanka
Australia	Dominica	Panamá	Tonga
Cabo Verde	Israel	Paraguay	Estados Unidos
Canadá	Japón	Filipinas	
Chile	Mauricio	Senegal	

Fuente: Consejo de Europa
Elaboración: Propia
Fecha de revisión: 11/09/2018

De igual manera, en base a su participación, se puede distribuir los Estados Parte de la siguiente manera:

- Cuarenta y tres Estados miembros del Consejo de Europa y tres no miembros que participaron en la elaboración del Convenio y están vinculados por aprobación o ratificaron.
- Quince Estados no miembros del Consejo de Europa que aceptaron su vinculación mediante la adhesión.

Todos los Estados miembros del Consejo de Europa firmaron el Convenio, pero no todos ratificaron el mismo. Los Estados que a la fecha no ratifican su vinculación al Convenio son Irlanda, Rusia, San Marino y Suecia (COE, s.f.a).

Destacar ocho Estados Parte que pertenecen a la región de América Latina y el Caribe, ya sea por su apoyo en la elaboración del instrumento o por su posterior adhesión. Estos son Argentina, Canadá, Chile, Costa Rica, República Dominicana, Estados Unidos, Panamá y Paraguay.

De igual manera se resalta el hecho que otros países de la región fueron invitados, como son los casos de Colombia y el Perú. En el primer caso, el 22 de junio de 2018 su Congreso aprobó la adhesión de Colombia al Convenio de Budapest (El Tiempo, 2018), por lo que dentro del primer cuatrimestre del año 2019 podrían ya estar adheridos si depositan el instrumento de adhesión en lo que queda del presente año. El caso peruano se encuentra en una situación similar, pero con menor avance, el cual se detallará y explicará en el Capítulo III de la presente tesis.

En la sección de anexos se encuentran los cuadros que detallan los Estados Parte por categoría, la fecha de firma, ratificación (o adhesión) y entrada en vigor del tratado para los mismos.

2.3.1. Las declaraciones de los Estados Parte

Según lo establecido por el artículo 39, los Estados Parte presentaron declaraciones en referencia a los artículos 2, 3, 6.1.b), 7, 9.3 y 27.9.e) al momento del depósito del instrumento aprobación, ratificación o adhesión (COE, s.f.b).

Todos los Estados Parte realizaron declaraciones para confirmar a su autoridad responsable para enviar o recibir demandas de extradición o de detención provisional en ausencia de tratado (art. 24.7); todos menos Argentina confirmaron su autoridad central responsable de enviar o responder solicitudes de asistencia mutua (art. 27.2) vía declaración; y todos menos Argentina, Montenegro, Reino Unido, Suiza y Ucrania confirmaron a su entidad responsable de la Red 25/7 (art. 35) por la misma vía.

Las reservas al artículo 2, realizadas por doce Estados Parte se realizaron por requerimientos internos en los que se considera el concepto de intención criminal, intención de defraudar o causar daño, infringir medidas de seguridad, entre otros.

Finalmente, se realizaron declaraciones referidas a otros artículos que habilitaban dicha posibilidad y que también requerían consideraciones específicas por parte de los Estado Parte que las presentaron. Un caso a resaltar es el de aplicación territorial (art. 38), donde Estados como Azerbaiyán, Dinamarca, Países Bajos y la República de Moldavia especifican en qué territorios se acepta la aplicación o en cuales no se asegurará el mismo hasta nuevo aviso.

El siguiente cuadro incluye los artículos sobre los cuales se realizaron declaraciones, los cuales están organizados por número de declaraciones realizadas por los Estados Parte.

Cuadro Nº 4: Las declaraciones de los Estados Parte

Artículo	Número de declaraciones
Art. 24.7 – Confirmación de la autoridad responsable de enviar o recibir demandas de extradición o de detención provisional en ausencia de tratado	61
Art. 27.2 – Confirmación de la autoridad central responsable de enviar o responder solicitudes de asistencia mutua	60
Art. 35 – Red 24/7	56
Art. 2 – Acceso ilícito	12
Art. 27.9.e – Solicitudes dirigidas sobre el párrafo “e” deben enviarse a la autoridad central	11
Art. 7 – Falsificación informática	6
Art. 40 - Declaraciones	6
Art. 29.4 – Exigencia de la doble tipificación penal como condición para atender a una solicitud de asistencia mutua con vistas al registro o al acceso por un medio similar, a la confiscación o a la obtención por un medio similar o a la revelación de los datos almacenados en relación con delitos diferentes de los previstos de conformidad con los artículos 2 a 11	4
Art. 38 – Aplicación territorial	4
Art. 3 – Interceptación ilícita	3
Art. 6 – Abuso de dispositivos	2
Art. 24.5 – Denegación de extradición	2
Declaraciones sin relación a un artículo del Convenio	2
Art. 4 – Ataque a la integridad de datos	1
Art. 9 – Delitos relacionados con la pornografía infantil	1
Art. 10 – Delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines	1
Art. 21 – Interceptación de datos relativos al contenido	1

Fuente: Consejo de Europa
Elaboración: Propia
Fecha de revisión: 11/09/2018

En la sección de anexos se encuentran todas las declaraciones realizadas por cada Estado Parte al momento de depositar el instrumento aprobación,

ratificación o adhesión. Las cuales están organizadas por el número de artículo sobre el cual hacen mención las mismas.

2.3.2. Las reservas de los Estados Parte

Según lo establecido por el artículo 42, los Estados Parte que vieron conveniente acogerse a una o varias reservas previstas, las hicieron en relación con el párrafo 2 del artículo 4, el párrafo 3 del artículo 6, el párrafo 4 del artículo 9, el párrafo 3 del artículo 10, el párrafo 3 del artículo 11, el párrafo 3 del artículo 14, el párrafo 2 del artículo 22, el párrafo 4 del artículo 29 y el párrafo 1 del artículo 41 al momento del depósito del instrumento aprobación, ratificación o adhesión (COE, s.f.b).

La principal reserva presentada por los Estados Parte está relacionada al derecho de denegarse a solicitudes de conservación cuando al momento de la revelación de datos no se cumpla la condición de doble tipificación exigida por una Parte como condición para la asistencia mutua (párr. 4 art. 29). Esta reserva fue presentada por trece Estados europeos, Argentina y Chile

Otra cantidad importante de reservas se refieren a la aplicación de disposiciones de procedimiento (art. 14) y delitos relacionados con la pornografía infantil (art. 9). En el último caso por ejemplo se reservan, según el Estado, el derecho a no aplicar parte o todo el artículo cuando una persona luce visualmente como un menor de edad que actúa con conducta sexualmente explícita, o cuando se tiene posesión de material de un menor de edad con por lo menos 15 años con su consentimiento, porque la legislación de un territorio no tiene tipificado el delito.

También se presentaron reservas en el caso de posesión de dispositivos para la comisión de los delitos de los artículos 2 al 5 o cuando la posesión de los

mismos no afecte a la venta, distribución o puesta a disposición de contraseñas, códigos de acceso o datos informáticos para acceder a un sistema (párr. 3 art. 6); y otras reservas relacionadas a la obtención de datos, acceso ilícito, conservación rápida de datos, entre otros.

El siguiente cuadro incluye los artículos sobre los cuales se realizaron reservas, las cuales están organizadas por el número de reservas realizadas por los Estados Parte.

Cuadro Nº 5: Las reservas de los Estados Parte

Artículo	Número de Reservas
Art. 29.4 – Exigencia de la doble tipificación penal como condición para atender a una solicitud de asistencia mutua con vistas al registro o al acceso por un medio similar, a la confiscación o a la obtención por un medio similar o a la revelación de los datos almacenados en relación con delitos diferentes de los previstos de conformidad con los artículos 2 a 11	15
Art. 9 – Delitos relacionados con la pornografía infantil	14
Art. 14 – Ámbito de aplicación de las disposiciones de procedimiento	12
Art. 6 – Abuso de los dispositivos	11
Art. 42 – Reservas	11
Art. 22 – Jurisdicción	10
Art. 4 – Ataques a la integridad de los datos	7
Art. 11 – Tentativa y complicidad	4
Art. 10 – Delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines	3
Art. 20 – Obtención en tiempo real de datos relativos al tráfico	3
Art. 2 – Acceso ilícito	1
Art. 13 – Sanciones y medidas	1
Art. 16 – Conservación rápida de datos informáticos almacenados	1
Art. 21 – Interceptación de datos relativos al contenido	1
Art. 41 – Cláusula federal	1

Fuente: Consejo de Europa
Elaboración: Propia
Fecha de revisión: 11/09/2018

En la sección de anexos se encuentran todas las reservas realizadas por cada Estado Parte al momento de depositar el instrumento aprobación, ratificación o adhesión. Las cuales están organizadas por el número de artículo sobre el cual hacen mención las mismas.

2.4. Los beneficios del Convenio

El Convenio de Budapest sobre la Ciberdelincuencia trae una serie de importantes beneficios para los Estados Parte que hicieron constancia internacional de su consentimiento a obligarse por este instrumento internacional.

Estos beneficios podrán ser aprovechados y potenciados en la medida que las brechas tecnológicas y dificultades técnicas de cada Estado Parte se logren resolver, para lo cual se contará con la cooperación internacional de los involucrados.

En base a lo estipulado en el Convenio, se rescata los principales beneficios para los Estados Parte del Convenio son los siguientes.

- Aplicar una política penal común con objeto de proteger a la sociedad frente a la ciberdelincuencia, mediante la adopción de una legislación adecuada.
- Complementar como herramienta la legislación nacional vigente de cada uno de los Estados Parte.
- Permitir la protección de los intereses legítimos en la utilización y el desarrollo de las tecnologías de la información.
- Usar herramientas establecidas en el mismo Convenio para prevenir delitos que pongan en riesgo o abusen de sistemas y datos informáticos.

- Lograr cooperación en materia penal rápida y fiable, lo que fortalecerá las capacidades de detección, investigación y sanción de los Estados Parte para la lucha efectiva contra los delitos previstos en los artículos del capítulo II del Convenio.
- Conseguir la aplicación de programas técnicos y de capacitación sobre la ciberdelincuencia y temas afines patrocinados por el Consejo de Europa y otras organizaciones internacionales.
- Brindar asistencia a los Estados miembros para el desarrollo y despliegue de notificaciones que puedan ser vinculantes con las de otros actores clave.
- Permitir la participación de actores clave de suma importancia para una mejor lucha contra la ciberdelincuencia como son: otros Estados, agencias, el sector privado y la sociedad civil.

2.5. Los avances para la adhesión en América Latina y el Caribe

Desde el año 2004 mediante la Reunión de Ministros de Justicia o de Fiscales Generales de las Américas (REMJA/OEA) y su Grupo de Trabajo en Delito Cibernético ha alentado a sus miembros a implementar los principios del Convenio de Budapest sobre la Ciberdelincuencia y a considerar su adhesión al tratado. En América Latina y el Caribe, la Comisión Económica para América Latina y el Caribe (CEPAL) con la Agenda Digital para América Latina y el Caribe (eLAC) eLAC2007, eLAC2010 y eLAC2015 ha influido de manera decisiva en el desarrollo de instrumentos nacionales armonizados para la ciberlegislación conforme al contexto regional.

Los países de la región continúan avanzando a velocidades distintas, con brechas dentro de ellos y entre ellos, así como diferencias frente a las economías más desarrolladas. Por tal motivo, la CEPAL con la eLAC2018 busca fortalecer el proceso de integración regional en materia digital,

atendiendo al dinamismo tecnológico, los cambios sociales y la transición hacia una sociedad del conocimiento. Ese objetivo se logrará trabajando en 23 objetivos de cinco áreas de acción: acceso e infraestructura; economía digital, innovación y competitividad; gobierno electrónico y ciudadanía; desarrollo sostenible e inclusión y gobernanza para la sociedad de la información (Cepal, 2015, p. 3-6).

América Latina

En referencia a los países de la región de América Latina, al 1 de noviembre de 2018, el Convenio ya fue ratificado y entró en vigor para los Estados de Argentina, Chile, Costa Rica, República Dominicana, Panamá y Paraguay; y fue ratificado y entrará en vigor a inicios del año 2019 para Colombia (COE, s.f.a).

Los países mencionados previamente adecuaron su legislación interna, en los casos que fue requerido, y cumplieron con los procedimientos establecidos por el Convenio para su adhesión.

Un caso a destacar es el de Argentina, país invitado por el Consejo de Europa el 27 de septiembre de 2017 para adherirse al Convenio, y que para quincena de diciembre del mismo año su congreso ya había aprobado la adhesión al Convenio, para finalmente adherirse con el depósito del instrumento correspondiente el 5 de junio de 2018. Desde el 1 de octubre de 2018 el Convenio se encuentra en vigor para ese país (COE, s.f.a).

Por otra parte, Brasil fue invitado el 10 de mayo de 2017, encontrándose en proceso de cumplir los requisitos para la adhesión; México no tiene avances en la adhesión por intereses internos que no le permiten dar el paso para modernizar su legislación nacional; y el Perú se encuentra en la etapa final del procedimiento interno de perfeccionamiento a la espera de la aprobación del

Congreso de la República mediante la Resolución Legislativa correspondiente, para que posteriormente el señor Presidente de la República ratifique el Convenio a través de un Decreto Supremo, lo que permite continuar con el trámite correspondiente a la expresión de la voluntad internacional que se materializa en la elaboración del instrumento de adhesión para su depósito ante el Secretario General del Consejo de Europa. (COE, s.f.c).

Finalmente, Bolivia, Ecuador, Venezuela y otros países aún no han mostrado interés o avances para una futura adhesión al Convenio de Budapest sobre la Ciberdelincuencia

El Caribe

La Unión Internacional de Telecomunicaciones elaboró un Informe de Evaluación de Ciberdelincuencia y Delitos Electrónicos en Países del Caribe. El informe en mención de la ITU menciona que la ciberdelincuencia es uno de los temas abordados por la Commonwealth para la armonización de sus legislaciones, la cual busca facilitar la cooperación internacional en la materia (ITU, 2014, p. 155).

Para lograr tal fin, a inicios del año 2002, los Ministros de Derecho de la Commonwealth decidieron ordenar un grupo de expertos para desarrollar un marco legal común basado en el Convenio de Budapest sobre la Ciberdelincuencia para combatir ese problema que afectaba a todos los miembros. A finales del mismo año se presentó el Proyecto de Ley sobre Informática y Delincuencia Informática que contenía normas que cumplían los estándares definidos por el Convenio de Budapest (ITU, 2014, p. 155).

Al 1 de noviembre de 2018, Canadá es el único Estado miembro de la Commonwealth en el continente que ha logrado la adhesión al Convenio de Budapest sobre la Ciberdelincuencia (COE, s.f.a).

3. EL PERÚ: LA ADHESIÓN, LAS OPORTUNIDADES Y LOS DESAFIOS

El tercer capítulo de la tesis tiene como principales objetivos el dar a conocer los avances realizados por el Perú para la lucha contra los delitos informáticos y ciberdelincuencia; y determinar los desafíos y oportunidades que el Perú deberá considerar ante su futura adhesión al Convenio de Budapest sobre la Ciberdelincuencia, para que el Ministerio de Relaciones Exteriores, junto a otras instituciones del Estado competentes, pueda desarrollar acciones en pro de la población peruana y del cumplimiento de los compromisos adquiridos.

El capítulo está divido en dos partes. La primera presentará el contexto e intención del Perú para adherirse al Convenio, presentando eventos y situaciones que llevan al Estado peruano a comprometerse más con el objetivo de la adhesión; los antecedentes legales a la Ley 30096, Ley de Delitos Informáticos y Ley 30171, que modifica la Ley 30096, Ley de Delitos Informáticos; los avances del Perú en materia de legislación nacional para el cumplimiento de los requisitos establecidos por el Convenio.

La segunda parte del capítulo tratará los trabajos realizados por el Ministerio de Relaciones Exteriores, y otras instituciones y sectores del Estado peruano para el perfeccionamiento interno y la futura adhesión al Convenio; las declaraciones y reservas que presentará el Estado peruano al momento de depositar el instrumento de adhesión; y finalmente, las oportunidades y desafíos que el Perú tendrá aprovechar y enfrentar tras la adhesión al Convenio de Budapest sobre la Ciberdelincuencia.

Todos estos elementos permitirán tener una mejor visión de la situación actual del Estado peruano y el papel que la Cancillería deberá tomar en este nuevo escenario donde el ciberespacio y la ciberdelincuencia tienen un peso cada vez mayor en el escenario internacional.

3.1. El contexto y la intención del Perú al adherirse al Convenio

Desde la creación del Convenio de Budapest sobre la Ciberdelincuencia en el año 2001, se mostró un gran interés por parte del Estado peruano de adherirse al Convenio cuando la posibilidad estuviera disponible, pero en ese momento se tenía que trabajar internamente en términos de adecuación normativa y coordinación entre instituciones. De igual manera fue visible la necesidad de la participación de un ente que diera las directrices y llevara adelante los nuevos proyectos relacionados al ciberespacio, y a las Tecnologías de la Información y Comunicación.

En el año 2003, tras la creación de la Comisión Multisectorial para el Desarrollo de la Sociedad de la Información (CODESI) y la fusión de la Subjefatura de Informática del Instituto Nacional de Estadística e Informática (INEI) con la PCM, se da a conocer la Oficina Nacional de Gobierno Electrónico mediante Decreto Supremo Nº 067-2003-PCM. Una de las primeras actividades de la ONGEI fue la creación de Agendas Digitales y la Política de Modernización del Estado (PCM, 2013, p. 34).

Tras participar en la Cumbre sobre la Sociedad de la Información, realizada en Túnez en 2005, y habiéndose comprometido con los Objetivos de Desarrollo del Milenio (ahora conocido como Objetivos de Desarrollo Sostenible); el Perú comprendió la importancia de las TICs como una herramienta para el desarrollo humano equitativo y sostenible, que se verá reflejado en la competitividad, y crecimiento económico y social de su población (PCM, 2011, p. 16-37).

Un paso importante fue la creación de la Agenda Digital 2.0 en el año 2011, la cual buscaba desarrollar la Sociedad de la Información en el Perú. Esta iniciativa se complementaría con la Política Nacional de Gobierno Electrónico

2013-2017, buscando las dos la futura la adhesión del Perú al Convenio de Budapest sobre la Ciberdelincuencia.

Con el proceso de adhesión encaminado, el Ministerio de Relaciones Exteriores informó en el mes de junio del 2017 vía Nota Informativa 339-17, que el Perú está muy cerca de convertirse en un Estado miembro del Convenio de Budapest contra sobre la Ciberdelincuencia. En la misma nota resalta que la integración a este acuerdo es importante y necesario porque ayudará a prevenir los actos que pongan en peligro la confidencialidad, la integridad y la disponibilidad de los sistemas, redes y datos informáticos, así como su abuso.

> "(…) la próxima adhesión de nuestro país al Convenio resulta importante y necesaria, para ayudar a prevenir los actos que pongan en peligro la confidencialidad, la integridad y la disponibilidad de los sistemas, redes y datos informáticos, así como su abuso; garantizando la tipificación como delito de dichos actos, facilitando su detección, investigación y posterior sanción, tanto a nivel nacional como internacional, y estableciendo disposiciones que permitan una cooperación judicial internacional rápida y fiable. (...)La adhesión permitirá al Perú aplicar a programas técnicos y de capacitación sobre Ciberdelincuencia y temas afines. A su vez, se beneficiará de la cooperación entre los países parte del Convenio. Al incorporarnos, nuestro país será pionero en la región latinoamericana en la lucha frontal contra la Ciberdelincuencia. Con ese objetivo, esta Cancillería ha desplegado sus mejores esfuerzos para que la adhesión al Convenio sea realizada de la forma más expeditiva posible, y así lograr que el Perú, y particularmente su sistema judicial, pueda beneficiar a todos los peruanos a través de las herramientas que pone a nuestra disposición el Convenio de Budapest sobre Ciberdelincuencia" (MRE, 2017).

Unos meses después, en agosto de 2017, se hace entrega formal de la Política de Estado 35 – “Sociedad de la Información y Sociedad del Conocimiento”, con la cual el Perú se compromete a impulsar una sociedad de la información hacia una sociedad del conocimiento orientada al desarrollo humano, promover el acceso universal al conocimiento a través de las TIC,

fortalecer la gobernabilidad democrática y desarrollo sostenible, entre otros (Acuerdo Nacional, 2017).

Finalmente, durante el año 2018 se publicaron los Lineamientos para el uso de servicios en la nube para entidades de la Administración Pública del Estado Peruano, mediante Resolución de Secretaría de Gobierno Digital Nº 001-2018-PCM/SEGDI (SEGI, 2018ª, p. 1-2); la disposición para la creación de un Comité de Gobierno Digital en cada entidad de la Administración Pública, mediante Resolución Ministerial Nº 119-2018-PCM (SEGDI, 2018b, p. 1-3); la aprobación de la Definición de Seguridad Digital en el Ámbito Nacional, Mediante Decreto Supremo Nº 050-2018-PCM (SEGDI, 2018c, p. 1-2); y el Decreto Legislativo que Aprueba la Ley de Gobierno Digital mediante Decreto Legislativo Nº 1412 (SEGI, 2018d, p. 1-5). Junto a esto, se tiene desarrollada una Política Nacional de Ciberseguridad aún no se encuentra vigente.

Por lo tanto, es claro que, tras todos los compromisos y pasos dados por el Estado peruano, la adhesión al Convenio de Budapest es un objetivo importante para dar soporte a los avances previos antes mencionados. El Convenio complementará y brindará herramientas para el cumplimiento de la Política Nacional 35 que a su vez permitirá el paso de la sociedad de la información hacia la sociedad del conocimiento y el desarrollo del país, y por ende, el cumplimiento de los Objetivos de Desarrollo Sostenible (ODS).

3.2. Antecedentes legales

El Perú fue de los primeros países en la región de América Latina en considerar temas de ciberdelincuencia mediante una legislación que consideraba los delitos informáticos. Villavicencio detalla la evolución de la legislación referida a ciberdelincuencia en el Perú al indicar que el delito informático en un inicio se encontraba tipificado en el artículo 186, inciso 3,

segundo párrafo del Código Penal de 1991. Esta regulación no era propia de un delito autónomo, sino como una agravante del delito de hurto. Posteriormente se reconocieron en el Código Penal peruano otros delitos informáticos como la interferencia, acceso o copia ilícita contenida en base de datos (art. 207-A); alteración, daño o destrucción de base de datos (art. 207-B); circunstancias cualificantes agravantes (art. 207-C) y tráfico ilegal de datos (art. 207-D) (Villavicencio, 2014, p. 287).

Desde el año 2013 en el Perú se legislan los casos de delitos informáticos con la Ley 30096 (Ley de Delitos Informáticos), la cual actualiza los delitos y sus penas, y deroga los artículos 207-A, 207-B, 207-C y 207-D del Código Penal. La nueva ley está conformada por siete capítulos que se estructuran de la siguiente manera: finalidad y objeto de la ley (Capítulo I), delitos contra datos y sistemas informáticos (Capítulo II), delitos informáticos contra la indemnidad y libertad sexual (Capítulo III), delitos informáticos contra la intimidad y el secreto de las comunicaciones (Capítulo IV), delitos informáticos contra el patrimonio (Capítulo V), delitos informáticos contra la fe pública (Capítulo VI) y las disposiciones comunes (Capítulo VII).

Unos meses después, en marzo de 2014 se promulgó la Ley 30171, Ley que modifica la Ley 30096, Ley de Delitos Informáticos. La finalidad de esta ley fue adecuar la Ley 30096 a los estándares legales del Convenio sobre la Ciberdelincuencia al incorporar, en la redacción típica de los artículos 2, 3, 4, 7, 8 y 10, la posibilidad de cometer el delito deliberada e ilegítimamente.

Cabe resaltar que la legislación peruana en muchos de sus artículos, supera a su contraparte del Convenio de Budapest sobre la Ciberdelincuencia al considerar elementos de importancia que dan soporte para determinar el delito informático y refuerzan el establecimiento de responsabilidad penal.

3.2.1. Correlación del Convenio de Budapest y legislación peruana

El presente cuadro incluye las leyes nacionales y convenios con los que cuenta el Perú para sustentar que cumple con los estándares requeridos por el Consejo de Europa para su adhesión al Convenio de Budapest sobre la Ciberdelincuencia.

Cuadro Nº 6: Cuadro de correlación del Convenio de Budapest y legislación peruana

Convenio de Budapest	El Perú
Capítulo I - Terminología	
Artículo 1 - Definiciones	El Código Penal no señala definiciones.
Capítulo II - Medidas que deberán adoptarse a nivel nacional	
Artículos 2, 3, 4, 5, 6, 7*, 8, 9, 10, 11, 12, 13, 14, 15, 16, 20, 21, 22	Artículos 2, 3, 4, 7, 8, 10** de la Ley 30096, Ley de delitos informáticos, y su modificatoria Ley 30171; Artículos 16 al 19 del Capítulo II, Artículos 23 al 27 del Capítulo IV, Artículos 28, 105, 181-A., 183-A. del Código Penal; Artículo VIII del Título preliminar, Título III de la Sección 2, Capítulo VI, Capítulo VII, Artículos 19, 220, 221, 230 del Código Penal Procesal; Convención de Roma
Capítulo III - Cooperación Internacional	
Artículos 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35	Artículos 508, 510, 511, 513 del Código Penal Procesal; el Perú está suscrito a la Red 24/7.
Capítulo IV - Cláusulas finales	
Artículo 42 - Reservas	El tratado establece que los Estados pueden presentar reservas al momento de su adhesión.

Fuente: Comunidad Octupus de Ciberdelincuencia del Consejo de Europa.
Elaboración: Propia
*La legislación peruana no prevé la figura del art. 7 del Convenio, pero puede exigir que exista una intención fraudulenta o delictiva similar para generar responsabilidad penal.
**La legislación peruana no sanciona actos preparatorios, pero sí la tenencia ilegal de armas (delito de peligro).

En la sección de anexos se encuentra el cuadro de correlación de los artículos del Convenio de Budapest y la legislación peruana presentado previamente de manera detallada, con comentarios adicionales por cada artículo para una mejor relación de los conceptos.

Normativa peruana relacionada

En el Perú existe normativa relacionada al cumplimiento de los artículos del Convenio de Budapest sobre la Ciberdelincuencia, la cual está conformada por la Ley 30096, la Ley 30171, el Código Penal Peruano y el Código Procesal Penal.

La normativa mencionada previamente se complementa y está relacionada directamente en su aplicación con otras leyes que versan sobre delitos, organización de entidades del Estado peruano y el Código de Ejecución Penal según la siguiente lista.

- Código Penal Peruano,
- Código Procesal Penal,
- Código de Ejecución Penal,
- Ley Orgánica del Poder Judicial,
- Ley Orgánica del Ministerio Público,
- Ley Nº 27697, Ley que otorga la facultad al fiscal para la intervención y control de comunicaciones y documentos privados en caso excepcional,
- Ley Nº 28493, Ley que regula el uso del Correo Comercial No Solicitado (SPAM),
- Ley Nº 28774, Ley que crea el Registro Nacional de Terminales de Telefonía Celular, Establece Prohibiciones y Sanciona Penalmente a quienes Alteren y Comercialicen Celulares de Procedencia Dudosa,
- Ley Nº 29499, Ley que Establece la Vigilancia Electrónica Procesal,
- Ley Nº 29733, Ley de Protección de Datos Personales,
- Ley Nº 29867, Ley que Incorpora Diversos Artículos al Código Penal Relativos a la Seguridad en los Centros de Detención o Reclusión,
- Ley Nº 30076, Ley que Modifica el Código Penal, Código Procesal Penal, Código de Ejecución Penal y el Código de los Niños y Adolescentes y

Crea Registro y Protocolos con la Finalidad de Combatir la Seguridad Ciudadana,

- Ley Nº 30077, Ley en contra del Crimen Organizado,
- Ley Nº 30096, Ley de Delitos Informáticos, y
- Ley Nº 30171, Ley que modifica la Ley 30096.

Documentación peruana relacionada

El Ministerio de Justicia y Derechos Humanos, la Dirección General de Tratados del Ministerio de Relaciones Exteriores, la Comisión de Relaciones Exteriores del Congreso de la República y la Presidencia de la República, elaboraron informes, un dictamen y un proyecto de Resolución Legislativa que dan fe sobre el cumplimiento por parte del Estado peruano de los requisitos normativos establecidos por el Consejo de Europa para la adhesión de Estados no Miembros y la no necesidad de realizar modificaciones o derogación de leyes para la posterior aprobación del Convenio por parte del Pleno del Congreso de la República mediante Resolución Legislativa y la ratificación por parte del Presidente de la República mediante Decreto Supremo. Los documentos son los siguientes.

- Informe Usuario Nº 14-2017-JUS/DGAC,
- Informe /DGT Nº 030-2017,
- Dictamen de la Comisión de Relaciones Exteriores Periodo Anual de Sesiones 2017-2018,
- Proyecto de Resolución Legislativa peruana que aprueba el Convenio sobre la Ciberdelincuencia.

3.3. Antecedentes al proceso de adhesión

Tras la decisión 14 de la reunión 1168 del Consejo de Europa, realizada el 10 de abril de 2013, se estableció la posibilidad de invitar a Estados no miembros para adherirse al Convenio. Esta invitación tendrá una vigencia de cinco años desde su adopción.

Con la opción habilitada para adhesión y la legislación nacional adecuada a los requisitos del Convenio en relación al derecho procesal sustantivo, el Perú -mediante su Embajada en Francia- presentó el 8 de septiembre de 2014 a la Secretaría General del Consejo de Europa una carta que expresaba el deseo de ser invitado al Convenio.

Siguiendo los procedimientos establecidos para la adhesión de Estados no miembros, el cual respetó la decisión de la mayoría establecida en el Estatuto del Consejo de Europa (artículo 20.d), y con el voto unánime de los Estados que forman parte del Comité de Ministros, se decidió tratar el tema de la solicitud de adhesión del Estado peruano.

Posteriormente, en la reunión 1215 del 9 y 10 de diciembre de 2014, y en la reunión 1220 del 18 de febrero de 2015 se invita formalmente al Perú a adherirse al Convenio.

Como se estableció en la decisión 14 de la reunión 1168, el Perú tendrá plazo hasta el 18 de febrero de 2020 para su adhesión al Convenio de Budapest sobre la Ciberdelincuencia.

3.4. Proceso de Perfeccionamiento Interno del Tratado

En el Perú, el proceso de perfeccionamiento interno de un tratado internacional es realizado mediante la participación y coordinación de los sectores del Estado involucrados.

Una vez obtenida la invitación para la adhesión por parte del Consejo de Europa, se debe iniciar el proceso de perfeccionamiento interno, en el cual la Cancillería tendrá un papel de suma importancia, tanto como ente rector a relacionado a tratados internacionales, así como orientador de otras entidades de la Administración Pública para ejecución eficaz y oportuna de procesos a seguir.

El primer paso a seguir según lo establecido en los puntos 6.2.1 y 6.2.2 de la Directiva N° 002-DGT/RE-2013, es la realización de solicitudes de opiniones a los sectores e instituciones vinculados con la materia del Convenio, para el perfeccionamiento interno (MRE, 2013, p. 4).

La entidad encargada de las consultas, coordinaciones y seguimiento para la adhesión al Convenio de Budapest sobre la Ciberdelincuencia es la Dirección de Ciencia y Tecnología, la cual pertenece a la Dirección General para Asuntos Económicos. Esta función, junto a las de promover y participar en la negociación de instrumentos internacionales referidos a su competencia; coadyuvar a su cumplimiento; formular y ejecutar acciones relacionadas a la sociedad de la información; informar a las entidades correspondientes de convenciones internacionales relacionadas a su competencia; concertar y coordinar con otros sectores temas relevantes a ciencia y tecnología, entre otros; le es otorgada en los incisos a) al j) del artículo 108 del Reglamento de Organización y Funciones del Ministerio de Relaciones Exteriores, aprobado por Decreto Supremo Nº 135-2010-RE (MRE, 2010, p. 44).

Por otro lado, la Dirección General de Tratados tiene la función, establecida en los artículos 128 y 129 del ROF del Ministerio de Relaciones Exteriores, de Formular, proponer y evaluar las normas y lineamientos técnicos para la adecuada suscripción, perfeccionamiento interno y registro de los tratados y demás instrumentos internacionales que suscriba el Perú; así como emitir opinión de carácter técnico sobre proyectos de tratados u otros instrumentos jurídicos internacionales, brindar asesoramiento, emitir opinión para determinar la vía constitucional aplicable, solicitar opinión a los sectores que corresponda, entre otros (MRE, 2010, p. 52).

Respecto al perfeccionamiento interno, este se puede realizar por vía simplificada o agravada. Esto significa, en el primer caso, que solo se requiere la ratificación por parte del Presidente de la República mediante Decreto Supremo; y en el segundo caso, se requiere la aprobación previa por el Congreso de la República mediante Resolución Legislativa y posterior ratificación del Presidente de la República a través de Decreto Supremo (MRE, 2013, p. 4).

Al tratar el Convenio de Budapest sobre la Ciberdelincuencia de manera implícita algunos temas de derechos humanos y de soberanía, dominio o integridad del Estado; se debe proceder al perfeccionamiento interno mediante el perfeccionamiento por vía agravada, tal como establece el artículo 56 de la Constitución Política del Perú de 1993. Esta atribución se le otorga en el artículo 102 de la Constitución mencionada previamente (Congreso, 1993, p. 33).

El siguiente paso a seguir será elaborar un informe de perfeccionamiento que será anexado al Proyecto de Resolución Legislativa, el cual se presentará al Congreso de la República. Esta labor la debe realizar la DGT después de una evaluación que considere las opiniones, aportes obtenidos de los demás

órganos del Ministerio de Relaciones Exteriores y sectores competentes del Estado, y los lineamientos técnicos establecidos.

Una vez que se tiene la documentación necesaria para presentar al Congreso de la República, se elabora y presenta el Proyecto de Resolución Legislativa con la firma del Presidente de la República, del Presidente del Consejo de Ministros y Ministro de Relaciones Exteriores, mediante un oficio dirigido al Presidente del Congreso de la República. Dicho oficio debe ir acompañado de un expediente que sustente la adhesión al Convenio.

Se debe considerar las siguientes indicaciones que establece el Manual del Proceso legislativo del Congreso de la República: el señor Presidente de la República debe remitir al Presidente del Congreso de la República las proposiciones de resolución legislativa para la aprobación de tratados, acompañadas por el texto íntegro del instrumento internacional, sus antecedentes, un informe sustentatorio que contenga las razones por las cuales el Poder Ejecutivo considera que debe ser aprobado por el Congreso, la opinión técnica favorable del sector o sectores competentes actualizada, y la resolución suprema que aprueba la remisión del tratado al Poder Legislativo; posteriormente, será decretada a la Comisión de Relaciones Exteriores del Congreso u otra comisión según el caso, para seguir el trámite hasta su finalización cuando el Pleno del Congreso apruebe la adhesión mediante voto favorable por mayoría simple, sin necesidad de incurrir a una doble votación (Congreso, 2012, p. 174-175).

Tras la aprobación del Congreso de la República, se procede con la ratificación del Convenio por parte del Presidente de la República mediante Decreto Supremo, según se establece en el artículo 118 de la Constitución Política del Perú de 1993 (Congreso, 1993, p. 38); para después hacer el depósito del instrumento de adhesión al Secretario General del Consejo de

Europa por intermedio del representante designado por el Ministerio de Relaciones Exteriores.

Finalmente, siguiendo las indicaciones del artículo 4 Decreto Supremo N° 001-2009-JUS, el Convenio debe ser publicados en el Diario Oficial El Peruano (MINJUSDH, 2009, p. 1-3). Para la publicación se deben considerar lo concerniente a la Ficha 119-A Publicación de los Tratados en el Diario Oficial del Manual del Proceso Legislativo del Congreso de la República, el cual establece que:

> El texto íntegro de los tratados celebrados y aprobados por el Estado peruano debe ser publicado en el diario oficial. Dicha publicación comprende, de ser el caso, uno o más instrumentos anexos. Asimismo, debe señalar el número y fecha de la resolución legislativa que los aprobó.
>
> La publicación del texto de los tratados se realiza en un plazo máximo de treinta días útiles contados a partir de la fecha en que son recibidos en el diario oficial.
>
> Corresponde al Ministerio de Relaciones Exteriores comunicar al diario oficial, en cuanto se hayan cumplido las condiciones establecidas en el tratado, para que publique la fecha de la entrada en vigor del mismo, a partir de la cual se incorpora al derecho nacional.

Asimismo, el artículo 55 de la Constitución Política del Perú dispone lo siguiente: Los tratados celebrados por el Estado y en vigor forman parte del derecho nacional (Congreso, 1993, p. 18).

Se hace mención que la ficha 119-A tiene como fuente la Ley 26647, Ley que regula los actos relativos al perfeccionamiento nacional de los tratados celebrados por el Estado peruano (Congreso, 2012, p. 176).

Al 1 de noviembre, aún se está en espera de la aprobación del Congreso de la República para la posterior ratificación por parte del Presidente de la República y depósito del instrumento de adhesión. Cabe señalar que el mismo

cuenta ya con un dictamen aprobado por unanimidad por parte de la Comisión de Relaciones Exteriores del Congreso.

3.4.1. El proceso seguido por el MRE y otros Ministerios

- 30/04/2015: Mediante Oficio RE (DAE-DCT) Nº 2-19-A/39, la Dirección de Ciencia y Tecnología (DCT) del Ministerio de Relaciones Exteriores del Perú (MRE) requirió al Ministerio de Justicia y Derechos humanos (MINJUSDH), como rector en la materia, absuelva algunos puntos del proceso de perfeccionamiento interno del Convenio de Budapest sobre la Ciberdelincuencia.

- 15/06/2015: La Dirección General de Asuntos Criminológicos (DGPCP) del MINJUSDH elaboró el borrador de un informe dando respuestas a los puntos requeridos el MRE, el cual presentó al grupo multisectorial conformado por funcionarios del Poder Judicial, Ministerio Público, Policía Nacional del Perú (PNP) y la Oficina Nacional de Gobierno Electrónico e Informática (que después sería la Secretaría de Gobierno Digital - SEGDI). La reunión sirvió para recoger comentarios y sugerencias para la mejora del informe final.

- 22/06/2015: Mediante Informe Nº 053-2015-JUS/DGPCP, la DGPCP emitió opinión respecto a los puntos del proceso de perfeccionamiento del Convenio, dando conclusiones favorables en relación a los beneficios en términos de llenado de vacíos, la cooperación internacional y la sanción de los delitos cometidos, y recomendaciones de declaraciones y reservas a presentar al momento del depósito del instrumento de adhesión.

- 11/04/2016: El Viceministro de Relaciones Exteriores del Perú confirma, vía Oficio RE (DAE-DCT) Nº 2-19-A/16, que los sectores nacionales

concernidos expresaron su conformidad con las reservas y declaraciones formuladas por la DGPCP.

- 19/04/2016: Vía Informe Nº 071-2016-JUS/DGPCP, la DGPCP concluye que las recomendaciones planteadas fueron recogidas en su totalidad en relación a las declaraciones a presentar al momento de la adhesión.

- 8/03/2017: Mediante Informe Nº 28-2017-JUS/DGJC-DCJI, se presentó una evaluación del Capítulo III del Convenio - Cooperación Internacional, el cual fue elaborado por la Dirección de Cooperación Judicial Internacional del MINJUSDH. En el informe se deja constancia que los alcances del Convenio no contravienen la normativa nacional.

- 29/03/2017: Mediante Oficio RE (DAE-DCT) Nº 2-19-B/146, la DCT convoca a la DGPCP a una reunión de trabajo para concretar los últimos pasos del perfeccionamiento interno para la adhesión del Perú al Convenio.

- La DGT solicita una reunión de Coordinación con la DGPCP vía Oficio RE (DAE-DCT) Nº 2-19-B/85.

- 15/03/2017: Mediante Oficio Nº 584-2017-JUS/DGPCP, la DGPCP informa a la DCT sobre algunas precisiones de temas que fueron materia de consulta sobre la futura adhesión del Perú al Convenio de Budapest sobre la Ciberdelincuencia.

- 31/03/2017: Se llevó a cabo una reunión multisectorial de coordinación en torno a la adhesión del Perú al Convenio de Budapest convocada por el MRE, en la que participaron funcionarios representantes de la DGPCP, de la SEGDI de la PCM, la Secretaría de Seguridad y Defensa Nacional del Ministerio de Defensa, la PNP, el Ministerio Público, el Poder Judicial y la DCT. En la reunión se acordó la importancia, los beneficios, las

oportunidades y la conformidad con lo relativo al capítulo de Cooperación Judicial del Convenio. Finalmente, todos concuerdan que no se requiere derogación o modificación de leyes y coinciden en la pertinencia de efectuar reservas y declaraciones al Convenio, delegando al MINJUSDH la evaluación y visto bueno de ellas. Posterior a la reunión, se elaboró una propuesta de Declaraciones y Reservas al Convenio de Budapest. Se consideraban declaraciones para los artículos 2, 3, 7, 27 y reservas para los artículos 6, 9 y 27.

- 12/06/2017: Vía Memorándum (DCT) Nº DCT0122/2017, la DCT solicita a la DGT el inicio del perfeccionamiento interno para la adhesión del Perú al Convenio de Budapest sobre la Ciberdelincuencia.

- 10/07/2017: Mediante Memorándum (OGJ) Nº OCJ0339/2017, la Oficina de Cooperación Judicial de la Oficina General de Asuntos Legales del Ministerio de Relaciones Exteriores se pronunció sobre el Convenio, en especial a lo referido al Capítulo III – Cooperación Internacional.

- 18/08/2017: La DGPCP del MINJUSDH mediante el Oficio Nº 149-2017-JUS/DGAC remite el Informe Usuario Nº 14-2017-JUS/DGAC, elaborado por la abogada especialista Eliana Carbajal Lovatón, que analiza y propone una serie de Declaraciones y Reservas que el Perú presentará al momento de adherirse al Convenio. Ese mismo día, mediante Memorándum (DCT) Nº DCT00162/2017, la DCT remite el informe preparado por el DGPCP y propuesta de texto de declaraciones y reservas revisada por la Dirección a la DGT, confirmando que la Autoridad Central correspondiente a los artículos 24.7, 27.2 y 35.1 será el Ministerio Público-Fiscalía de la Nación, a través de la Unidad de Cooperación Judicial Internacional y Extradiciones.

- 23/08/2017: La DGT del Ministerio de Relaciones Exteriores concluyó y presentó el Informe (DGT) Nº 030-2017 donde confirma que, en base a un análisis considerando todos los elementos disponibles recopilados en más de dos años, corresponde en primer término la aprobación por el Congreso de la República mediante Resolución Legislativa y luego su ratificación internamente por el Presidente de la República mediante Decreto Supremo.

- 27/09/2017: Vía Resolución Suprema Nº 209-2017-RE, refrendada por la Presidenta del Consejo de Ministros y Ministro de Relaciones Exteriores, y en conformidad de los artículos 56º y 102º inciso 3 de la Constitución Política del Perú y primer párrafo del artículo 2º de la Ley Nº 26647, se remite al Congreso de la República la documentación relativa al Convenio sobre la Ciberdelincuencia para su aprobación.

- 2/05/2018, mediante Oficio Nº 077-2018-PR, se solicita al Presidente del Congreso de la República se someta a consideración el Proyecto de Resolución Legislativa que aprueba el "Convenio sobre la Ciberdelincuencia", acompañando al mismo un expediente de sustento en cumplimiento de los requisitos dispuestos en los artículos 75º y 76º.1f) del Reglamento del Congreso de la República. El proyecto de Resolución legislativa contó con la firma del Presidente de la República, Presidente del Consejo de Ministros y Ministros de Relaciones Exteriores.

Para todo el proceso se siguieron las directrices establecidas en la Directiva Nº 002-DGT/RE-2013 "Lineamientos Generales sobre la suscripción, perfeccionamiento y registro de los Tratados", aprobada por Resolución Ministerial Nº 0231/RE-3013.

3.4.2. Las declaraciones a presentar por parte del Perú

Las declaraciones que presentará el Estado peruano al momento de la adhesión al Convenio de Budapest sobre la Ciberdelincuencia, mediante el depósito del instrumento de adhesión al Secretario General del Consejo de Europa, están referidas a la confirmación de la existencia de los delitos establecidos en Convenio en su legislación interna, los procedimientos en casos específicos y la confirmación de la autoridad central a la cual se dirigirán las solicitudes. A continuación, se muestra el gráfico correspondiente.

Cuadro Nº 7: Las declaraciones a presentar por parte del Perú

Artículo	Declaración
2	De conformidad con lo dispuesto en el artículo 2 del Convenio sobre la Ciberdelincuencia, la República del Perú declara que su legislación exige que el delito de acceso ilícito se cometa infringiendo medidas de seguridad.
3	De conformidad con lo dispuesto en el artículo 3 del Convenio sobre la Ciberdelincuencia, la República del Perú declara que su legislación exige que el delito de interceptación ilícita se cometa con intención delictiva y que dicho delito puede cometerse en relación con un sistema informático conectado a otro sistema informático.
7	De conformidad con lo dispuesto en el artículo 7 del Convenio sobre la Ciberdelincuencia, la República del Perú declara que podrá exigir que exista una intención fraudulenta o delictiva similar, conforme a lo establecido en su derecho interno, para que las conductas descritas en dicho artículo generen responsabilidad penal.
27.9.e	De conformidad con lo establecido en el artículo 27, numeral 9, literal e) del Convenio sobre la Ciberdelincuencia, la República del Perú declara que, en aras de la eficacia, las solicitudes efectuadas en virtud de lo dispuesto en el numeral 9 del Convenio deberán dirigirse a su autoridad central.

Fuente: Proyecto de Resolución Legislativa que aprueba el Convenio sobre la Ciberdelincuencia.
Elaboración: Propia

La declaración al artículo 2 del Convenio busca complementarla en su aplicación considerando la condición de infringir medidas de seguridad, la cual está considerada en el artículo 2 de la Ley 30096 y su modificatoria Ley 30171. Respecto a la declaración al artículo 3 del Convenio, se busca dar a conocer que la legislación peruana exige las condiciones del delito, estando contenido en el artículo 7 de la Ley 30096 y su modificatoria Ley 30171 bajo el nombre de “interceptación de datos informáticos.

En relación a la declaración del artículo 7, la legislación peruana no prevé la figura de falsedad informática, pero se podría incorporar dentro del título de delitos contra la Fe Pública como conducta que utiliza sistemas informáticos para la comisión del delito.

Finalmente, la declaración al artículo 27.9.e busca que las solicitudes sean enviadas a su autoridad central. Cabe resaltar que no menciona explícitamente que, según el Código Penal Procesal, se trata de la Fiscalía de la Nación, a través de la Unidad de Cooperación Judicial Internacional y Extradiciones.

3.4.3. Las reservas a presentar por parte del Perú

Las reservas que presentará el Estado peruano al momento de su adhesión al Convenio de Budapest sobre la Ciberdelincuencia, mediante el depósito del instrumento de adhesión al Secretario General del Consejo de Europa, están referidas a la no aplicación de todo o parte de un artículo al no entrar en conflicto con una ley interna, a conceptos y a condiciones para la aplicación de un artículo. A continuación, se muestra el gráfico correspondiente.

Cuadro Nº 8: Las reservas a presentar por parte del Perú

Artículo	Reservas
6.3	De conformidad con lo dispuesto en el párrafo 3 del artículo 6 del Convenio sobre la Ciberdelincuencia, la República del Perú se reserva el derecho de no aplicar el artículo 6, párrafo 1, literal b del Convenio.
9.4	De conformidad con el numeral 4 del artículo 9 del Convenio sobre la Ciberdelincuencia, la República del Perú considera que el bien jurídico tutelado en el derecho interno con respecto a la pornografía infantil es la libertad y/o indemnidad sexual de un menor, por lo que formula una reserva a los literales b) y c) del párrafo 2 del citado artículo, debido a que las conductas contempladas en dichas disposiciones no involucran la participación de un menor de edad.
29.4	Conforme al numeral 4 del artículo 29 del Convenio sobre la Ciberdelincuencia, la República del Perú se reserva el derecho a denegar la solicitud de conservación en virtud de dicho artículo en el caso que tenga motivos para creer que, en el momento de la revelación de los datos, no se cumplirá con la condición de doble tipificación penal.

Fuente: Proyecto de Resolución Legislativa que aprueba el Convenio sobre la Ciberdelincuencia.
Elaboración: Propia

La presentación de una reserva al artículo 6, párrafo 3 del Convenio tiene como finalidad la no aplicación al no poderse regular por la legislación interna del Perú.

En relación a la reserva del artículo 9, párrafo 4 del Convenio; al no involucrar un menor de edad, no se puede aplicar la ejecución debido a la no regulación de ese supuesto en la legislación peruana.

Finalmente, la tercera reserva, referida al párrafo 4 del artículo 29 del Convenio, busca mantener la concordancia con la legislación interna, la cual contempla la doble incriminación en los procesos de extradición según el Código Procesal Penal.

3.5. Los desafíos de la adhesión al Convenio

Los desafíos que enfrentará el Perú una vez que se adhiera al Convenio de Budapest sobre la Ciberdelincuencia están relacionados a la adecuación interna, reducción de las brechas tecnológicas y capacitaciones para poder responder de manera rápida y efectiva ante diferentes situaciones relacionada a los delitos informáticos y la ciberdelincuencia.

Un factor a considerar es que el Ministerio de Relaciones Exteriores, mediante la Dirección de Ciencia y Tecnología, tiene la función de supervisar y coadyuvar a otros Ministerios para el cumplimiento del Convenio, formulando y ejecutando acciones para dar soporte en el ámbito de su competencia. Por tal motivo, muchos de los desafíos que enfrentará el Estado peruano al momento de la adhesión serán responsabilidad del MINJUSDH y Ministerio Público.

En ese sentido, las acciones a ser realizadas por el MRE son las siguientes.

- Capacitar a personal del Ministerio de Relaciones Exteriores, Ministerio de Justicia y Derechos Humanos, Poder Judicial y Corte Suprema de la República, y otras instituciones del Estado relacionadas por su naturaleza, para cumplir con los compromisos adquiridos al momento de la adhesión al Convenio.
- Mantener plazos cortos para la recepción, análisis, respuesta y aplicación de las solicitudes de cooperación enviado por los otros Estados Parte.
- Asegurar el funcionamiento continuo del punto de contacto nacional para la red 24/7 que estará bajo responsabilidad de la Oficina de Cooperación Judicial, Internacional y Extradiciones de la Fiscalía de la Nación.
- Crear un mecanismo de cooperación para la gestión de información entre la División de Investigación en Delitos de Alta Tecnología (DIVINDAT) y el

Ministerio Público para agilizar los tiempos de toma de decisiones y respuesta ante casos de ciberdelincuencia.

- Reducir las brechas tecnológicas en instituciones del Estado para estar a la par de los otros Estados Parte y cumplir de manera correcta con las obligaciones adquiridas desde el momento que se realice la adhesión al Convenio.
- Responder de manera rápida, efectiva y adecuada ante solicitudes de cooperación judicial y de intercambio de información por parte de terceros Estados.
- Obtener recursos de Cooperación Internacional para el Desarrollo por parte de la Agencia Peruana de Cooperación Internacional (APCI) para responder a las solicitudes de Cooperación Internacional referidas fortalecimiento de infraestructura o de capacitación de instituciones o personal.

3.6. Las oportunidades de la adhesión al Convenio

Las oportunidades de las cuales el Perú podrá beneficiarse una vez que se adhiera al Convenio de Budapest sobre la Ciberdelincuencia están relacionados a la cooperación internacional, intercambio de conocimientos y experiencias, reducción de las brechas tecnológicas, participación de capacitaciones y cursos para poder responder de manera rápida y efectiva ante diferentes situaciones relacionada a los delitos informáticos y la ciberdelincuencia.

Al igual que en el caso de los desafíos, la labor del Ministerio de Relaciones Exteriores, mediante la Dirección de Ciencia y Tecnología, es de supervisar y coadyuvar a otros Ministerios para el cumplimiento del Convenio, formulando y ejecutando acciones para dar soporte en el ámbito de su competencia.

- Contar, vía la cooperación internacional de los Estados parte, con herramientas idóneas para la obtención de información para la investigación de un delito cometido por medios informáticos, facilitando el trabajo de las autoridades encargadas del cumplimiento de las responsabilidades del Convenio en cada país.
- Compartir conocimiento y experiencias con más de sesenta Estados Parte del Convenio y otros nuevos que se adherirán en los siguientes meses que están pasando por los mismos o similares casos de ciberdelincuencia en sus territorios.
- Convertirse, una vez que el Perú sea oficialmente un Estado Parte del Convenio, en un país prioritario para recepción de la cooperación internacional por parte del Consejo de Europa en temas relacionados a la ciberdelincuencia y delitos informáticos, y con eso, beneficiarse de fondos dedicados como los provenientes del proyecto GLACY+ (Global Action on Cybercrime).
- Solicitar a Estados Unidos, China o países de Europa cooperación para la reducción de las brechas tecnológicas en las instituciones que desempeñarán un trabajo directo para el cumplimiento del Convenio, sobre todo al Ministerio Justicia y Derechos Humanos y la Fiscalía de la Nación.
- Realizar coordinaciones con la Oficina de Naciones Unidas contra la Droga y el Crimen (UNODC) para la obtención mediante sus Estados miembros de conocimientos, experiencias y recursos para la lucha contra la ciberdelincuencia.
- Aprovechar las herramientas disponibles para lograr avances de importancia en los compromisos asumidos con la Política Nacional 35 – Sociedad de la información y sociedad del conocimiento, los Objetivos de Desarrollo Sostenible, la Organización para la Cooperación y Desarrollo Económico (OCDE), la Cumbre Mundial sobre la Sociedad de la Información, la Agenda Digital 2.0 y la Política Nacional de Gobierno Electrónico.

- Liderar una política de ciberseguridad y lucha contra la ciberdelincuencia dentro de la Alianza del Pacífico y posteriormente en otras organizaciones de la región.
- Fortalecer las buenas relaciones que tenemos con México ofreciendo en el marco de la Alianza del Pacífico colaboración con experiencias, conocimientos y guía por parte de especialistas para su futura adhesión al Convenio de Budapest sobre la Ciberdelincuencia.
- Fomentar junto a Colombia, Chile, México y otros países del continente americano, la realización de una Capacitación Avanzada de MISP (Malware Information Sharing Platform) cofinanciada con recursos de la Unión Europea, para potenciar una herramienta que será de mucha ayuda para la prevención de casos de ciberdelitos mediante un trabajo en conjunto efectivo realizado por todos los usuarios de la plataforma de información.

CONCLUSIONES

Los ciberdelitos y las modalidades como se realizan estos tipos de delitos informáticos se encuentran en constante evolución desde la masificación del Internet a inicios de la década de los 90, generando pérdidas económicas y daños sociales cada vez mayores gracias al uso de nuevas tecnologías y software para la comisión del delito desde cualquier punto del planeta y en cualquier momento. Para protegerse de los ciberdelitos, instituciones y empresas están realizando inversiones en ciberseguridad, generando más perdidas económicas reflejadas en menores ingresos y posibles déficits proyectados, y no haciendo frente al principal problema, el cual dejó de ser un exclusivo de un país, para ser un problema que debe ser combatido por todos los Estados mediante la cooperación internacional en materia jurídica, de conocimientos, experiencias e información relevante para establecer responsabilidad penal a los involucrados.

El Convenio de Budapest sobre la Ciberdelincuencia es una herramienta de gran utilidad en materia de derecho penal sustantivo y procesal para todos los Estados Parte al buscar la una política penal común ante los ciberdelitos, y el incrementar las capacidades y eficiencia en la investigación, persecución y proceso penal. Un factor adicional que deben considerar los Estados que deseen adherirse es la cooperación internacional, tanto en materia judicial y para la reducción de las brechas de conocimientos y tecnología, lo que permitirá un mejor accionar ante diferentes situaciones. Los avances en el proceso de adhesión varían entre cada Estado, en el caso de América Latina y el Caribe, son pocos los Estados adheridos o que están en fase avanzada de adecuación para su adhesión.

El Estado peruano ha desarrollado una legislación interna relacionada a los delitos informáticos y ciberdelincuencia, que se adecúa y supera los estándares requeridos por el Convenio de Budapest sobre la

Ciberdelincuencia. Para ampliar su margen de acción, y obtener cooperación y acceso a información de importancia para la persecución del delito, inició el proceso de adhesión al Convenio, proceso que lleva más de 3 años y cuya invitación está próxima a vencer. Tras la adhesión, el Perú asumirá responsabilidades que deberá cumplir, pero para lograrlo deberá fortalecer a instituciones como el Ministerio de Relaciones Exteriores, Ministerio de Justicia y Derechos Humanos y el Ministerio Público. Este fortalecimiento debe conseguir reducir las brechas tecnológicas que tiene cada institución del Estado y agilizar los procesos internos para responder adecuadamente ante solicitudes de otros Estados Parte. De igual manera, se deberá aprovechar las opciones disponibles en el Convenio para captar cooperación internacional, y adecuarnos correctamente a los constantes cambios en el ciberespacio y combatir a los ciberdelitos que evolucionan constantemente.

RECOMENDACIONES

Habiendo identificado, y descrito los desafíos y oportunidades para el Perú ante la futura adhesión al Convenio de Budapest sobre la Ciberdelincuencia en el ámbito de las competencias del Ministerio de Relaciones Exteriores, se sugiere lo siguiente.

1. Hacer incidencia para la aprobación en el pleno del Congreso de la República de la adhesión del Perú al Convenio de Budapest sobre la Ciberdelincuencia, teniendo en cuenta que el plazo de vigencia de la invitación realizada por el Consejo de Europa terminará en menos de un año y medio (18 de febrero de 2020).
2. Brindar todo el apoyo necesario, en términos de comunicación, representación y seguimiento continuo, al Ministerio de Justicia, Ministerio Público, Corte Suprema y otras instituciones competentes del Estado para facilitar sus iniciativas de captación de cooperación internacional para la reducción de sus brechas tecnológicas, capacitación de los funcionarios públicos y el aseguramiento de interconexión de data en tiempo real y rápida con otros Estados Parte del Convenio.
3. Realizar una reunión con la Agencia Peruana de Cooperación Internacional para solicitar recursos a futuro que serán destinados para el cumplimiento de los compromisos de cooperación internacional en temas de desarrollo tecnológico y capacitación del personal de otros Estados Parte y ajenos al Convenio (artículo 23 del Convenio).
4. Programar cursos de capacitación para el personal del Ministerio de Relaciones Exteriores en relación a los delitos informáticos y ciberdelitos, a fin de poder utilizar los conocimientos en propuestas que nazcan en foros u organizaciones internacionales.
5. Dar mayor peso a la Política Nacional 35 dentro de la Política Exterior del Perú y trabajar políticas internas a miras de trabajar una imagen de líder regional en la lucha contra la ciberdelincuencia y avances en el

aprovechamiento del ciberespacio para generar desarrollo para su población.

6. Desarrollar y liderar una política regional para la colaboración e intercambio de conocimientos para la reducción de brechas con países de Norteamérica, Europa y Así, comenzando en una primera etapa con la Alianza del Pacífico.
7. Aunar esfuerzos con aquellos países con los cuáles el Perú comparte la preocupación sobre la prevención de ciberdelitos, sugiriendo capacitaciones en el uso de nuevas herramientas para su combate, lo cual contribuirá al fortalecimiento de las capacidades y habilidades de los sectores y entidades involucrados.

BIBLIOGRAFÍA

¿Qué es ALTERACIÓN? Recuperado el 24 de octubre de 2018 de https://espanol.thelawdictionary.org/alteracion/

Acuerdo Nacional. (2017). Sesión 123: Entrega formal de la política de Estado 35 – "Sociedad de la Información y Sociedad del Conocimiento". Recuperado de http://acuerdonacional.pe/2017/08/sesion-123-entrega-formal-de-la-politica-de-estado-35/

Alanya, W. (2017). Efectos de la Revolución Digital: Delitos Informáticos [diapositivas de PowerPoint]. Recuperado de https://es.slideshare.net/WalterEdisonAlanyaFlores

Applesfera. (2016). Apple recompensará a quienes encuentren fallos de seguridad en sus sistemas. Recuperado de https://www.applesfera.com/apple-1/apple-recompensara-a-quienes-encuentren-fallos-de-seguridad-en-sus-sistemas

Arias, J., Aristizábal, C. (2011). El dato, la información, el conocimiento y su productividad en empresas del sector público de Medellín. Semestre Económico. 14 (28), 98.

BBC. (2017). NHS 'could have prevented' WannaCry ransomware attack. Recuperado de https://www.bbc.com/news/technology-41753022

BID. (2016). Ciberseguridad ¿Estamos preparados en América Latina y el Caribe? Informe Ciberseguridad 2016. Recuperado de https://publications.iadb.org/handle/11319/7449?locale-attribute=es

Bueno, F. (2014). Prueba Electrónica y Proceso 2.0. Valencia. tirant lo Blanch

Callegari, N. (1985). Delitos Informáticos y Legislación. Revista de la Facultad de Derecho y Ciencias Políticas. 70, 115.

CCI. (2017). La Ciberseguridad Industrial en el Perú. Recuperado de https://www.cci-es.org/web/cci/detalle-pais/-/journal_content/56/10694/301898

CDI. (1999). Anual de la Comisión de Derecho Internacional Volumen II Segunda Parte. Recuperado de http://legal.un.org/ilc/publications/yearbooks/spanish/ilc_1999_v2_p2.pdf

CEPAL. (2015). Agenda Digital para América Latina y el Caribe (eLAC2018). Recuperado de https://repositorio.cepal.org/bitstream/handle/11362/38886/1/S1500758_es.pdf

Clarke, R. & Knake (2011). Guerra en la red, los nuevos campos de batalla. Barcelona. Editorial Planeta.

COE. (2001a). Convenio de Budapest sobre la Ciberdelincuencia. Budapest, Hungría, 23 de septiembre de 2001.

COE. (2001b). Informe explicativo Convenio sobre la Ciberdelincuencia. Recuperado de https://rm.coe.int/16802fa403

COE. (s.f.a). Chart of signatures and ratifications of Treaty 185. Recuperado el 01 de noviembre de 2018 de https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=KcsCsxd3

COE. (s.f.b). Reservations and Declarations for Treaty No.185 - Convention on Cybercrime. Recuperado el 01 de noviembre de 2018 de https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/declarations?p_auth=KcsCsxd3

COE. (s.f.c). *Five years validity of an invitation to sign and ratify or to accede to the Council of Europe's treaties*. Recuperado el 01 de noviembre de 2018 de https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016806cac22

Concepto de destrucción. (s.f.). Recuperado el 24 de octubre de 2018 de https://deconceptos.com/general/destruccion

Congreso. (1992). Manual del Proceso Legislativo. Lima, septiembre de 2012.

Congreso. (1993). Constitución Política del Perú. (1993). Lima, Perú, 29 de diciembre de 1993.

Congreso. (2007). Ley N°29158, Ley Orgánica del Poder Ejecutivo. Lima, 20 de diciembre de 2007.

Congreso. (2013). Ley 30096, Ley de Delitos informáticos. Diario Oficial El Peruano. Lima, Perú, 22 de octubre de 2013.

Congreso. (2014). Ley 30171, Ley que modifica la Ley 30096, Ley de Delitos informáticos. Diario Oficial El Peruano. Lima, Perú, 10 de marzo de 2014.

Deloitte. (2016). Encuesta 2016 sobre Tendencias de Ciber-Riesgos y

Seguridad de la Información en Latinoamérica. Recuperado de https://www2.deloitte.com/.../Deloitte/.../Deloitte%202016%20Cyber%20Risk%20%20...

El Tiempo. (2018). Colombia, a un paso del Convenio de Budapest ¿Por qué es importante? Recuperado de https://www.eltiempo.com/tecnosfera/novedades-tecnologia/congreso-aprobo-ley-de-adhesion-al-convencion-de-budapest-234264

Falsificación. (2014). Recuperado el 24 de octubre de 2018 de http://www.enciclopedia-juridica.biz14.com/d/falsificaci%C3%B3n/falsificaci%C3%B3n.htm

FBI. (2014). A Byte Out of History. $10 Million Hack, 1994-Style. Recuperado de https://www.fbi.gov/news/stories/a-byte-out-of-history-10-million-hack

García, F., Jeldres, A., Mardones, M. (2007). Conducta del consumidor y Piratería en la Industria Musical (Tesis de pregrado). Universidad de Chile. Santiago de Chile.

Garnica, C. (2011). Reservas y declaraciones interpretativas de los tratados internacionales. Recuperado de http://cijfldm.blogspot.com/2011/11/reservas-y-declaraciones.html

Gestión. (2017). Perú registrará US$ 4,782 millones en pérdidas por ciberdelitos en 2017. Recuperado de https://gestion.pe/tecnologia/peru-registrara-us-4-782-millones-perdidas-ciberdelitos-2017-141411

Google. (s.f.). Project Zero. Recuperado el 24 de octubre de 2018 de https://googleprojectzero.blogspot.com/

IIBI UNAM. (s.f.) Diferencia entre dato, información y conocimiento. Recuperado el 24 de octubre de 2018 de http://iibi.unam.mx/voutssasmt/documentos/dato%20informacion%20conocimiento.pdf

ITU. (2014). Comprensión del Ciberdelito: Fenómenos, Dificultades y Respuesta Jurídica. Recuperado de https://www.itu.int/en/ITU-D/Cybersecurity/Documents/Cybercrime2014_S.pdf

Kienyke. (2017). Así le robaron cibernéticamente $700 millones a un banco. Krimen y Korrupción. Recuperado de https://www.kienyke.com/krimen/asi-fue-el-robo-de-700-millones-de-pesos-a-un-banco-colombiano

López, B. (s.f.). Piratería. Compilación para la materia Computación. Universidad Nacional de la Patagonia Austral. Río Gallegos.

Martínez, L., Leyva, M., Félix, L., Cecenas, P., Ontiveros, V. (2014). Recuperado de http://www.upd.edu.mx/PDF/Libros/Ciberespacio.pdf

Mehan, J. (2014). CyberWar, CyberTerror, CyberCrime and CyberActivism, 2nd Edition. Londres. IT Governance Publishing.

MINJUSDH, (2009). Decreto Supremo Nº 001-2009-JUS “Reglamento que establece disposiciones relativas a la publicidad, publicación de ProyectosNormativos y difusión de Normas Legales de Carácter General”. Lima, 15 de enero de 2009.

Morgan, S. (2016a). Cyber Crime Costs Projected To Reach $2 Trillion by 2019. Recuperado de https://www.forbes.com/sites/stevemorgan/2016/01/17/cyber-crime-costs-projected-to-reach-2-trillion-by-2019/#7eea15993a91

Morgan, S. (2016b). Cybercrime Damages $6 Trillion By 2021. Cybersecurity Ventures. Recuperado de https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/

Morgan, S. (2017). *Cybercrime Report 2017*. Cybersecurity Ventures. Recuperado de https://cybersecurityventures.com/2015-wp/wp-content/uploads/2017/10/2017-Cybercrime-Report.pdf

MRE. (2010). Reglamento de Organización y Funciones del Ministerio de Relaciones Exteriores. Lima, 18 de diciembre de 2010.

MRE. (2013a). Directiva N° 002-DGT/RE-2013 “Lineamientos Generales sobre la suscripción, perfeccionamiento y registro de los Tratados”. Lima, Perú, 06 de marzo de 2013.

MRE. (2017). Nota Informativa 339-17 El Perú se encuentra ad portas de ser parte del Convenio de Budapest sobre Ciberdelincuencia. Recuperado de www.rree.gob.pe/SitePages/noticia_informativa.aspx?id=NI-339-17

Novak, F., García-Corrochano, L. (2016). Derecho Internacional Público. Tomo I: Introducción y fuentes. Lima. Thomson Reuters.

OEA. (2018). Critical Infrastructure Protection in Latin América and the Caribbean 2018. Recuperado de https://www.oas.org/es/sms/cicte/cipreport.pdf

ONU. (s.f.). Declaraciones y Reservas de la Convención de Viena sobre el Derecho de los Tratados. Recuperado de https://treaties.un.org/pages/ViewDetailsIII.aspx?src=TREATY&mtdsg_no=XXIII-1&chapter=23&Temp=mtdsg3&clang=_en#EndDec

ONU. (1996). Convención de Viena sobre el derecho de los tratados. Recuperado de https://www.oas.org/36ag/espanol/doc_referencia/convencion_viena.pdf

ONU. (2010). Resolución Asamblea General 64/211. Creación de una Cultura Global de Ciberseguridad y Análisis de los Esfuerzos Nacionales para Proteger las Infraestructuras de Información Críticas. Recuperado de http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/64/211&Lang=S

ONU. (2018). Biblioteca ¡Pregunta a DAG! Dag Hammarskjold. Recuperado el 17 de octubre de 2018 de http://ask.un.org/es/faq/65354

PCM. (2011). Aprueban el “Plan de Desarrollo de la Sociedad de la Información en el Perú La Agenda Digital 2.0”. Recuperado de http://www2.congreso.gob.pe/sicr/cendocbib/con4_uibd.nsf/ED55672B8B71A5EF05257C22005806F7/$FILE/AgendaDigital20_28julio_2011.pdf

PCM. (2013). Una Morada al Gobierno Electrónico en el Perú. La oportunidad de acercar el Estado a los ciudadanos a través de las TIC. Recuperado de http://www2.congreso.gob.pe/sicr/cendocbib/con4_uibd.nsf/0D6D8CA5D781070305257E9200775428/$FILE/3_pdfsam_libro_ongei.pdf

RPP. (2018). Hackeo: Bancos asumirán pérdidas de clientes ante ciberataques. Recuperado de https://rpp.pe/economia/economia/hackeo-bancos-asumirian-perdidas-de-clientes-ante-ciberataques-noticia-1144474

Sánchez, M. (2011). Infraestructuras Críticas y Ciberseguridad. Recuperado de https://manuelsanchez.com/2011/07/06/infraestructuras-criticas-y-ciberseguridad/

Sarachaga, A. (2017). Privacidad desde una perspectiva internacional: Introducción. Recuperado de https://blogs.deusto.es/master-informatica/privacidad-introduccion/

SEGDI. (2018a). Resolución de Secretaría de Gobierno Digital Nº 001-2018-PCM/SEGDI “Aprueban Lineamientos para uso de servicios en la nube para entidades de la Administración Pública del Estado Peruano”. Lima, 12 de enero de 2018

SEGDI. (2018b). Resolución Ministerial Nº 119-2018-PCM “Disponen la creación de un Comité de Gobierno Digital en cada entidad de la Administración Pública”. Lima, 10 de mayo de 2018.

SEGDI. (2018c). Decreto Supremo Nº 050-2018-PCM “Aprueban la definición de Seguridad Digital en el Ámbito Nacional”. Lima, 15 de mayo de 2018.

SEGDI. (2018d). Decreto Legislativo Nº 1412 “Decreto Legislativo que aprueba la Ley de Gobierno Digital”. Lima, 13 de septiembre de 2018.

The Sun. (2017). *ATTACK OF THE HACK Five of the worst cases of cybercrime the world has ever seen – from data theft of one BILLION Yahoo users to crippling the NHS.* Recuperado de https://www.thesun.co.uk/tech/4120942/five-of-the-worst-cases-of-cyber-crime-the-world-has-ever-seen-from-data-theft-of-one-billion-yahoo-users-to-crippling-the-nhs/amp/

Thil, E. (2010). VI Congreso argentino de administración Pública. Recuperado de http://www.asociacionag.org.ar/pdfcap/6/THILL_EDUARDO_ACERCANDO.pdf

Trettenero, G. (2017). La ciberdelincuencia, una amenaza para la banca de América Latina. Recuperado de https://www.bbva.com/es/ciberdelincuencia-amenaza-banca-america-latina/

Villavicencio, F. (2014). *Cybercrimes*. Revista IUS ET VERITAS. 49, 286-287.

What is Confidential Data? (s.f.). Recuperado el 24 de octubre de 2018 de https://iso.iowa.gov/faq/what-confidential-data

Torres, R. (2005). Sociedad de la Información / Sociedad del Conocimiento. http://www.ub.edu/prometheus21/articulos/obsciberprome/socinfsoccon.pdf

ANEXOS

Anexo 1: Los Estados Parte del Convenio de Budapest sobre la Ciberdelincuencia

Los Estados miembros del Consejo de Europa

Estado	Firma	Ratificación	Entrada en Vigor
Albania	23/11/2001	20/06/2002	01/07/2004
Andorra	23/04/2013	16/11/2016	01/03/2017
Armenia	23/11/2001	12/10/2006	01/02/2007
Austria	23/11/2001	13/06/2012	01/10/2012
Azerbaiyán	30/06/2008	15/03/2010	01/07/2010
Bélgica	23/11/2001	20/08/2012	01/12/2012
Bosnia y Herzegovina	09/02/2005	19/05/2006	01/09/2006
Bulgaria	23/11/2001	07/04/2005	01/08/2005
Croacia	23/11/2001	17/10/2002	01/07/2004
Chipre	23/11/2001	19/01/2005	01/05/2005
República Checa	09/02/2005	22/08/2013	01/12/2013
Dinamarca	22/04/2003	21/06/2005	01/10/2005
Estonia	23/11/2001	12/05/2003	01/07/2004
Finlandia	23/11/2001	24/05/2007	01/09/2007
Francia	23/11/2001	10/01/2006	01/05/2006
Georgia	01/04/2008	06/06/2012	01/10/2012
Alemania	23/11/2001	09/03/2009	01/07/2009
Grecia	23/11/2001	25/01/2017	01/05/2017
Hungría	23/11/2001	04/12/2003	01/07/2004
Islandia	30/11/2001	29/01/2007	01/05/2007
Italia	23/11/2001	05/06/2008	01/10/2008
Letonia	05/05/2004	14/02/2007	01/06/2007
Liechtenstein	17/11/2008	27/01/2016	01/05/2016
Lituania	23/06/2003	18/03/2004	01/07/2004
Luxemburgo	28/01/2003	16/10/2014	01/02/2015
Malta	17/01/2002	12/04/2012	01/08/2012
Mónaco	02/05/2013	17/03/2017	01/07/2017
Montenegro	07/04/2005	03/03/2010	01/07/2010
Países Bajos	23/11/2001	16/11/2006	01/03/2007

Noruega	23/11/2001	30/06/2006	01/10/2006
Polonia	23/11/2001	20/02/2015	01/06/2015
Portugal	23/11/2001	24/03/2010	01/07/2010
República de Moldavia	23/11/2001	12/05/2009	01/09/2009
Rumania	23/11/2001	12/05/2004	01/09/2004
Serbia	07/04/2005	14/04/2009	01/08/2009
República Eslovaca	04/02/2005	08/01/2008	01/05/2008
Eslovenia	24/07/2002	08/09/2004	01/01/2005
España	23/11/2001	03/06/2010	01/10/2010
Suiza	23/11/2001	21/09/2011	01/01/2012
República de Macedonia	23/11/2001	15/09/2004	01/01/2005
Turquía	10/11/2010	29/09/2014	01/01/2015
Ucrania	23/11/2001	10/03/2006	01/07/2006
Reino Unido	23/11/2001	25/05/2011	01/09/2011

Fuente: Consejo de Europa
Elaboración: Propia
Fecha de revisión: 11/09/2018

Los Estados no miembros del Consejo de Europa

Estado	Firma	Ratificación	Entrada en Vigor
Argentina		05/06/2018 a	01/10/2018
Australia		30/11/2012 a	01/03/2013
Cabo Verde		19/06/2018 a	01/10/2018
Canadá	23/11/2001	08/07/2015	01/11/2015
Chile		20/04/2017 a	01/08/2017
Costa Rica		22/09/2017 a	01/01/2018
Dominica		07/02/2013 a	01/06/2013
Israel		09/05/2016 a	01/09/2016
Japón	23/11/2001	03/07/2012	01/11/2012
Mauricio		15/11/2013 a	01/03/2014
Marruecos		26/06/2018 a	01/10/2018
Panamá		05/03/2014 a	01/07/2014
Paraguay		30/07/2018 a	01/11/2018
Filipinas		28/03/2018 a	01/07/2018
Senegal		16/12/2016 a	01/04/2017
Sri Lanka		29/05/2015 a	01/09/2015

Tonga		09/05/2017 a	01/09/2017
Estados Unidos	23/11/2001	29/09/2006	01/01/2007

Fuente: Consejo de Europa
Elaboración: Propia
Fecha de revisión: 11/09/2018
(a): Adhesión

Anexo 2: Las declaraciones de los Estado Parte al momento de ratificar o adherirse al Convenio

Artículo 2 – Acceso ilícito

Estado	Declaración
Alemania	El elemento adicional de comisión por las medidas de seguridad infractoras se incluye como un elemento del delito de espionaje de datos.
Bélgica	Solo considerado delito si la acción se realiza con intención de defraudar o causar daño.
Canadá	Se requerirá que la ofensa sea cometida con una intención deshonesta.
Chile	Se requerirá que el delito sea cometido con una intención criminal.
Estados Unidos	De conformidad con la legislación de los Estados Unidos, los delitos enunciados incluyen un requisito adicional de la intención de obtener datos informáticos.
Finlandia	requiere para la punibilidad del acceso ilegal que el delito se cometa al infringir medidas de seguridad.
Japón	Se requiere que las infracciones se cometan al infringir medidas de seguridad y en relación con un sistema informático conectado a otro sistema informático.
Lituania	La responsabilidad penal se produce al acceder a la totalidad o en parte de un sistema informático sin derecho, al infringir las medidas de seguridad de una computadora o una red informática.
República Checa	La responsabilidad penal se produce al infringir las medidas de seguridad para obtener acceso no autorizado a la totalidad o parte de un sistema informático.
República Eslovaca	Puede exigir un elemento adicional en el sentido del artículo 2 del Convenio, y que la responsabilidad penal del acceso ilegal exige que el delito se cometa al infringir medidas de seguridad con la intención de obtener datos u otra intención deshonesta, o en relación con un sistema informático que está conectado a otro sistema informático.

Suiza	Aplicará si el delito es cometido infringiendo medidas de seguridad.
Turquía	Se requiere que los delitos se cometan infringiendo medidas de seguridad, con la intención de obtener datos de la computadora u otro intento deshonesto, o en relación con un sistema informático que está conectado a otro sistema informático.

Artículo 3 – Interceptación ilícita

Estado	Declaración
Chile	Se requerirá que el delito sea cometido con una intención criminal.
Japón	Se requiere que los delitos se cometan en relación con un sistema informático que está conectado a otro sistema informático, y que, además, se cometa con intención deshonesta.
Suiza	Aplicará si el delito es cometido con la intención de enriquecimiento ilícito.

Artículo 4.2 – Ataque a la integridad de los datos

Estado	Declaración
Lituania	La responsabilidad penal se produce si los actos resultan en daños graves.

Artículo 6 – Abuso de dispositivos

Estado	Declaración
Estados Unidos	Bajo la ley de los Estados Unidos, la ofensa establecida en el párrafo (1) (b) del Artículo 6 ("Uso indebido de dispositivos") incluye el requisito de poseer un número mínimo de artículos. El número mínimo será el mismo que el establecido por la ley federal aplicable de los Estados Unidos.
Georgia	La responsabilidad penal por los actos previstos en el artículo 6, párrafo 1, a) puede imponerse cuando un dispositivo, incluido un programa informático, está diseñado o puede adaptarse para la realización de actos en virtud de los artículos 2 a 5 del Convenio.

Artículo 7 – Falsificación informática

Estado	Declaración
Alemania	El elemento adicional de un "intento de defraudar, o una intención deshonesta similar" que toma la forma de engaño en transacciones legales, se incluye como un elemento del delito de falsificación de datos legalmente relevantes.

Bélgica	Solo considerado delito si la acción se realiza con intención de defraudar o causar daño.
Chile	Se requerirá que el delito sea cometido con una intención criminal
Estados Unidos	De conformidad con la legislación de los Estados Unidos, el delito previsto en el Artículo 7 ("Falsificación relacionada con computadoras") incluye un requisito de intención de defraudar.
Suiza	Únicamente en la medida en que el delito se cometa con el fin de proporcionar un beneficio a uno mismo o a un tercero o causar daños y perjuicios.
Turquía	La ofensa establecida respecto a la falsificación relacionada con la computadora requiere un intento de defraudar o una intención deshonesta similar bajo la Ley turca.

Artículo 9 – Delitos relacionados a con la pornografía infantil

Estado	Declaración
Suiza	Considera por el término “menor” a cualquier persona menor a dieciséis años.

Artículo 10 – Delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines

Estado	Declaración
Costa Rica	No habrá pena si el uso de derechos de autor de obras obtenidas por sistemas informáticos tienen fines de ilustración para la enseñanza, siempre que dicho uso se haga de acuerdo con un uso adecuado.

Artículo 21 – Interceptación de datos relativos al contenido

Estado	Declaración
Francia	Aplicará las disposiciones contenidas solo si el delito perseguido se castiga con una privación de libertad superior o igual a dos años de prisión preventiva.

Artículo 24.5 – Denegación de extradición

Estado	Declaración
Costa Rica	No se extraditará a un nacional costarricense que se encuentre en territorio de Costa Rica.
Portugal	• No concederá la extradición de personas que:

	a) deben ser juzgados por un tribunal excepcional o deben cumplir una sentencia dictada por dicho tribunal; b) se haya demostrado estarán sujetos a un juicio que no ofrece garantías jurídicas de procedimientos penales que cumplan las condiciones internacionalmente reconocidas como esenciales para la protección de los derechos humanos, o cumplirán sus condenas en condiciones inhumanas; c) están siendo demandadas en relación con una ofensa castigada con una sentencia de por vida o una orden de detención de por vida. • Se concederá la extradición solo por delitos punibles con pena de privación de libertad superior a un año. • No se concederá la extradición de nacionales portugueses. • No se concederá la extradición por delitos punibles con la pena de muerte en virtud de la legislación del Estado requirente. • Se autoriza el tránsito a través de su territorio nacional únicamente respecto de las personas cuyas circunstancias sean tales que permita su extradición.

Artículo 24.7 – Confirmación de la autoridad responsable de enviar o recibir demandas de extradición o de detención provisional en ausencia de tratado y su dirección

Estado	Autoridad Responsable	Dependencia
Albania	Ministerio de Justicia	-
Alemania	Oficina Federal de Relaciones Exteriores	
Andorra	Ministerio de Relaciones Exteriores	Departamento de Asuntos Generales y Legales
Argentina	Ministerio de Asuntos Exteriores y Culto*	-
Armenia	Policía de la República de Armenia	Departamento Principal de Lucha contra el Crimen Organizado
Australia	Departamento del Fiscal General	Autoridad Central de Cooperación Internacional contra el Crimen
Austria	Ministerio Federal de Justicia	División IV 4 Asuntos Penales Internacionales

Azerbaiyán	Ministerio de Justicia	-
Bélgica	Justicia Federal del Servicio Público	Servicio de Cooperación Criminal Internacional
Bosnia y Herzegovina	Ministerio de Seguridad	Agencia Estatal de Investigación y Protección
Bulgaria	Ministerio de Justicia*	-
Cabo Verde	Procuraduría General de la República	Departamento Central de Cooperación y Ley Comparada
Canadá	Departamento de Justicia	Grupo de Asistencia Internacional
Chile	Ministerio de Relaciones Exteriores	-
Costa Rica	Ministerio Público	Oficina de Asesoría Técnica y Relaciones Internacionales, Fiscalía General de la República
Croacia	Ministerio de Justicia	-
Chipre	Ministerio de Justicia y Orden Público	-
Dinamarca	Fiscalía	Director de la Fiscalía
Eslovenia	1. Ministerio de Relaciones Exteriores (extradición)	-
	2. Ministerio del Interior (arresto provicional)	Dirección de la Policía de Investigaciones Criminales, Sección de Cooperación Policial Internacional
España	Ministerio de Justicia	Subdirección General de Cooperación Jurídica Internacional
Estados Unidos	Sin designar (seguirá dependiendo de tratados bilaterales de extradición)	-
Estonia	Ministerio de Justicia	-
Filipinas	Departamento de Justicia	-
Finlandia	1. Ministerio de Justicia (extradición)	-
	2. Oficina Nacional de Investigación (arresto provicional)	
Francia	1. Ministerio de Asuntos Exteriores (extradición)	-
	2. Fiscalía (arresto provicional)	
Georgia	Ministerio de Justicia	-

Grecia	Ministerio de Justicia, Transparencia y Derechos Humanos	Dirección de Trabajo Legislativo, Relaciones Internacionales y Cooperación Judicial Internacional, Departamento de Cooperación Judicial Internacional en Casos Civiles y Criminales
Hungría	La Oficina Central Nacional de Interpol	-
Islandia	Ministerio de Justicia	-
Israel	Ministerio de Justicia	Oficina del fiscal del estado de Israel, Departamento de Asuntos Internacionales
Italia	Ministerio de Justicia	Dirección General de Justicia Criminal
Japón	Ministerio de Relaciones Exteriores	-
Letonia	Fiscalía General	-
Liechtenstein	Ministerio de Justicia	-
Lituania	1. Ministerio de Justicia 2. fiscalía General	-
Luxemburgo	Ministerio de Justicia (extradición)	-
Malta	Ministerio de Justicia	Oficina del Primer Ministro
Mauricio	Oficina del Primer Ministro	-
Monaco	Dirección de Servicios Judiciales	-
Montenegro	Ministerio de Justicia	-
Marruecos	Ministerio de Justicia	Dirección de Asuntos Penales y Gracias
Noruega	1. Real Ministerio de Justicia 2. Policía	-
Países Bajos	Ministerio de Justicia	Oficina de Asistencia Legal Internacional en Asuntos Penales
Panamá	Ministerio de Relaciones Exteriores	Dirección General de Asuntos Jurídicos y Tratados
Paraguay	Ministerio Público	Dirección de Asuntos Internacionales y Cooperación Jurídica Internacional
Polonia	1. Fiscal General ((solicitudes en procedimientos preparatorios)	-

	2. Ministerio de Justicia (otras solicitudes)	
Portugal	Fiscalía General de la República	-
Reino Unido	1. Oficina del Hogar	Unidad de Cooperación Judicial
	2. Gobierno Escocés (cuando se cree que la persona esá en Escocia)	División de Procedimiento Criminal
República Checa	Ministerio de Justicia*	-
República de Macedonia	Ministerio de Justicia	-
República de Moldavia	1. Oficina del Fiscal General (fase de enjuiciamiento penal)	-
	2. Ministerio de Justicia (fase de ejecución del castigo)	
República Dominicana	Procuraduría General de la República	-
República Eslovaca	1. Ministerio de Justicia (extradición y arresto provisional)	-
	2. Oficina del Fiscal Regional (arresto provisional)	
Rumanía	Ministerio de Justicia	-
Senegal	Departamento de Asuntos Penales y Perdón del Ministerio de Justicia	-
Serbia	Ministerio del Interior	Dirección de Policía Criminal, Departamento de Lucha Contra el Crimen Organizado
Sri Lanka	Secretaría del Ministerio de Ley y Orden	-
Suiza	Oficina Federal de Justicia	Departamento Federal de Justicia y Policía
Tonga	Oficina del Fiscal General	Fiscal General Interino y el Director del Ministerio Público
Turquía	Ministerio de Justicia	-

Ucrania	1. Ministerio de Justicia (investigaciones judiciales)	-
	2. Fiscalía General (investigaciones de los órganos de investigación prejudicial)	

*: No confirma dirección

Artículo 27.2 – Confirmación de la autoridad central responsable de enviar o responder solicitudes de asistencia mutua

Estado	Autoridad Responsable	Dependencia
Albania	Ministerio de Justicia	-
Alemania	Ministerio de Relaciones Exteriores	-
Andorra	El Ministerio de Justicia, Asuntos Sociales e Interior	-
Armenia	Policía de la República de Armenia	Departamento Principal de Lucha contra el Crimen Organizado
Australia	Departamento del Fiscal General	Autoridad Central de Cooperación Internacional contra el Crimen
Austria	Ministerio Federal de Justicia	División IV 4 Asuntos penales internacionales
Azerbaiyán	Ministerio de Seguridad Nacional	-
Bélgica	Justicia Federal del Servicio Público	Servicio de cooperación criminal internacional
Bosnia y Herzegovina	Ministerio de Seguridad	Agencia Estatal de Investigación y Protección
Bulgaria	1. Fiscalía Suprema de Casación (etapa pre-juicio) *	-
	2. Ministerio de Justicia (etapa juicio)*	
Cabo Verde	Procuraduría General de la República	Departamento Central de Cooperación y Ley Comparada
Canadá	Departamento de Justicia	Grupo de Asistencia Internacional
Chile	Fiscalía de Chile	Unidad de Cooperación Internacional y Extradición

Costa Rica	Ministerio Público	Oficina de Asesoría Técnica y Relaciones Internacionales, Fiscalía General de la República
Croacia	Ministerio de Justicia	-
Chipre	Ministerio de Justicia y Orden Público	-
Dinamarca	Fiscalía	Director de la Fiscalía
Eslovenia	Ministerio de Justicia	-
España	Ministerio de Justicia	Subdirección General de Cooperación Jurídica Internacional
Estados Unidos	Departamento de Justicia	Oficina de Asuntos Internacionales
Estonia	Ministerio de Justicia	-
Filipinas	Departamento de Justicia	-
Finlandia	Ministerio de Justicia	-
Francia	1. Ministerio de Justicia (envío) 2. Ministerio de Asuntos Exteriores (recepción)	-
Georgia	Ministerio de Justicia	-
Grecia	Ministerio de Justicia, Transparencia y Derechos Humanos	Dirección de Trabajo Legislativo, Relaciones Internacionales y Cooperación Judicial Internacional, Departamento de Cooperación Judicial Internacional en Casos Civiles y Criminales
Hungría	1. Policía Nacional (etapa pre-juicio) * 2. Fiscalía General (etapa juicio)*	-
Islandia	Ministerio de Justicia	-
Israel	Administración de Tribunales	Oficina del Asesor Legal, Asistencia legal al departamento de países extranjeros
Italia	Ministerio de Justicia	Dirección General de Justicia Criminal
Japón	Ministerio de Justicia	1. Oficina de Asuntos Criminales (recepción)

		2. Comisión Nacional de Seguridad Pública (envío)
Letonia	Ministerio de Justicia	-
Liechtenstein	Oficina de Justicia del Principado de Liechtenstein	-
Lituania	1. Ministerio de Justicia	-
	2. fiscalía General	
Luxemburgo	Fiscalía del Gran Ducado de Luxemburgo (solicitudes)	-
Malta	Oficina del Procurador General	-
Mauricio	1. Ministerio de Tecnología de la Información y la Comunicación	-
	2. Autoridad de Tecnologías de la Información y la Comunicación	
	3. Fuerza Policial de Mauricio	
Mónaco	Dirección de Servicios Judiciales	-
Montenegro	Ministerio de Justicia	-
Marruecos	Ministerio de Justicia	Dirección de Asuntos Penales y Gracias
Noruega	Servicio Nacional de Investigación Criminal KRIPOS	División de Delitos de Alta Tecnología
Países Bajos	Oficina Nacional del Ministerio Público	-
Panamá	1. Ministerio de Justicia	Fiscalía de Asuntos Internacionales
	2. Fiscalía Superior Especializada en Delitos Contra la Propiedad Intelectual y Seguridad de la Información	
Paraguay	Ministerio Público	Unidad Especializada de Delitos Informáticos
Polonia	1. Fiscal General ((solicitudes en procedimientos preparatorios)	-
	2. Ministerio de Justicia (otras solicitudes)	
Portugal	Fiscalía General de la República	-
Reino Unido	1. Autoridad Central de Reino Unido (relacionado a Inglaterra, Gales e Irlanda del Norte)	Oficina del Hogar

	2. Unidad de Cooperación Internacional (relacionado a Escocia)	-
	3. División de Aplicación de la Ley y Asesoramiento Internacional	Ingresos y Aduanas HM, Oficina del Procurador
República Checa	1. Fiscalía Suprema	-
	2. Ministerio de Justicia	
República de Macedonia	Ministerio de Justicia	-
República de Moldavia	1. Oficina del Fiscal General (fase de enjuiciamiento penal)	-
	2. Ministerio de Justicia (fase de ejecución del castigo)	
República Dominicana	Procuraduría General de la República	-
República Eslovaca	1. Ministerio de Justicia	-
	2. Oficina del Fiscal General	
Rumanía	1. Fiscalía ante el Tribunal Superior de Casación y Justicia (investigación antes del juicio)	-
	2. Ministerio de Justicia (durante el juicio o ejecución del castigo)	
Senegal	Departamento de Asuntos Penales y Perdón del Ministerio de Justicia	-
Serbia	Ministerio del Interior	Dirección de Policía Criminal, Departamento de Lucha Contra el Crimen Organizado
Sri Lanka	Secretaría del Ministerio de Justicia	-
Suiza	Oficina Federal de Justicia	Departamento Federal de Justicia y Policía
Tonga	Oficina del Fiscal General	Fiscal General Interino y el Director del Ministerio Público
Turquía	Ministerio de Justicia	-
Ucrania	1. Ministerio de Justicia (investigaciones judiciales)	-

	2. Fiscalía General (investigaciones de los órganos de investigación prejudicial)	

*: No confirma dirección

Artículo 27.9.e – Solicitudes dirigidas sobre el párrafo e deben enviarse a la autoridad central

Estado	Autoridad Central
Azerbaiyán	-
Canadá	-
Estados Unidos	-
Georgia	-
Hungría	-
República Checa	-
Japón	-
Liechtenstein	Ministerio de Justicia
Lituania	-
República de Moldavia	Fiscalía General (fase judicial) y Ministerio de Justicia (aplicación del castigo)
Suiza	Departamento Federal de Justicia y Policía

Artículo 29.4 – Exigencia de la doble tipificación penal como condición para atender a una solicitud de asistencia mutua con vistas al registro o al acceso por un medio similar, a la confiscación o a la obtención por un medio similar o a la revelación de los datos almacenados en relación con delitos diferentes de los previstos de conformidad con los artículos 2 a 11

Estado	Declaración
Andorra	Solo si cumple condición al momento de la solicitud.
Austria	Solo si cumple la condición
Japón	se reserva el derecho de rechazar la solicitud de preservación en los casos en que tenga motivos para creer que en el momento de la divulgación no se puede cumplir la condición de doble incriminación.

Lituania	Se reserva el derecho de negarse a ejecutar la solicitud de preservación de los datos en los casos en que haya motivos para creer que, en el momento de la divulgación, el delito en el que se basa la solicitud de preservación de los datos no se considera delito por las leyes de la República de Lituania.

Artículo 35 – Red 24/7

Estado	Autoridad Responsable	Dependencia
Albania	Ministerio del Interior	La Policía del Estado
Alemania	Oficina Federal de la Policía Criminal	La Unidad Nacional de Delitos de Alta Tecnología
Andorra	Departamento de Policía	-
Armenia	Policía de la República de Armenia	Departamento Principal de Lucha contra el Crimen Organizado
Australia	Policía Federal Australiana	Operaciones AOCC Watchfloor
Austria	Ministerio Federal del Interior	Oficina Federal de la Policía Criminal
Azerbaiyán	Ministerio de Seguridad Nacional	-
Bélgica	Sin confirmar	-
Bosnia y Herzegovina	Ministerio de Seguridad	Dirección de cooperación de los cuerpos policiales, Sector de Cooperación Policial Internacional
Bulgaria	Ministerio del Interior	División de delitos informáticos y propiedad intelectual, Dirección General "Lucha contra la Delincuencia Organizada"
Cabo Verde	1. Dirección Nacional de Policía Criminal 2. Departamento Central de Cooperación y Ley Comparada	Oficina de Cooperación Internacional
Canadá	Real Policía Montada de Canadá	-
Chile	Fiscalía de Chile	Unidad de Cooperación Internacional y Extradición
Costa Rica	Autoridad Judicial*	-
Croacia	Ministerio del Interior	1. Dirección General de la Policía

		2. Dirección de la Policía Criminal
		3. Oficina Nacional de Policía para la Represión de la Corrupción y el Crimen Organizado
		4. Departamento de Delincuencia Económica y Corrupción
Chipre	Ministerio de Justicia y Orden Público	-
Dinamarca	Policía Nacional	Departamento Policial
Eslovenia	Ministerio del Interior	Dirección de la Policía de Investigaciones Criminales, Sección de Cooperación Policial Internacional
España	Ministerio del Interior	Comisariado General de la Policía Judicial
Estados Unidos	Departamento de Justicia	Sección de delitos informáticos y propiedad intelectual
Estonia	Consejo de la Guardia de Fronteras y Policía de Estonia	Oficina de Inteligencia Criminal, Departamento de Policía Criminal
Filipinas	Departamento de Justicia	Oficina de Ciberdelincuencia
Finlandia	Oficina Nacional de Investigación	-
Francia	Ministerio del Interior	Dirección Central de la Policía Judicial, Oficina Central de Lucha contra el Delito de las Tecnologías de la Información y las Comunicaciones
Georgia	Ministerio del Interior	Departamento de Policía Criminal
Grecia	Jefatura de Policía Helénica	División de Delitos Cibernéticos
Hungría	Policía Nacional	Centro Internacional para la Implementación de la Cooperación
Islandia	Comisionado Nacional de la Policía de Islandia	-
Israel	Policia de Israel	Mesa de operaciones, Unidad LAHAV 433
Italia	Servicio de policía postal y de comunicaciones	-

Japón	Agencia Nacional de Policía	Departamento de Delincuencia Organizada, División de Operaciones de Investigación Internacional
Letonia	Departamento de la Policía Estatal	Departamento de Cooperación Internacional de la Policía Criminal Central
Liechtenstein	Policiía Nacional	Cooperación Policial Internacional
Lituania	Ministerio del Interior	Departamento de Policía
Luxemburgo	Fiscalía del Tribunal de Distrito de Luxemburgo	-
Malta	Policía de Malta	Unidad de Ciberdelincuencia
Mauricio	Secretario Permanente Adjunto	-
Monaco	Oficina de Interpol	División de Policía Judicial
Marruecos	1. Oficina Central Nacional de Interpol Rabat	Dirección de Policiía Judicial
	2. Presidencia de la Fiscalía General	Polo de Seguimiento de Casos Penales y Protección de Categorías Especiales
Noruega	Servicio Nacional de Investigación Criminal KRIPOS	División de Delitos de Alta Tecnología
Países Bajos	Oficina Nacional del Ministerio Público	-
Panamá	Oficina Central Nacional de Interpol	Unidad de Investigación Judicial
Paraguay	Ministerio Público	Unidad Especializada de Delitos Informáticos
Polonia	Policía General	Oficina de Servicios Criminales, Unidad de Apoyo a la Lucha contra el Delito Cibernético
Portugal	Policía Judicial	-
República Checa	Policía de la República Checa	Sede Nacional del Crimen Organizado, Servicio de Policía Criminal e Investigación, Sección de delito cibernético
República de Macedonia	Oficina del Fiscal	Fiscal Adjunto, Departamento de Lucha contra el Delito y la Corrupción

República de Moldavia	Ministerio del Interior	Dirección de Prevención y Lucha contra los Delitos Cibernéticos, de Información y Transnacionales
República Dominicana	Palacio de la Policía	Departamento de Investigaciones de Crímenes y Delitos de Alta Tecnología de la Policía Nacional
República Eslovaca	Sede Principal de la Policía	Oficina de Cooperación Policial Internacional, Oficina Central Nacional de Interpol
Rumanía	Tribunal Superior de Casación y Justicia	Servicio de lucha contra la ciberdelincuencia, Sección de lucha contra la delincuencia organizada y el tráfico de drogas
Senegal	Policía Nacional	Brigada Especial para Combatir el Delito Cibernético
Serbia	Ministerio del Interior	Dirección de Policía Criminal, Departamento de Lucha Contra el Crimen Organizado
Sri Lanka	Administración Senior DIG	-
Tonga	1. Oficina del Fiscal General	Fiscal General interino y el Director de la Fiscalía Pública / Abogado de la Corona
	2. Sede de la Policía	Comisionado de Policía Adjunto / Comandante Nacional del Crimen
Turquía	Policía Nacional	Departamento de Ciberdelitos

*: No confirma dirección

Artículo 38 – Aplicación territorial

Estado	Declaración
Azerbaiyán	No podrán asegurar el cumplimiento en los territorios ocupados por Armenia hasta que los territorios estén liberados de la ocupación
Dinamarca	Hasta nuevo aviso, la Convención no se aplicará a las Islas Feroe y Groenlandia
Países Bajos	El Reino de los Países Bajos acepta la Convención para el Reino en Europa

República de Moldavia	Las disposiciones de la Convención se aplicarán únicamente en el territorio controlado de manera efectiva por las autoridades de la República de Moldavia.

Artículo 40 – Declaraciones

Estado	Referencia
Alemania	Artículos 2 y 7
Canadá	Artículos 2, 3 y 27
República Checa	Artículo 2
República Eslovaca	Artículo 2
Suiza	Artículos 2, 3, 7, 9
Turquía	Artículos 2 y 7

Otras declaraciones (sin relación a un artículo específico)

- España sobre el escenario donde el Reino Unido le extendiera el Convenio a Gibraltar. El primero considera al último como territorio no autónomo, cuyas relaciones internacionales son responsabilidad de Reino Unido.
- Ucrania sobre la ocupación de Rusia en parte de su territorio nacional, considera que es una violación a la Carta de las Naciones Unidas y amenaza a la paz y seguridad. Le designan responsabilidad total por sus acciones.

Anexo 3: Las reservas de los Estado Parte al momento de ratificar o adherirse al Convenio

Artículo 2 – Acceso ilícito

Estado	Reserva	Vía
Andorra	Incriminará las conductas previstas en el artículo 2 cuando se cometan con intención delictiva para obtener datos sin tener derecho a ellos, para alterar o dañar datos o programas de un sistema informático, o con cualquier otro fin delictivo.	Nota Verbal del Ministerio de Relaciones Exteriores

Artículo 4 – Ataque a la integridad de los datos

Estado	Reserva	Vía
Argentina	Hace una reserva al artículo 29.4 debido a que no es transponible a su jurisdicción porque el requisito de doble incriminación es una de las bases fundamentales de la Ley de Cooperación Internacional en Asuntos Penales.	Instrumento de Adhesión
Austria	Rechazará una solicitud de asistencia mutua para ordenar la conservación de los datos informáticos almacenados, según lo dispuesto en el artículo 16 de la Convención, si no se cumple la condición de doble incriminación; esto no se aplica a los delitos establecidos de conformidad con los artículos 2 al 11.	Instrumento de Ratificación
Azerbaiyán	La responsabilidad penal se produce si los actos resultan en daños graves.	Instrumento de Ratificación
Chile	Se establecerá como delitos de acuerdo con su derecho interno, cuando se cometen intencionalmente, el daño, eliminación, deterioro, alteración o supresión de datos informáticos sin derecho, siempre que esta conducta da como resultado un daño serio.	Instrumento de Adhesión
Estados Unidos	Se reserva el derecho de exigir que la conducta resulte en daños graves, que se determinarán de conformidad con la ley federal aplicable de los Estados Unidos.	Instrumento de Ratificación
Lituania	la responsabilidad penal se produce si los actos descritos en el artículo 4 resultan en daños graves.	Instrumento de Ratificación
República Eslovaca	Se valga del derecho a exigir la responsabilidad penal de la conducta a que se refiere el artículo 4, párrafo 1, que ocasione un daño grave.	Instrumento de Ratificación

Artículo 6 – Abuso de dispositivos

Estado	Reserva	Vía
Andorra	Se reserva el derecho de no aplicar el artículo 6, apartado 1.a, sobre la adquisición de dispositivos de uso y el artículo 6, párrafo 1.b, con respecto a posesión de cualquiera de los artículos mencionados en los subpárrafos a.i o a.ii.	Nota Verbal del Ministerio de Relaciones Exteriores
Argentina	hace una reserva al artículo 6.1.b al no ser transponible a su jurisdicción porque contiene una anticipación de la sanción ya que las acciones preparatorias se establecen como ofensas	Instrumento de Adhesión

	criminales, lo cual es desconocido en la tradición legislativa argentina en materia penal legal asuntos.	
Azerbaiyán	En relación con el subpárrafo "b" del párrafo 1 y el párrafo 3, cuando los actos no se consideran delitos peligrosos para el público en general, serán evaluados no como delitos, sino como actos punibles considerados como una violación de la ley. En caso de que la perpetración deliberada de actos sujetos a la pena de riesgo que no son tratados como delitos peligrosos para el público en general (acción o inacción) genere un daño grave, entonces se los trata como delito.	Instrumento de Ratificación
Chile	No aplicará el párrafo 1 en la medida en que no afecte a la venta, distribución o puesta a disposición de los artículos mencionados en el párrafo 1 a) ii) del presente artículo.	Instrumento de Adhesión
Estados Unidos	Se reserva el derecho de no aplicar los párrafos 1.a.i y 1.b del Artículo 6 ("Uso indebido de dispositivos") con respecto a dispositivos diseñados o adaptados principalmente con el propósito de cometer los delitos establecidos en Artículo 4 ("Interferencia de datos") y Artículo 5 ("Interferencia del sistema").	Instrumento de Ratificación
Israel	De conformidad con el artículo 6, párrafo 3, y el artículo 42, se reserva el derecho de no aplicar: 1) El artículo 6, párrafo 1, cuando el delito se refiere a la contratación para su uso o importación, ya que se refieren al artículo 6, párrafos 1.a.i y 1.a.ii. 2) El artículo 6, párrafo 1.b, relativo a la posesión de los artículos designados en el párrafo 1.a.ii.	Instrumento de Adhesión

Japón	se reserva el derecho de no aplicar el artículo 6, párrafo 1, a excepción de: a) las ofensas establecidas en el artículo 168-2 (Creación de registros electromagnéticos de comandos no autorizados) o el artículo 168-3 (Obtención de registros electromagnéticos de comandos no autorizados) del Código Penal (Ley No. 45, 1907); b) los delitos establecidos en el artículo 4 (Prohibición de actos de obtención no autorizada del código de identificación de otra persona), artículo 5 (Prohibición de actos de facilitación de acceso no autorizado a computadoras) o artículo 6 (Prohibición de actos de almacenamiento no autorizado del codigo de identificación de otra persona) de la Ley sobre la prohibición del acceso no autorizado a computadoras (Ley No. 128, 1999).	Instrumento de Aprobación
Noruega	Se reserva el derecho de no aplicar el artículo 6, párrafo 1.	Instrumento de Ratificación
Sri Lanka	Se reserva el derecho de no aplicar el párrafo 1 del Artículo 6, con la excepción del párrafo 1.a.ii.	Instrumento de Adhesión
Suiza	Se reserva el derecho de aplicar el Artículo 6, párrafo 1, solo cuando la infracción se refiere a la venta, distribución o cualquier otra disposición de los artículos mencionados en el Artículo 6, párrafo 1 a.ii.	Instrumento de Ratificación
Ucrania	Se reserva el derecho de no aplicar el párrafo 1 del artículo 6 relativo al establecimiento de responsabilidad penal por la producción, adquisición para el uso y de otra manera poner a disposición para el uso de los objetos designados en el subpárrafo 1.a.i, y también la producción y adquisición para uso de los objetos designados en el subpárrafo 1.a.ii del Artículo 6.	Instrumento de Ratificación

Artículo 9 – Delitos relacionados a con la pornografía infantil

Estado	Reserva	Vía
Andorra	Se reserva el derecho de no aplicar el artículo 9, párrafo 2.b, relacionado con una persona que parezca ser un menor involucrada en una conducta sexualmente explícita, y también el derecho a no aplicar el artículo 9, párrafo 2.c, relacionado	Nota Verbal del Ministerio de Relaciones Exteriores

	con imágenes realistas que representen un menor involucrado en una conducta sexualmente explícita.	
Argentina	Hace una reserva a los artículos 9.1.d, 9.2.b y 9.2.c debido a que no son transferibles a su jurisdicción porque contienen supuestos anticipatorios incompatibles con el Código Penal en vigor y con el artículo 9.1.e porque solo es aplicable cuando el propósito manifiesto de la posesión en cuestión es la distribución o comercialización.	Instrumento de Adhesión
Chile	No se aplicará el párrafo 2, subpárrafos b y c del presente artículo.	Instrumento de Adhesión
Dinamarca	la zona delictiva de conformidad con el artículo 9 no comprenderá: 1) la posesión de imágenes obscenas de una persona que haya cumplido los 15 años, si la persona en cuestión ha dado su consentimiento a la posesión, (artículo 9, párrafo 1, letra e). 2) las representaciones visuales de una persona que parezca ser un menor involucrado en una conducta sexualmente explícita,(artículo 9, párrafo 2, letra b)	Instrumento de Ratificación
Estados Unidos	Se reserva el derecho de aplicar los párrafos 2.b y 2.c del artículo 9 solo en la medida compatible con la Constitución de los Estados Unidos según lo interpretado por los Estados Unidos y según lo dispuesto en su ley federal, que incluye, para ejemplo, delitos de distribución de material considerado obsceno bajo las normas aplicables de los Estados Unidos.	Instrumento de Ratificación
Francia	Se aplicará el artículo 9, párrafo 1, a cualquier material pornográfico que represente visualmente a una persona que parezca ser un menor que participa en una conducta sexualmente explícita, en la medida en que no se pruebe que dicha persona tenía 18 años el día de la fijación o el registro de su imagen.	Instrumento de Aprobación
Hungría	Se reserva el derecho de no aplicar el artículo 9, párrafo 2, inciso b.	Instrumento de Ratificación
Israel	De conformidad con el artículo 9, párrafo 4, y el artículo 42, se reserva el derecho de no aplicar: 1) El artículo 9, párrafo 2.b. 2) El artículo 9, párrafo 1.d.	Instrumento de Adhesión

Japón	Se reserva el derecho de no aplicar el artículo 9, párrafo 1.d y e, y el párrafo 2.b y c, a excepción de los delitos establecidos en el artículo 7 (Prestación de pornografía infantil y otras actividades relacionadas) de la Ley de Castigo de las Actividades Relacionadas a la prostitución infantil y la pornografía infantil, y la protección de los niños (Ley Nº 52, 1999).	Instrumento de Aprobación
Montenegro	De conformidad con el artículo 9, párrafo 4, y con respecto al artículo 9: a) párrafo 1, artículo e, la obtención de pornografía infantil a través de sistemas informáticos para uno mismo y otras personas y posesión de pornografía infantil en sistemas informáticos o en medios para almacenar datos informáticos no se considerarán delitos en caso de que la persona expuesta en estos materiales cumpliera los catorce años de edad y le entregara consentimiento. b) párrafo 2, artículo b, los materiales que presenten visualmente la cara mediante los cuales pueda concluirse que la persona es menor de edad involucrada en un acto explícito según lo establecido en el artículo 9, párrafo 2, inciso b, no se considerarán pornografía infantil.	Instrumento de Ratificación
Reino Unido	Se reserva el derecho de no aplicar el Artículo 9.2.b, que establece que "pornografía infantil" incluye "una persona que parece ser un menor dedicada a una conducta sexualmente explícita", ya que esta disposición es incompatible con el derecho interno con respecto a fotografías indecentes de niños. Adicionalmente se reserva también el derecho de no aplicar el artículo 9.2.c debido a que Escocia no tiene ningún delito que cubra una imagen "realista" que no es, y no se deriva de, una fotografía de una persona real.	Instrumento de Ratificación
Sri Lanka	Se reserva el derecho de no aplicar los subpárrafos 1 d y e y los subpárrafos 2 b y c.	Instrumento de Adhesión
Suiza	Se reserva el derecho a no aplicar el artículo 9.2.b	Instrumento de Adhesión

Ucrania	Se reserva el derecho de no aplicar en toda su extensión los subpárrafos 1.d y 1.e del Artículo 9.	Instrumento de Ratificación

Artículo 10 – Delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines

Estado	Reserva	Vía
Canadá	Se reserva el derecho de no imponer responsabilidad penal en virtud de los párrafos 1 y 2 del artículo 10, ya que la legislación canadiense dispone de recursos efectivos, como recursos civiles.	Nota Verbal de la Misión de Canadá en la Unión Europea e Instrumento de Ratificación
Estados Unidos	Se reserva el derecho de imponer otros recursos efectivos en lugar de responsabilidad penal según los párrafos 1 y 2 del artículo 10 ("Delitos relacionados con la violación de derechos de autor y derechos conexos") con respecto a infracciones de ciertos derechos de alquiler en la medida en que la penalización de tales infracciones no se requiere de conformidad con las obligaciones que los Estados Unidos han asumido en virtud de los acuerdos a los que se hace referencia en los párrafos 1 y 2.	Instrumento de Ratificación
Israel	Se reserva el derecho de no imponer una responsabilidad penal más amplia que la prevista en el Acuerdo sobre los ADPIC.	Instrumento de Adhesión

Artículo 11 – Tentativa y complicidad

Estado	Reserva	Vía
Andorra	Se reserva el derecho de no aplicar el Artículo 7 con respecto a ciertas formas de intentos de falsificación relacionados con la informática.	Nota Verbal del Ministerio de Relaciones Exteriores
Finlandia	No aplicará el párrafo 2, relativo a la penalización del intento, al daño penal menor ni a la falsificación menor.	Instrumento de Ratificación
Japón	Se reserva el derecho de no aplicar el artículo 11, párrafo 2, a los delitos establecidos de conformidad con el artículo 4, artículo 5, artículo 7 y artículo 9, párrafo 1.a y c, a excepción de los delitos enunciados en el artículo 168-2 (Creación de	Instrumento de Aprobación

	registro electromagnético de comandos no autorizados) o el artículo 234-2 (Obstrucción de negocios al dañar una computadora) del Código Penal.	
Turquía	Se reserva el derecho de establecer jurisdicción dentro del alcance de los artículos 11 y 13 de la Ley penal turca cuando el delito es cometido por un ciudadano turco fuera de su territorio soberano.	Instrumento de Ratificación

Artículo 13 – Sanciones y medidas

Estado	Reserva	Vía
Turquía	Se reserva el derecho de establecer jurisdicción dentro del alcance de los artículos 11 y 13 de la Ley penal turca cuando el delito es cometido por un ciudadano turco fuera de su territorio soberano.	Instrumento de Ratificación

Artículo 14 – Ámbito de aplicación de las disposiciones de procedimiento

Estado	Reserva	Vía
Andorra	Se reserva el derecho de aplicar las medidas previstas en el artículo 20 de la Convención únicamente a los delitos principales definidos en el Código Penal en vigor.	Nota Verbal del Ministerio de Relaciones Exteriores
Australia	se reserva el derecho de aplicar las medidas del artículo 20 solo a los delitos castigados con una pena de prisión de al menos 3 años y cualquier otro 'delito grave' según la legislación interna que rige la recolección y grabación de datos de tráfico en tiempo real y la interceptación de datos de contenido. De conformidad con la legislación australiana, las agencias nacionales solo pueden obtener acceso a los datos de tráfico recopilados y registrados en tiempo real en relación con delitos punibles con pena de prisión de al menos 3 años y otros "delitos graves". Las agencias nacionales solo pueden obtener acceso a datos de contenido interceptado en relación con "delitos graves".	Instrumento de Adhesión
Bulgaria	Se reserva el derecho de aplicar las medidas mencionadas en el artículo 20 solo a los delitos graves, tal como se definen en el Código Penal búlgaro.	Instrumento de Ratificación

Dinamarca	Solo aplicará el artículo 20 relativo al control de los datos de tráfico en la medida en que, de conformidad con el artículo 21, exista la obligación de facultar a las autoridades competentes para controlar los datos de contenido en relación con las investigaciones de delitos graves, según lo define la legislación nacional.	Instrumento de Ratificación
Finlandia	De conformidad con el párrafo 3.a del artículo 14, solo aplicará el artículo 20 a las infracciones cometidas contra un sistema informático cometido por el uso de equipos terminales de telecomunicaciones, el proxenetismo y la amenaza de personas para ser oídas en la administración de la justicia, la amenaza, los delitos de narcóticos o los intentos de los anteriores, la preparación de delitos que se cometan con intención de terrorismo y los delitos punibles con una pena de prisión de al menos cuatro años. De conformidad con el artículo 14, párrafo 3.b, no aplicarán las medidas mencionadas en los artículos 20 y 21 a las comunicaciones que se transmiten dentro de un sistema informático si el sistema funciona en beneficio de un grupo cerrado de usuarios y no emplea redes de comunicaciones públicas y no está conectado con otro sistema de computadora, ya sea público o privado.	Instrumento de Ratificación
Grecia	se reserva el derecho de aplicar las medidas mencionadas en el artículo 20, solo a las infracciones a las que se aplican las medidas mencionadas en el artículo 21.	Instrumento de Ratificación
Israel	Se reserva el derecho de aplicar las medidas mencionadas en el artículo 21 solo a los delitos definidos como delitos graves en la Ley Penal Israelí de 1977.	Instrumento de Adhesión
Liechtenstein	De conformidad con el artículo 14, párrafo 3, se reserva el derecho de aplicar las medidas a que se refiere el artículo 20 solo a los delitos y delitos castigados con penas de prisión de más de un año, tal como se definen en el Código Penal de Liechtenstein.	Instrumento de Ratificación
Montenegro	Las medidas del artículo 20 del Convenio se aplicarán únicamente sobre la base de la decisión de un tribunal	Instrumento de Ratificación

	montenegrino competente, si es necesario para llevar a cabo un procedimiento penal o por razones de seguridad en Montenegro.	
Noruega	se reserva el derecho de no aplicar las medidas a que se refiere el artículo 20 (Recopilación en tiempo real de datos de tráfico) en los casos de delitos menos graves.	Instrumento de Ratificación
Suiza	Se reserva el derecho de aplicar las medidas a que se refiere el artículo 20 a los delitos y delitos contemplados en su Código Penal	Instrumento de Ratificación
Turquía	Se reserva el derecho de no aplicar las medidas mencionadas en el artículo 20 y el artículo 21 a las comunicaciones que se transmiten dentro de un sistema informático si el sistema funciona en beneficio de un grupo cerrado de usuarios y no utiliza redes públicas de comunicaciones y no está conectado con cualquier otro sistema informático público o privado.	Instrumento de Ratificación

Artículo 16 – Conservación rápida de datos informáticos almacenados

Estado	Reserva	Vía
Liechtenstein	De conformidad con el párrafo 4 del artículo 29, rechazará una solicitud de asistencia mutua para ordenar la conservación de los datos informáticos almacenados, según lo dispuesto en el artículo 16 del Convenio, si no se cumple la condición de doble incriminación; esto no se aplica a los delitos establecidos de conformidad con los artículos 2 al 11.	Instrumento de Ratificación

Artículo 20 – Obtención en tiempo real de datos relativos al tráfico

Estado	Reserva	Vía
Liechtenstein	De conformidad con el artículo 14, párrafo 3, se reserva el derecho de aplicar las medidas a que se refiere el artículo 20 solo a los delitos y delitos castigados con penas de prisión de más de un año, tal como se definen en el Código Penal de Liechtenstein.	Instrumento de Ratificación
Montenegro	Las medidas del artículo 20 del Convenio se aplicarán únicamente sobre la base de la decisión de un tribunal montenegrino competente, si es necesario para llevar a cabo un procedimiento penal o por razones de seguridad en Montenegro.	Instrumento de Ratificación

Turquía	Se reserva el derecho de no aplicar las medidas mencionadas en el artículo 20 y el artículo 21 a las comunicaciones que se transmiten dentro de un sistema informático si el sistema funciona en beneficio de un grupo cerrado de usuarios y no utiliza redes públicas de comunicaciones y no está conectado con cualquier otro sistema informático público o privado.	Instrumento de Ratificación

Artículo 21 – Interceptación de datos relativos al contenido

Estado	Reserva	Vía
Turquía	Se reserva el derecho de no aplicar las medidas mencionadas en el artículo 20 y el artículo 21 a las comunicaciones que se transmiten dentro de un sistema informático si el sistema funciona en beneficio de un grupo cerrado de usuarios y no utiliza redes públicas de comunicaciones y no está conectado con cualquier otro sistema informático público o privado.	Instrumento de Ratificación

Artículo 22 - Jurisdicción

Estado	Reserva	Vía
Argentina	No es transponible a su jurisdicción porque su contenido difiere de las reglas que rigen la definición de jurisdicción penal nacional.	Instrumento de Adhesión
Australia	Se reserva el derecho de no aplicar las normas de competencia establecidas en el artículo 22, párrafo 1.bd, a las infracciones establecidas de conformidad con el artículo 7 (Falsificación informática), El artículo 8 (fraude informático) y el artículo 9 (Delitos relacionados con la pornografía infantil). El Parlamento de la Mancomunidad de Australia no cuenta con un poder plenario para promulgar leyes que establezcan infracciones relacionadas con la falsificación de computadoras, fraudes relacionados con la informática o delitos relacionados con la pornografía infantil. El Parlamento de la Mancomunidad de Australia ha establecido infracciones relacionadas con la falsificación informática, fraudes informáticos y delitos relacionados con la pornografía infantil cometidos a bordo de buques que enarbolan banderas australianas, a bordo de aeronaves registradas de conformidad con la legislación australiana o australianos fuera de Australia, donde la conducta ofensiva involucra algún tema con respecto al cual tiene poder	Instrumento de Adhesión

	legislativo. Además de esos delitos, los Estados y Territorios australianos también han tipificado los delitos de conformidad con los artículos 7, 8 y 9 cuando se cometen en su territorio.	
Bélgica	Se reserva la posibilidad de aplicar el artículo 22.1.c del Convenio solo si se cumplen las siguientes condiciones específicas: Artículo 36 de la Ley de 27 de junio de 1937, relativa a la reglamentación de la navegación aérea , considera cometidos en Bélgica los delitos cometidos a bordo de un avión belga en vuelo. Se reserva el derecho de aplicar el artículo 22.1.d de la Convención a un ciudadano belga que sea culpable de un delito cometido fuera del territorio del Reino, solo en los casos en que se considere tal delito ser una ofensa criminal de acuerdo con la ley belga, y el delito es castigado por la ley del país donde fue cometido, y el perpetrador se encuentra en Bélgica. Bélgica se reserva el derecho de iniciar procedimientos, en los casos en que la víctima del delito sea extranjera, solo previa denuncia de la víctima, su familia o un aviso oficial de las autoridades del Estado donde se cometió el delito.	Instrumento de Ratificación
Canadá	Se reserva el derecho de no ejercer su jurisdicción en relación con sus nacionales que cometan delitos establecidos de conformidad con la Convención fuera de su jurisdicción territorial.	Nota Verbal de la Misión de Canadá en la Unión Europea e Instrumento de Ratificación
Chile	No aplicará las reglas de jurisdicción establecidas en el párrafo 1.b del presente artículo.	Instrumento de Adhesión
Estados Unidos	Se reserva el derecho de no aplicar en los párrafos 1b, 1c y 1d de la parte del artículo 22 ("Jurisdicción"). Los Estados Unidos no prevén la jurisdicción plenaria sobre delitos cometidos fuera de su territorio por su ciudadano o a bordo de buques que enarbolen su pabellón o aeronaves registradas conforme a sus leyes. Sin embargo, la legislación de los Estados Unidos prevé la jurisdicción sobre una serie de delitos establecidos en la Convención que se cometen en el extranjero por nacionales de los Estados Unidos en circunstancias que implican intereses federales particulares, así como sobre una serie de delitos cometidos a bordo de los Estados Unidos. buques o aeronaves con pabellón registrado bajo la ley de	Instrumento de Ratificación

	los Estados Unidos. En consecuencia, los Estados Unidos implementarán los párrafos 1b, 1c y 1d en la medida prevista en su legislación federal.	
Francia	Se reserva el derecho de no establecer jurisdicción cuando el delito se comete fuera de la jurisdicción territorial de cualquier Estado. Francia declara también que, siempre que el delito sea punible conforme a la legislación penal cuando se haya cometido, el procedimiento se iniciará únicamente a petición del fiscal y deberá ir precedido de una denuncia de la víctima o sus beneficiarios o de una denuncia oficial. de las autoridades del Estado donde se cometió el acto (artículo 22, párrafo1.d)	Instrumento de Aprobación
Israel	Se reserva el derecho de no aplicar el artículo 22, párrafo 1.d, a menos que el delito sea punible conforme a la ley penal en el país donde se cometió, de conformidad con los límites de la doble incriminación y con la aprobación del Fiscal General de Israel.	Instrumento de Adhesión
Japón	Se reserva el derecho de no aplicar las reglas de jurisdicción establecidas en el artículo 22, párrafo 1.d, a los delitos establecidos de conformidad con el artículo 6, párrafo 1.a.ii, en lo que respecta a los delitos establecidos en el artículo 13 (Prohibición de actos de facilitar el acceso no autorizado a la computadora sin conocer el propósito del acceso no autorizado de la computadora del solicitante) de la Ley de prohibición de acceso no autorizado a computadoras.	Instrumento de Aprobación
Reino Unido	Se reserva el derecho de no aplicar el Artículo 22.1.d. El Reino Unido puede extender la jurisdicción extraterritorial sobre la mayoría de las ofensas en los artículos 2 a 11, aunque no sobre el fraude cometido en Escocia, bajo circunstancias específicas. Como no existe un acuerdo global que extienda la jurisdicción extraterritorial, el Reino Unido no puede decir que se aplicará en todos los casos.	Instrumento de Ratificación

Artículo 29 – Conservación rápida de datos informáticos almacenados

Estado	Reserva	Vía
Argentina	Hace una reserva al artículo 29.4 debido a que no es transponible a su jurisdicción porque el requisito de doble incriminación es una de las bases fundamentales de la Ley de Cooperación Internacional en Asuntos Penales.	Instrumento de Adhesión

Austria	Rechazará una solicitud de asistencia mutua para ordenar la conservación de los datos informáticos almacenados, según lo dispuesto en el artículo 16 de la Convención, si no se cumple la condición de doble incriminación; esto no se aplica a los delitos establecidos de conformidad con los artículos 2 al 11.	Instrumento de Ratificación
Azerbaiyán	Se reserva el derecho de rechazar la solicitud de preservación en virtud de este artículo en los casos en que tenga motivos para creer que en el momento de la divulgación no se puede cumplir la condición de doble incriminación.	Instrumento de Ratificación
Chile	Se reserva el derecho de rechazar la solicitud de asistencia internacional en los casos en que la conducta no esté definida por la legislación chilena en el momento de la solicitud.	Instrumento de Adhesión
Grecia	se reserva el derecho de rechazar una solicitud de preservación en virtud del artículo 29 en los casos en que no se cumpla la condición de doble incriminación.	Instrumento de Ratificación
Israel	En relación a los delitos distintos de los establecidos de conformidad con los artículos 2 a 11, el Estado de Israel se reserva el derecho de rechazar la solicitud de preservación prevista en el artículo 29 en los casos en que tenga motivos para creer que en el momento de la divulgación la condición de doble criminalidad no se puede cumplir.	Instrumento de Adhesión
Letonia	Se reserva el derecho de rechazar la solicitud de preservación en virtud de este artículo en los casos en que tenga motivos para creer que en el momento de la divulgación no se puede cumplir la condición de doble incriminación.	Instrumento de Ratificación
Liechtenstein	De conformidad con el párrafo 4 del artículo 29, rechazará una solicitud de asistencia mutua para ordenar la conservación de los datos informáticos almacenados, según lo dispuesto en el artículo 16 del Convenio, si no se cumple la condición de doble incriminación ; esto no se aplica a los delitos establecidos de conformidad con los artículos 2 al 11.	Instrumento de Ratificación
Lituania	Se reserva el derecho de negarse a ejecutar la solicitud de preservación de los datos en los casos en que haya motivos para creer que, en el momento de la divulgación, el delito en el	Instrumento de Ratificación

	que se basa la solicitud de preservación de los datos no se considera delito por las leyes de la República de Lituania.	
Noruega	Se reserva el derecho de rechazar la solicitud de preservación en virtud de este artículo en los casos en que tenga motivos para creer que en el momento de la divulgación no se puede cumplir la condición de doble incriminación.	Instrumento de Ratificación
Polonia	Se reserva la condición de que la ejecución de una solicitud de asistencia mutua con fines de búsqueda o acceso similar, incautación o afianzamiento similar, o revelación de datos almacenados, con respecto a delitos distintos de los establecidos de conformidad con los artículos 2 a 11, estará condicionado a la doble incriminación de esos delitos.	Instrumento de Ratificación
Reino Unido	Se reserva el derecho de no aplicar el Artículo 29 cuando la ejecución de la solicitud de preservación requiera el ejercicio de poderes coercitivos y cuando no se pueda establecer la doble incriminación.	Instrumento de Ratificación
República Checa	Se reserva el derecho de rechazar una solicitud de preservación en virtud del artículo 29 en los casos en que tenga motivos para creer que la condición de doble incriminación en relación con otros actos criminales distinta de las especificadas en los artículos 2 a 11 no puede cumplirse para ejecutar asistencia mutua para la búsqueda o acceso similar, confiscación o aseguramiento similar, o divulgación de los datos.	Instrumento de Ratificación
República Eslovaca	Se permite el derecho a rechazar la solicitud de preservación en los casos en que tenga motivos para creer que en el momento de la divulgación no se puede cumplir la condición de doble incriminación.	Instrumento de Ratificación
Suiza	Se reserva el derecho a someterse a la condición a que se refiere el artículo 29, párrafo 4, la ejecución de cualquier comisión rogatoria que requiera la aplicación de cualquier medida coercitiva.	Instrumento de Ratificación

Artículo 41 – Cláusula federal

Estado	Reserva	Vía
Estados Unidos	Se reserva el derecho de asumir obligaciones bajo el Capítulo II de una manera consistente con sus principios fundamentales de federalismo.	Instrumento de Ratificación

Artículo 42 - Reservas

Estado	Reserva	Vía
Alemania	a) No se aplicará el artículo 6, párrafo 1.a.i, en lo que se refiere a "dispositivos", y el subpárrafo b, b) el intento de cometer los actos especificados en el artículo 3 no se establecerá como delito con arreglo a la legislación nacional, y c) las solicitudes de preservación acelerada de los datos almacenados en virtud del artículo 29 pueden denegarse debido a que no se otorga la doble incriminación, siempre que haya razones para creer que en el momento de la divulgación no se puede cumplir la condición de doble incriminación, a menos que el delito en cuestión es un delito establecido de conformidad con los artículos 2 a 11.	Instrumento de Ratificación
Azerbaiyán	Referido al artículo 4.	Instrumento de Ratificación
Canadá	Referido al artículo 10 y 22.	Nota Verbal de la Misión de Canadá en la Unión Europea e Instrumento de Ratificación
Estados Unidos	Referido a los artículos 4, 6, 9, 10, 22 y 41	Instrumento de Ratificación
Israel	Referido a los artículos 6, 9, 10, 14, 22 y 29.	Instrumento de Adhesión
Lituania	Referido a los artículos 4 y 29.	Instrumento de Ratificación
Sri Lanka	Referido a los artículos 6 y 9.	Instrumento de Adhesión
Suiza	Referido a los artículos 6, 9, 14 y 29.	Instrumento de Ratificación
República Checa	Referido al artículo 29.	Instrumento de Ratificación
República Eslovaca	Referido a los artículos 4 y 29.	Instrumento de Ratificación

Turquía	Referido a los artículos 11, 13, 14, 20, 21, 22 y 29	Instrumento de Ratificación

Anexo 3 - Cuadro de correlación de artículos del Convenio de Budapest y legislación peruana vigente

Convenio de Budapest	El Perú	Comentarios
Capítulo I - Terminología		
Artículo 1 - Definiciones -Sistema informático, -Datos informáticos, -Proveedor de servicios, -Datos relativos al tráfico	El Código Penal no señala definiciones	Solo describe las conductas punibles y sus correspondientes sanciones.
Capítulo II - Medidas que deberán adoptarse a nivel nacional		
Sección 1 - Derecho penal sustantivo		
Título 1 - Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos		
Artículo 2 - Acceso ilícito	Artículo 2 de la Ley 30096, Ley de delitos informáticos - Acceso ilícito; y su modificatoria en la Ley 30171, Ley que modifica la Ley 30096.	El artículo 2 establece los plazos de pena privativa de libertad y los días multa.
Artículo 3 - Interceptación ilícita	Artículo 7 de la Ley 30096, Ley de delitos informáticos - Interceptación de datos informáticos; y su modificatoria en la Ley 30171, Ley que modifica la Ley 30096.	El artículo 7 establece los plazos de pena privativa de libertad.
Artículo 4 - Ataques a la integridad de los datos	Artículo 3 de la Ley 30096, Ley de delitos informáticos - Atentado a la integridad de datos informáticos; y su modificatoria en la Ley 30171, Ley que modifica la Ley 30096.	El artículo 3 establece plazos de pena privativa de libertad y días-multa.

Artículo 5 - Ataques a la integridad del sistema	Artículo 4 de la Ley 30096, Ley de delitos informáticos - Atentado a la integridad de sistemas informáticos; y su modificatoria en la Ley 30171, Ley que modifica la Ley 30096.	El artículo 4 establece plazos de pena privativa de libertad y días-multa.
Artículo 6 - Abuso de los dispositivos	*Artículo 10 de la Ley 30096, Ley de delitos informáticos - Abuso de mecanismos y dispositivos informáticos; y su modificatoria en la Ley 30171, Ley que modifica la Ley 30096.	*La legislación peruana no sanciona actos preparatorios, pero sí la tenencia ilegal de armas (delito de peligro). La legislación peruana podría incorporar los conceptos del Convenio.
Título 2 - Delitos informáticos		
Artículo 7 - Falsificación informática	La legislación peruana no prevé la figura de falsedad informática, pero se podría incorporar dentro del título de delitos contra la Fe Pública como conducta que utiliza sistemas informáticos.	En la declaración del artículo se hace mención de que se podrá exigir que exista una intención fraudulenta o delictiva similar para generar responsabilidad penal.
Artículo 8 - Fraude informático	Artículo 8 de la Ley 30096, Ley de delitos informáticos - Fraude Informático; y su modificatoria en la Ley 30171, Ley que modifica la Ley 30096.	El artículo 8 establece plazos de pena privativa de libertad y días-multa.
Título 3 - Delitos relacionados con el contenido		
Artículo 9 - Delitos relacionados con la pornografía infantil	Artículo 181-A. del Código Penal - Turismo sexual infantil y Artículo 183-A. del Código Penal - Pornografía Infantil.	Los artículos establecen el tiempo de pena privativa según los casos presentados y tendrán relación con el artículos 36. El artículo 183-A podría tener relación con el artículo 173 del Código Penal según las condiciones del caso.

Título 4 - Delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines		
Artículo 10 - Delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines	Temas en materia de Propiedad intelectual, industrial y de derechos conexos son regulados por la Convención de Roma.	El Código Penal prevé un título de delitos contra la propiedad intelectual y propiedad industrial.
Título 5 - Otras formas de responsabilidad y de sanción		
Artículo 11 - Tentativa y complicidad	El Código Penal trata la tentativa en el Capítulo II de la Parte General (artículos 16 al 19). En relación a la complicidad, está regulado en el Capítulo IV de la Parte General (artículos 23 al 27).	-
Artículo 12 - Responsabilidad de las personas jurídicas	Artículo 27 del Código Penal - Actuación en nombre de otro y Artículo 105 del Código Penal - Medidas aplicables a las personas jurídicas.	El artículo 27 describe los actos que generan responsabilidad penal y el artículo 105 las medidas aplicables como clausura, disolución, liquidación, suspensión, prohibición de actividades, con sus correspondientes plazos.
Artículo 13 - Sanciones y medidas	Artículo 28 del Código Penal - Clases de Pena y Artículo 105 - Medidas aplicables a las personas jurídicas.	El artículo 28 establece cuatro penas aplicables: privativa de libertad, restrictiva de libertad, limitativas de derechos y multa.
Sección 2 - Derecho procesal		
Título 1 - Disposiciones comunes		
Artículo 14 - Ámbito de aplicación de las disposiciones de procedimiento	Sección II del Código Procesal Penal del 2004: La prueba, Título III: La búsqueda de pruebas y restricción de derechos, Capítulo VI: La exhibición forzada y la incautación; y Capítulo VII: El control de las comunicaciones y documentos privados.	El Capítulo VI comprende los actos de Exhibición e incautación de bienes, la exhibición e incautación de actuaciones y documentos no privados.

Artículo 15 - Condiciones y salvaguardias	Artículo VIII del título preliminar del Código Procesal Penal del 2004: Legitimidad de la prueba.	La prueba será valorada solo si fue obtenida e incorporada al proceso por un procedimiento constitucionalmente legítimo.
Título 2 - Conservación rápida de datos informáticos almacenados		
Artículo 16 - Conservación rápida de datos informáticos almacenados	Artículo 221 del Código Procesal Penal - Conservación y exhibición; y Artículo 230 - Intervención o grabación o registro de comunicaciones telefónicas o de otras formas de comunicación.	-
Artículo 17 - Conservación y revelación parcial rápida de los datos relativos al tráfico	-	-
Título 3 - Orden de presentación		
Artículo 18 - Orden de presentación	-	-
Título 4 - Registro y confiscación de datos informáticos almacenados		
Artículo 19 - Registro y confiscación de datos informáticos almacenados	-	-
Título 5 - Obtención en tiempo real de datos informáticos		
Artículo 20 - Obtención en tiempo real de datos relativos al tráfico	Artículo 220 del Código Penal Procesal - Diligencia de secuestro o exhibición y Artículo 230 del Código Penal Procesal - Intervención o grabación o registro de comunicaciones telefónicas o de otras formas de comunicación (numerales 4 y 6)	El artículo 220 establece que un Fiscal determinará con precisión las condiciones y personas que intervendrán, y el artículo 230 que las empresas telefónicas y de telecomunicaciones deberán posibilitar la diligencia de intervención y grabación o registro (numeral 4), con su correspondiente plazo y prórroga (numeral 6).

Artículo 21 - Interceptación de datos relativos al contenido	Artículo 220 del Código Penal Procesal - Diligencia de secuestro o exhibición y Artículo 230 del Código Penal Procesal - Intervención o grabación o registro de comunicaciones telefónicas o de otras formas de comunicación (numerales 1 al 6).	En el caso del artículo 230 se incluyen los numerales 1, 2, 3 y 5 que consideran privación de libertad para proseguir las investigaciones; orden judicial contra el investigado o personas estimadas; resolución judicial; y la interrupción en caso los elementos de convicción desaparecen o transcurre el plazo fijado.
Sección 3 - Jurisdicción		
Artículo 22 - Jurisdicción	Artículo 19 del Código Penal Procesal - Determinación de la competencia.	-
Capítulo III - Cooperación Internacional		
Sección 1 - Principios generales		
Título 2 - Principios relativos a la extradición		
Artículo 24 - Extradición	Artículo 513 del Código Penal Procesal - Procedencia	El artículo establece la posibilidad de ser extraditado para ser juzgado o cumplir una sanción penal, y el procedimiento a aplicar en caso no exista tratado de extradición.
Título 3 - Principios generales relativos a la asistencia mutua		
Artículo 25 - Principios generales relativos a la asistencia mutua	Artículo 508 del Código Penal Procesal - Normatividad aplicable (numeral 1 y 2).	Las relaciones con autoridades extranjeras y con la Corte Penal Internacional se rigen por tratados internacionales o en su defecto, por el Principio de Reciprocidad (numeral 1), y de existir tratado, sus normas regirán el trámite de Cooperación Judicial Internacional (numeral 2).

Artículo 26 - Información espontánea	Artículo 510 del Código Penal Procesal - Competencia del país requirente y ejecución del acto de cooperación (numerales 1 al 3), y Artículo 511 del Código Penal Procesal - Actos de Cooperación Judicial Internacional (numeral 1, incisos a al m; y numeral 2).	El artículo 510 establece la forma de determinación de la competencia del país requirente, el motivo para desestimar una solicitud y la posibilidad de requerimiento de diligencia.
Título 4 - Procedimientos relativos a las solicitudes de asistencia mutua en ausencia de acuerdos internacionales aplicables		
Artículo 27 - Procedimientos relativos a las solicitudes de asistencia mutua en ausencia de acuerdos internacionales aplicables	Artículo 511 del Código Penal Procesal - Actos de Cooperación Judicial Internacional (numeral 1, incisos a al m; y numeral 2).	El artículo 511 establece los actos de Cooperación Judicial Internacional sin perjuicio de lo dispuesto por tratados.
Artículo 28 - Confidencialidad y restricciones de uso	Artículo 511 del Código Penal Procesal - Actos de Cooperación Judicial Internacional (numeral 1, incisos a al m; y numeral 2).	El artículo 511 establece los actos de Cooperación Judicial Internacional sin perjuicio de lo dispuesto por tratados.
Sección 2 - Disposiciones específicas		
Título 1 - Asistencia mutua en materia de medidas provisionales		
Artículo 29 - Conservación rápida de datos informáticos almacenados	Artículo 511 del Código Penal Procesal - Actos de Cooperación Judicial Internacional (numeral 1, incisos a al m; y numeral 2).	El artículo 511 establece los actos de Cooperación Judicial Internacional sin perjuicio de lo dispuesto por tratados.
Artículo 30 - Revelación rápida de datos conservados	Artículo 511 del Código Penal Procesal - Actos de Cooperación Judicial Internacional (numeral 1, incisos a al m; y numeral 2).	El artículo 511 establece los actos de Cooperación Judicial Internacional sin perjuicio de lo dispuesto por tratados.
Artículo 31 - Asistencia mutua en relación con el acceso a datos almacenados	Artículo 511 del Código Penal Procesal - Actos de Cooperación Judicial Internacional (numeral 1, incisos a al m; y numeral 2).	El artículo 511 establece los actos de Cooperación Judicial Internacional sin perjuicio de lo dispuesto por tratados.

Artículo 32 - Acceso transfronterizo a datos almacenados, con consentimiento o cuando sean accesibles al público	Artículo 511 del Código Penal Procesal - Actos de Cooperación Judicial Internacional (numeral 1, incisos a al m; y numeral 2).	El artículo 511 establece los actos de Cooperación Judicial Internacional sin perjuicio de lo dispuesto por tratados.
Artículo 33 - Asistencia mutua en relación con la interceptación de datos relativos al contenido	Artículo 511 del Código Penal Procesal - Actos de Cooperación Judicial Internacional (numeral 1, incisos a al m; y numeral 2).	El artículo 511 establece los actos de Cooperación Judicial Internacional sin perjuicio de lo dispuesto por tratados.
Artículo 34 - Asistencia mutua en relación con la interceptación de datos relativos al contenido	Artículo 511 del Código Penal Procesal - Actos de Cooperación Judicial Internacional (numeral 1, incisos a al m; y numeral 2).	El artículo 511 establece los actos de Cooperación Judicial Internacional sin perjuicio de lo dispuesto por tratados.
Artículo 35 - Red 24/7	El Perú está suscrito a la Red 24/7.	
Capítulo IV - Cláusulas finales		
Artículo 42 - Reservas	-	El tratado establece que los Estados pueden presentar reservas al momento de su adhesión.

Fuente: Comunidad Octupus de Ciberdelincuencia del Consejo de Europa.
Elaboración: Propia