Artículo original

Los cyberdelitos y su incorporación al derecho penal paraguayo
Cybercrimes and their incorporation into Paraguayan criminal law
Ciberdelito kuéra ha ijegueroike ñande derecho penal -pe

Rossana Maldonado Núñez*
https://orcid.org/0000-0003-0730-7227
Poder Judicial. Asunción, Paraguay. Universidad Nacional de Pilar - Instituto de Estudios Comparados en Ciencias Penales y Sociales del Paraguay. Asunción, Paraguay

Resumen

Con el objetivo de conocer el marco normativo que castiga el cyberdelito en Paraguay, se realizó una breve revisión y análisis del desarrollo de las normativas vigentes a nivel nacional, exponiendo los principales conceptos, así como las leyes que protegen los derechos de los ciudadanos. Para ese fin, se optó por una investigación con un enfoque cualitativo de tipo descriptivo, de diseño no experimental; como técnica de recolección de datos se utilizó el análisis documental y como instrumento las fichas bibliográficas. En tal sentido, se puede afirmar que Paraguay con el afán de cumplir con los compromisos internacionales, entre ellas el Convenio de Budapest, ha incluido reformas al Código Procesal Penal, como asimismo, agregó nuevas figuras, desarrolladas en el apartado correspondiente. Sin embargo, hay mucho por Trabajar en materia legislativa para la prevención y la represión al cyberdelito. Por ello, es necesario un acuerdo o pacto social y regional para dar viabilidad y sostenibilidad al nuevo sistema legal en la materia y

Recibido: 08.06.2022 Aprobado: 4/10/2022

*Trabajo realizado en el marco de la Maestría en Garantismo Penal y Derecho Procesal Penal de la Universidad Nacional de Pilar-INECIP.

* Juez Penal de Sentencia de la capital. E-mail: rossanamaldonado@hotmail.com
Abogada (1998). Escribana y Notaria Pública (2002) egresada de la Facultad de Derecho y Ciencias Sociales de la UNA, Máster en Ciencia de la Educación (2018) Universidad Privada del Guairá, Máster en Derecho Penal Económico (2020) UNIR, Máster en Metodología de la Investigación Científica (2021) UNIBE, Estudiante de la maestría en Garantismo Penal y Derecho Procesal. Universidad Nacional del Pilar e INECIP.

ISSN 2415-5063 Versión impresa ISSN 2415-5071 Versión en línea
https://ojs.ministeriopublico.gov.py Contacto: dip.informaciones@ministeriopublico.gov.py

una actualización constante. Se debe resaltar que, con el uso de la tecnología aumentan los delitos que podrían configurar fuera de la definición ordinaria, esto aplicaría también a otros delitos como el hurto o la extorsión, y sin embargo, no se tipifican de forma especial. Los temas vinculados a la ciberseguridad y el cyberdelito requieren de un análisis multidisciplinario e interinstitucional para alcanzar una solución efectiva. Estas acciones deben involucrar además, a comunidades educativas y sociedad civil a fin de, poner en práctica acciones preventivas.

Palabras claves: Cyberdelito, tecnología, respuesta estatal, regulación, Convenio de Budapest.

Abstract

With the aim of knowing the regulatory framework that punishes cybercrime in Paraguay, a brief review and analysis of the development of the regulations in force at the national level was carried out, exposing the main concepts, as well as the laws that protect the rights of citizens. For this purpose, it was opted for a qualitative, descriptive, non-experimental design research approach; documentary analysis was used as a data collection technique and bibliographic files were used as an instrument. In this regard, it can be stated that Paraguay, in an effort to comply with international commitments, including the Budapest Convention, has included reforms to the Code of Criminal Procedure, as well as added new figures, developed in the corresponding section. However, there is still much to be done in terms of legislation for the prevention and repression of cybercrime. Therefore, a social and regional agreement or pact is necessary to give viability and sustainability to the new legal system in this area and constant updating. It should be noted that, with the use of technology, the crimes that could be configured outside the ordinary definition increase, this would also apply to other crimes such as theft or extortion, and yet, they are not typified in a special way. Issues related to cybersecurity and cybercrime require a multidisciplinary and inter-institutional analysis in order to reach an effective solution. These actions must also involve educational communities and civil society in order to implement preventive actions.

Key words: Cybercrime, technology, state response, regulation, Budapest Convention.

Ñemombyky

Ojekuaségui umi léi ojeahaímava ocastigaha cyberdelito tetã Paraguáipe, ojehecha ha oñehesa'ỹijo mba'éichapa oñemboheko léi-kuéra ñane retãme oñemyesakã porã mba'épa umíva, ha upéicha avei umi léi oñangarekóva guive tetãygua rehe. Upevarã, ojeporavo pe investigacion hérava enfoque cualitativo, tipo descriptivo, ha oguerekóva diseño no experimental; ha ombyatypa haguã umi oikotevẽva katu ojesareko kuatiañe'ẽ ojehaímava hesegua ha upéicha avei oiporu ficha ohechaukahápe heta aranduka upéva rehegua. Umi mba'e rupi, ikatu oje'e ko tetã Paraguái añetehápe ojepytasoha oikóvo ojapopa haguã opaite compromiso ambue tetãndigua, umíva apytépe oĩ pe Convenio Budapest, ha upépe oikéma avei pe Código Procesal Penal, upéichante avei, oñemoĩ hendive léi pyahu omyesakãva ko jehaipyrépe. Upeichavéramo jepe, ojehechakuaa tekotevẽha gueteri heta oñemba'apo léi kuéra rehe ikatu haguã ojehapejoko ha oñemuña cyberdelito. Upévare, tekotevẽ oñeñemoĩmba peteĩ ñe'ẽme tojejapo pacto social tuichaháicha oñembohape ha oñemopyrenda haguã ko sistema legal pyahu ha taipyahu manterei. Ojekuaauka va'erã opárupi pe tecnología jeporu rupive ojejapoha heta ha opaichagua delito ndojegueroikéitiva

pe definición ordinaria-pe, kóva ojeporu kuaáta avei ambueve delito taha'e ñemonda'imimi térã extorsión, ha katu ndojetipifikái gueterívape. Umi tema ojoajúva ciberseguridad ha cyberdetilo oikotevẽ ohesa'ỹijo heta iñarandúva, ha avei oñemoĩmbava'erã hese institución ojejuhu peve peteĩ solución oiko porãva. Ko'ã tembiaporãme ojeikepava'erã, tekombo'eguáva, ha sociedad civil ikatu haguãicha oñembohape hendárupi porã ha tojehapejoko.

Ñe'ẽ tee: cyberdelito, tembiporupyahu, estado mbohovái, ñemohenda, Convenio de Budapest.

Introducción

El escenario actual a nivel mundial en relación a las tecnologías de la información y de la comunicación, crean el espacio virtual denominado cyberespacio, estas circunstancias ofrecen un abanico de posibilidades en lo que respecta a la delincuencia, facilitando la afectación de bienes jurídicamente tutelados a una distancia y con una velocidad increíblemente rápida.

Al respecto, se genera un problema a nivel internacional con las legislaciones y su aplicación, cuando estos hechos por su naturaleza, trascienden las fronteras. Es por ello, que se hace necesario desarrollar procesos de globalización legislativa, leyes de fondo y forma para la cooperación entre los Estados y evitar la impunidad.

Con la aparición de la tecnología, se dio el inicio a una nueva forma de criminalidad vinculados a esta, es por esa razón que los Estados a nivel global se dedicaron a pensar la manera de contrarrestar la problemática del cyberdelito. En tal sentido, el objetivo de la investigación es analizar el marco normativo que castiga el cyberdelito como consecuencia de los compromisos internacionales asumidos por el Paraguay, para ello, se realizó una revisión del desarrollo de las normativas en el derecho paraguayo, exponiendo los principales conceptos, así como las leyes que protegen los derechos de los ciudadanos.

Conceptualización de delitos informáticos

En la actualidad se vive en el epicentro de la información a un solo clic, gracias a las diversas tecnologías disponibles, es decir, el desarrollo y uso de la tecnología se ha vuelto necesaria para la sociedad y es por esta razón que ha abierto un campo que el derecho debe regular. Referente a este aspecto nace el derecho informático, en el apogeo de la era de la información y comunicación, cuya implicancia es el nacimiento de nuevas modalidades delictivas, por lo que resulta esencial perseguir aquellas conductas que dañen derechos e intereses de los ciudadanos.

En tal sentido, el término delito informático se utilizó por primera vez a finales de los años noventa, procesualmente con la expansión que el internet tenía por el mundo. Así como se extendía el uso de internet, también daba inicios a nuevos problemas. Tal fue el caso, que las naciones que conforman el grupo denominado G8, utilizaron el término en una reunión para describir aquellos delitos que se cometían en las redes informáticas (Alcívar, et al 2015).

Considerando, que existe un debate con respecto al alcance y significado de delitos informáticos, pues según Casabona, citado en Acurio del Pino (2016) se ha utilizado dicho término para relacionarlo con la tecnología a través de la que actúa. Sin embargo, a su vez señala que no existe puridad, en la terminología, porque la única nota común es su vinculación a las computadoras. Es así que para este autor es preferible hablar de delincuencia vinculada a las tecnologías de la

información y comunicación.

Por otro lado, Gómez Perals (1994) refiere que se trata de comportamientos dignos de reproche penal, que se realiza a través del sistema informático o que están en relación significativa y presenta formas de lesión a diversos bienes jurídicos.

Así también para Rodríguez, citado en Alcívar et al (2015) el delito informático es la realización de una acción que reúne ciertas características que hacen al concepto de delito, utilizando un elemento informático o telemático con el fin de vulnerar los derechos del titular de un elemento informático, ya sea hardware o software.

Igualmente, Téllez (1999) resume los delitos informáticos en dos modalidades; en primer lugar define como las conductas típicas, antijurídicas y culpables en las que se tiene a las computadoras como instrumento o fin; y, por otro lado, señala a las actitudes ilícitas para las que se tienen a las computadoras como instrumento o fin.

Es así que son varios los autores quienes coinciden que el instrumento para realizar los hechos delictivos son elementos relacionados con las tecnologías; no obstante, existe una falencia en cuanto a la tipificación de los hechos punibles en términos de delitos informáticos. En esta línea, Parker, citado en Acurio del Pino (2016) elabora una tabla en la que se define los delitos informáticos de acuerdo al propósito que se persigue:

Tabla 1

Definición de los delitos informáticos según el propósito

Propósito	Definición
Investigación de la seguridad	Abuso informático es cualquier acto intencional o malicioso que involucre a un computador como objeto, sujeto, instrumento o símbolo donde una víctima sufrió o podría sufrir una pérdida y el perpetrador obtuvo o pudo haber obtenido una ganancia.
Investigación y acusación	Abuso informático es cualquier acto intencional o malicioso que involucre a un computador como objeto, sujeto, instrumento o símbolo donde una víctima sufrió o podría haber sufrido una pérdida y el perpetrador obtuvo o pudo haber obtenido una ganancia.
Legal	Delito informático es cualquier acto tal como está especificado en una ley sobre delito informático en la jurisdicción en que la norma se aplica.
Otros	Abuso informático –sea cual sea su objetivo–, es cualquier delito que no puede ser cometido sin un computador.

Fuente: Parker, Nycum y Oura, 1973, p. 13.

Sin embargo, Acurio del Pino (2016) señala que, independientemente de los propósitos que se persigan, no se justifica la diversidad de las definiciones para una sustancia de entidad única. Así afirma, que los delitos no afectan solo al ámbito patrimonial, sino que estas conductas pueden ser objeto de aflicción para otros bienes jurídicos protegidos como la intimidad personal hasta afectar bienes colectivos, como es la seguridad nacional.

Con base a lo expuesto, los delitos informáticos tienen dos sujetos; el primero, el sujeto activo es quien ejecuta el hecho, este debe tener conocimiento medio o elevado referente al uso y manipulación de la tecnología, y el segundo, el pasivo es decir quien recibe el daño puede ser una persona física o jurídica tales como: bancos, ONG, Gobierno y otros.

Con respecto a ese enfoque de delitos informáticos, la Unidad Especializada de Delitos Informáticos del Ministerio Público conceptualiza el término refiriéndose como: «todas las acciones dirigidas a lesionar la integridad, disposición y confiabilidad de datos y de sistemas informáticos, así como aquellas conductas que atentan contra el patrimonio de las personas utilizando herramientas tecnológicas e informáticas» (2022).

En ese orden, para configurarse un delito informático es necesario la intervención de toda acción dolosa que genere un perjuicio a personas físicas o jurídicas, con la intervención de ordenadores informáticos y sus elementos. Asimismo, no se habla necesariamente de nuevos delitos, sino una nueva forma de llevar a cabo los delitos tradicionales. Aunque la definición de la transgresión depende de los sistemas legales y políticos de cada jurisdicción.

Clasificación de delitos informáticos en el Convenio sobre ciberdelincuencia

El citado convenio conocido también como Convenio de Budapest n.º 185 del Consejo de Europa, conocido así por el lugar de la firma, es un acuerdo internacional para combatir el crimen organizado transnacional, específicamente los delitos informáticos, cuyo objetivo es establecer una legislación penal y procedimientos comunes entre sus Estados partes. Al respecto, se considera como un referente obligado en los esfuerzos de la comunidad internacional, para fortalecer el Estado de derecho en el ciberespacio del cual Paraguay forma parte desde el 20 de noviembre del 2017, a través de la Ley n.° 5994/17 (2001).

Los diferentes delitos informáticos están desglosados en el Capítulo II del convenio titulado «Medidas que deberán adoptarse a nivel nacional», en la Sección 1 del Derecho penal sustantivo, en los títulos 1, 2 y 3.

En ese entendimiento, el Título 1, clasifica los delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos.

Al mismo tiempo, en el art. 2, dispone que:

> 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, el acceso doloso y sin autorización a todo o parte de un sistema informático. Los Estados podrán exigir que la infracción sea cometida con vulneración de medidas de seguridad, con la intención de obtener los datos informáticos o con otra intención delictiva, o también podrán requerir que la infracción se perpetre en un sistema informático conectado a otro sistema informático (Convenio de Budapest).

Mientras que por mandato del art. 3 se dispone:

> 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, la interceptación dolosa y sin autorización, cometida a través de medios técnicos, de datos informáticos –en transmisiones no públicas– en el destino, origen o en el interior de un

> sistema informático, incluidas las emisiones electromagnéticas provenientes de un sistema informático que transporta tales datos informáticos. Los Estados podrán exigir que la infracción sea cometida con alguna intención delictiva o también podrán requerir que la infracción se perpetre en un sistema informático conectado a otro sistema informático (Convenio de Budapest, 2001).

En tal sentido, adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno todo acto deliberado e ilegítimo que dañe, borre, deteriore, altere o suprima datos.

De igual manera, por imperio del art. 5° se establece:

> 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, la obstaculización grave, cometida de forma dolosa y sin autorización, del funcionamiento de un sistema informático, mediante la introducción, transmisión, daño, borrado, deterioro, alteración o supresión de datos informáticos (Convenio de Budapest, 2001).

Estas medidas o de otra naturaleza que resulten necesarias para tipificar como delito en su derecho interno, por disposición del art. 6 refiere:

> La comisión deliberada e ilegítima de los siguientes actos: Producción, venta, obtención para su utilización, importación, difusión u otra forma de puesta a disposición de cualquier dispositivo, incluido un programa informático, concebido o adaptado principalmente para la comisión de cualquiera de los delitos previstos en los arts. 2 al 5 del convenio tales como: Contraseña, código de acceso o datos informáticos similares que permitan acceder a todo o parte de un sistema informático, con intención de que sean utilizados para cometer cualquiera de los delitos contemplados en los arts. 2 al 5; y b, la posesión de alguno de los elementos contemplados en los incisos i) o ii) del apartado anterior, con intención de que sean utilizados para cometer cualquiera de los delitos previstos en los arts. 2 al 5 (Convenio de Budapest, 2001).

Igualmente, las partes podrán exigir en su derecho interno la posesión de un número determinado de dichos elementos para considerar que existe responsabilidad penal.

No obstante, algunos expertos afirman que este artículo pone en riesgo la libertad de expresión y a su vez penaliza actividades legítimas de profesionales y empresas de seguridad informática.

Por otro lado, en lo que refiere a los delitos informáticos previstos por el convenio están tipificados en el art. 7 y siguientes, entre ellos se prevé:

> La falsificación informática, fraude informático, delitos relacionados con el contenido, pornografía infantil, delitos relativos con infracciones de la propiedad intelectual y de los derechos afines. En este aspecto, cada parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno en lo que respecta a la introducción, alteración, borrado o supresión deliberados e ilegítimos 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 no de manera directa. Por tanto, las partes podrán exigir la evidencia de una intención dolosa o delictiva similar, para que se considere que existe responsabilidad

penal (Convenio de Budapest, 2001).

Así también, 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 (art. 8).

En esa línea de pensamiento, el art. 9, versa respecto a los delitos relacionados con la pornografía infantil. Al respecto, establece que cada Estado parte adoptarán las normas 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 difundirla 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.

En el mismo artículo, define a la pornografía infantil, como:

Todo material pornográfico que contenga la representación visual de: un menor adoptando un comportamiento sexualmente explícito; una persona que parezca un menor adoptando un comportamiento sexualmente explícito; imágenes realistas que representen a un menor adoptando un comportamiento sexualmente explícito (Convenio de Budapest, 2001).

La referida norma protege a los niños y adolescentes de la explotación sexual. Es decir para que se cumpla el presupuesto del tipo penal, el objeto sobre el cual recae la acción debe ser un menor de edad.

En cuanto a los delitos referentes a infracciones de la propiedad intelectual y de los derechos afines establece:

1. Cada parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno las infracciones de la propiedad intelectual que defina su legislación, de conformidad con las obligaciones que haya contraído en aplicación del Acta de París del 24 de julio de 1971, por la cual se revisó el Convenio de Berna para la protección de las 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 otorgado por dichos onvenios, cuando tales actos se cometan deliberadamente, a escala comercial y por medio de un sistema informático.

2. Cada parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para

tipificar como delito en su derecho interno las infracciones de los derechos afines definidas en su legislación, de conformidad con las obligaciones que haya asumido en aplicación de la Convención Internacional sobre la Protección de los Artistas Intérpretes o Ejecutantes, los Productores de Fonogramas y los Organismos de Radiodifusión –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 dichos Convenios, cuando tales actos se cometan deliberadamente, a escala comercial y por medio de un sistema informático. 3. En circunstancias bien delimitadas, toda parte podrá reservarse el derecho de no imponer responsabilidad penal en virtud de los párrafos 1 y 2 del presente artículo, siempre que se disponga de otros recursos efectivos y que dicha reserva no vulnere las obligaciones internacionales que incumban a dicha parte en aplicación de los instrumentos internacionales mencionados en los párrafos 1 y 2 del presente artículo (art. 9).

Método

Esta investigación analiza el marco normativo del cyberdelito o ciberdelincuencia en el sistema jurídico paraguayo a partir de los compromisos asumidos por el país a través del Convenio de Budapest y para este efecto se utilizó un enfoque cualitativo con un nivel descriptivo, a través del análisis documental, que se dio por medio de la revisión de la doctrina, instrumentos jurídicos nacionales e internacionales y la jurisprudencia nacional.

Resultado

Marco jurídico vigente

El Estado paraguayo carece de una regulación específica respecto al cyberdelito en un solo cuerpo normativo, más bien se encuentra repartido en varias normativas que tratan diversos aspectos vinculados al tema.

La Constitución Nacional vigente tutela entre otros derechos: la intimidad personal y familiar, así como el respeto a la vida privada, que considera inviolables y en este aspecto sostiene que:

> La conducta de las personas, en tanto no afecte al orden público establecido en la ley o a los derechos de terceros, está exenta de la autoridad pública. Se garantizan el derecho a la protección de la intimidad, de la dignidad y de la imagen privada de las personas (art. 33).

Igualmente, gozan de protección constitucional el patrimonio documental y de la comunicación privada; la prueba de la verdad, y el derecho a informarse; estos derechos son inviolables, salvo las excepciones previstas en la ley.

A nivel internacional, la ciberdelincuencia constituye uno de los aspectos más importantes vinculados a la ciberseguridad y el Convenio de Budapest, constituye el principal tratado internacional para combatirla. Su objetivo es aplicar una política penal común, encaminada a la protección de la sociedad contra el cibercriminal, especialmente, mediante la adopción de una legislación adecuada y el fomento de la cooperación internacional. A pesar de que el Estado paraguayo ratificó dicho instrumento internacional, por otra parte, muchos otros países no

contemplan las principales prácticas para combatirla en sus respectivas legislaciones.

En cuanto a la regulación de este fenómeno, en el año 2011 fue aprobada la Ley n.° 4439/11 que modifica y amplía artículos del C. P., mejor conocida como ley contra los delitos informáticos, y de esta manera se adapta la legislación penal nacional a los estándares mínimos, establecidos en el referido convenio.

En este entendimiento, la ley modificó tres artículos del C. P., relativos a pornografía a niños, niñas y adolescentes, sabotaje de sistemas informáticos y estafa mediante sistemas informáticos, y a su vez introdujo seis nuevos tipos penales que se detalla a continuación: Acceso indebido de datos, preparación de acceso indebido e interceptación de datos, acceso indebido a sistemas informáticos, a la instancia, y a la falsificación de las tarjetas de débito o de crédito y otros medios electrónicos de pagos.

Cabe señalar que a través de la Ley n.° 5994/17, el Estado paraguayo se adhirió oficialmente al convenio referente a cyberdelincuencia del Consejo de Europa, adoptado en la ciudad de Budapest el 23 de noviembre de 2001, además del protocolo adicional respecto a la penalización de actos de índole racista y xenófoba.

En ese orden, las adoptadas prevenciones involucran aspectos legales, pero también refieren directamente a las tareas propias de especialistas en seguridad informática, que pueden discutir y ayudar al estudio de la problemática.

Ahora bien, para enfrentar el problema se realizan intervenciones que en la mayoría de los casos se encuentran gran cantidad de pornografía infantil, que afectan a menores de diferentes edades.

En cuanto al acceso indebido a datos, se refiere a datos de la propiedad privada, cuando se rompe alguna seguridad y se obtiene la información que se encontraba resguardada, y de ahí se determina una sanción.

Referente a este aspecto, el C. P. de 1997, previó varios hechos punibles relacionados a la criminalidad informática, de los cuales se pueden citar los arts.:174, 175, 188 y 248. Luego fueron modificadas tres arts., de los citados –140, 175 y 188– por la Ley n.° 4439/11.

En tal sentido, el art. 140 fue modificado en tres puntos: Primeramente, reformuló el núm. 1 del inc. 1°, simplificando los dos tipos penales contenidos en el mismo. Es así que se eliminaron en ambos, los elementos subjetivos adicionales que establecían además del dolo, una finalidad al producir las publicaciones.

Simultáneamente, el segundo punto consistió en introducir en el núm. 1 del inc. 3°, la facultad para la agravación del marco penal, dar acceso a niños –menores de 14 años– tanto a publicaciones como espectáculos descriptos en los incs. 1° y 2°. Anteriormente, solo se consideraba en este número cuando los niños participaban de las publicaciones o los espectáculos y no cuando se les daba acceso para que los vean.

Por último, la referida ley derogó el inc. 6°, el cual establecía: «Los condenados por la comisión de hechos punibles descriptos en este artículo, generalmente no podrán ser beneficiados con el régimen de libertad condicional».

Por su parte, el art. 175 –sabotaje de computadoras– pasa a denominarse sabotaje de sistemas informáticos. También, se amplía el alcance del tipo al eliminar el requerimiento de que

los datos sean de importancia vital e incluyéndose a los –particulares– como posible objeto del ataque.

Con anterioridad el tipo objetivo era más restringido, en cuanto exigía que el procesamiento de datos sea de importancia vital. Con la reforma, basta obstaculizar un procesamiento de datos, sea o no de importancia para el titular.

Acerca del art. 188, queda como estafa mediante sistemas informáticos. A su vez, se reformulan los términos en los que se enuncian las modalidades contenidas en los núm. del inc. 1°, aunque se debe aclarar que las interpretaciones de los tipos penales descritos no se alteran.

En cambio, la innovación más significativa es la inclusión de un inc. 3° en el cual se prevé el castigo de conductas consistentes en actos preparatorios de los tipos penales señalados en el inc. 1°. Por último, se adiciona un inc. 4° vinculado estrechamente al anterior, pues prevé casos en los cuales se elimina la punibilidad, si se colabora en evitar que los actos preparatorios se consumen.

Por la misma ley se amplía la gama de conductas del C. P, a través los arts.146b, 146c, 146d, 174b, 175b, y 248b. En este entendimiento, el acceso indebido a datos –art. 146b– llena el vacío de punibilidad del fenómeno denominado *hacking* y que afecta la inviolabilidad del ámbito de la vida y la intimidad de un individuo.

En cuanto, al art. 174b acceso indebido a sistemas informáticos, la ubicación sistemática dada en el C. P., lo ubica entre los «hechos punibles contra otros derechos patrimoniales» por lo que no parece condecirse la sintaxis del bien jurídico protegido, en relación a los tipos penales descritos en esta parte, pues estas se relacionan con la protección del derecho a la intimidad. Es más, lo que se pretende castigar ya está cubierto por el art. 146 b, acceso indebido a datos. Asimismo, el art. 174 b introduce el elemento «sistemas informáticos».

En lo que refiere al art. 175 b, se establece que los hechos punibles señalados en los arts. 174 y 175 son a instancia de la víctima, salvo que haya interés público en la persecución. No se hace referencia al criticado art. 174b, con lo cual para la persecución del acceso indebido a sistemas informáticos no resulta necesaria la instancia.

Finalmente, la última incorporación de la Ley n.° 4439/11 al C. P., es el art. 248 b, relativo a la falsificación de tarjetas de débito o de crédito y otros medios electrónicos de pago, ubicada dentro del capítulo de los «hechos punibles contra la prueba documental».

De manera que, el referido artículo contiene cinco inciso. En tal sentido, el 4° y el 5° definen tarjeta de crédito y medios electrónicos de pago, respectivamente. Mientras que el inciso 1°, se divide en dos numerales, que a su vez contiene seis conductas, las cuales si se combinan con los diversos objetos: tarjetas de crédito u otro medio electrónico de pago totalizan doce tipos penales. Es así que, se castiga tanto las conductas de falsificar o alterar una tarjeta de crédito u otro medio de pago electrónico, al igual que la de adquirir, ofrecer, entregar o utilizarla.

Legislación comparada

En las legislaciones de Latinoamérica y el Convenio de Budapest relativo a la ciberdelincuencia, las respuestas ofrecidas por quienes lo firmaron consistirían principalmente en modificar la legislación penal, como es el caso de Argentina, Bolivia, Costa Rica, Guatemala, México, Paraguay y Perú, seguido por la introducción de leyes específicas, como en Brasil, Chile,

Colombia y Venezuela (Convenio de Budapest, 2001).

Por su parte, Ecuador ha utilizado una ley civil y comercial para introducir sanciones penales, mientras que Uruguay solo prevé una ley de protección a los derechos de autor. En los países en que no se dio una reforma en este campo, se trata de reinterpretar la normativa vigente en materia penal, para incluir la tipología de delitos informáticos (Rodríguez Flores, 2013).

En el caso de los E.E. U.U., es pionera en la materia acuñando el concepto cybercrimen, con una acepción amplia del término, a este respecto comprende aquellas situaciones en que el elemento informático se encuentra en el objeto de la conducta penada, intromisión ilegal a bancos de datos, y aquellas en que dicho elemento es el medio para realizar un fin ilícito, por ejemplo, estafa por internet (BCN, 2014).

En ese orden, el ciberdelito en un sentido amplio abarca tanto delitos comunes que se ejecutan a través de medios informáticos, como las nuevas formas de delitos cuya ejecución sólo es posible gracias a la existencia de dichos medios. Esto implica que la respuesta a este tipo de criminalidad apele tanto a la legislación general como a leyes especialmente diseñadas para combatirla, sin perjuicio de que se critique la inadecuación de la legislación basada en la jurisdicción estatal para perseguir un fenómeno de alcance global.

De esta manera, la legislación norteamericana tipifica bajo la denominación genérica de cyberdelitos figuras de terrorismo, Ley USA Patriot refiere a: obscenidades, diversas figuras de pornografía, prohibición de dominios engañosos, prohibición de uso de recursos públicos para adquisición de ordenadores sin filtros, seducción de menores para propósitos sexuales, protección de *copyright*, difamación, amenazas y acoso cibernético, etc., todos ellos cometidos por medios informáticos (BCN, 2014).

Jurisprudencia nacional

En este punto, se lleva al análisis el fallo judicial de la causa n.° 407/16 «Gladys Fernández Molinas s/ estafa mediante sistemas informáticos y otros». Referente a esta causa, el Tribunal de Sentencia luego de sopesar las pruebas, determinó que la acusada, cometió los hechos punibles de estafa mediante sistemas informáticos y apropiación grave.

En ese entendimiento, durante el juicio el Ministerio Público y la querella demostraron que la acusada se valió de falencias informáticas entre dos softwares de gestión de ventas de pasajes, y con ello pudo enriquecerse generando un perjuicio patrimonial a la empresa para la cual trabajaba.

El caso se habría registrado entre enero y mayo del 2016, cuando la condenada descubrió un mecanismo de estafa, mediante las reservas y cancelaciones de pasajes al Brasil. Pues recibía el dinero de los pasajeros a través de giros tigo o pago en efectivo, hacía la reserva pero antes de la medianoche las cancelaba, a través de un mecanismo que solo un profesional lo haría. El pasajero viajaba sin embargo, no se registraba el pago en la agencia.

Bajo ese razonamiento, fue hallada culpable y sentenciada a la pena privativa de libertad de siete años, de cumplimiento efectivo con revocación de medidas alternativas. Esta es una de las

condenas de mayor relevancia en materia de delitos informáticos en los últimos años.

Unidad especializada de delitos informáticos

Esta unidad especializada fue creada para combatir hechos punibles cometidos por medio de la tecnología y que a su vez precisa un tratamiento especializado, ya que en este tipo de investigación se requiere un conocimiento especializado en el manejo de la evidencia digital.

En este contexto, se señala los delitos informáticos como conductas que atentan contra el patrimonio de las personas. Además, según las Resoluciones n.° 3459/10 y n.° 4408/11, señalan los siguientes tipos penales:

> Acceso indebido a datos, interceptación, preparación al acceso indebido a datos, alteración de datos, acceso indebido a sistemas informáticos, sabotaje a sistemas informáticos, alteración de datos relevantes, falsificación de tarjetas de crédito y débito y estafa mediante sistemas informáticos (2010/2011).

Igualmente, la unidad ofrece apoyo técnico-jurídico a los agentes fiscales en la realización de diligencias, teniendo en cuenta lo establecido el art. 228 del C. P.; también realiza el registro o decomiso de datos informáticos almacenados de conformidad con los arts. 183, 192, 193 y 196 del C. P. P.

Así también, realiza charlas en instituciones educativas de todo el país en el marco del programa de prevención contra el *ciberbulling, sexting*, pornografía infantil y *grooming*.

Dicho lo anterior, según datos oficiales, en octubre del 2021 en dicha unidad ingresaron 3.452 causas que abarcaban pornografía, acceso indebido, estafas mediante sistemas informáticos, alteración de datos, falsificación de tarjetas de crédito y débito (Ministerio Público, 2021).

Ahora bien, para comprender mejor el tema se pasa analizar las modalidades en las que estos criminales operan, que se resumen de la siguiente manera:

La modalidad denominada *phishing* se ejecuta a través del engaño, se utiliza la ingeniería social para acceder a información de carácter confidencial como pueden ser correos, contraseñas y números de tarjetas de crédito. Estas se hacen a través del envío de mensaje en la que se pide al usuario el ingreso o actualización de datos, por motivos de seguridad o para confirmar su cuenta, a fin de que estos faciliten sus datos personales, claves, etc. (MARKEDATA, 2022).

De manera semejante se encuentra la otra modalidad denominada *smiching*, el cual consiste en un método bastante común en el Paraguay. Esta forma de engaño se trata de mensajes de texto vía WhatsApp anunciando un premio, brindando un número de teléfono al que el supuesto ganador debe acudir, la victima llama al número y el supuesto beneficiador le solicita un poco de dinero para agilizar los gastos. Ejemplo, se comunican a una ONG le dice que en la aduana de Ciudad del Este están retenidos aparatos tecnológicos, pero que necesitan el valor del combustible para el traslado hasta la ciudad de Asunción (López, 2019).

Luego se puede analizar el *pharming*, que se ejecuta cuando los criminales alteran la red y reconducen a sitios falsos, la victima tiene la certeza que es una página válida, rellena los

formularios con información confidencial, es decir, usuarios, números de teléfonos, contraseñas, tarjetas de crédito. Otra forma de perpetrar este hecho punible es a través de los virus.

Por último, se ubica al *vishing*, esto es un método también frecuente donde el estafador se comunica con la víctima y con argumentos falsos obtiene datos que luego utilizara para la estafa. Es el caso de las llamadas que se hacen comunicando falsas premiaciones y exigiendo depósitos de dinero para entregarlas (López, 2019).

Conclusión

En el presente trabajo de investigación se analizó el Convenio de Budapest que obliga a los Estados partes a adoptar en sus respectivas legislaciones, normas legales y procesales para combatir la ciberdelincuencia en el ámbito punitivo.

Dicho convenio, en relación a las normativas penales de fondo establece que los Estados deberán incluir en sus ordenamientos jurídicos normativas penales, la tipificación de los siguientes delitos: a) delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos: acceso ilícito, la intercepción ilícita, ataques a la integridad de los datos, ataques a la integridad del sistema, abuso de los dispositivos; b) delitos informáticos: falsificación informática y fraude informático; c) delitos relacionados con el contenido: pornografía infantil; d) delitos relacionados con infracciones de propiedad intelectual y de los derechos afines: derechos de autor y derechos conexos; e) otras formas de responsabilidad y sanción: tentativa y complicidad, responsabilidad de las personas jurídicas. Además, todos los delitos deberán estar sujetos a sanciones efectivas, proporcionadas y disuasorias, incluidas penas privativas de libertad.

Uno de los aspectos criticados es la inclusión de delitos ordinarios como la: falsificación, fraude y pornografía infantil. Como se puede apreciar, los mismos ya se encuentran en los ordenamientos jurídicos de las naciones modernas a través de sus leyes penales, entre ellas la legislación paraguaya.

En este entendimiento, Paraguay, con el afán de cumplir con los compromisos internacionales, entre ellas el citado convenio, ha incluido reformas al C. P., como asimismo, agregó nuevas figuras desarrolladas en el apartado correspondiente. Sin embargo, hay mucho por recorrer en materia legislativa de represión y castigo al ciberdelito.

En este punto, la realidad actual en la materia demuestra variados y complejos desafíos que deben ser seriamente analizados, a fin de buscar alternativas para la superación o al menos su mitigación. Los esfuerzos deberán estar fundados en espacios de diálogo y consenso, ya que no solo existe la necesidad de legislar y prevenir sino de respetar los derechos y las libertades de las personas.

Por ello, es necesario llegar a un acuerdo o pacto social y regional que brinde sostenibilidad y viabilidad al nuevo sistema legal en la materia y una actualización constante.

A pesar de presumir que, con el uso de la tecnología aumentan los casos en que algunos delitos caerían fuera de la definición ordinaria, esto podría aplicarse también a otros delitos

ordinarios como por ejemplo: el hurto o la extorsión, y sin embargo no se tipifican de forma especial. Los temas vinculados a la ciberseguridad y el ciberdelito requieren de una discusión multidisciplinaria en la que expertos legales, en ciberseguridad y en educación deben aportar para alcanzar una solución efectiva. Estas acciones deben involucrar a comunidades educativas y sociedad civil, a fin de poner en práctica acciones preventivas también.

Referencias

Acurio del Pino, S. (2016). *Delitos informáticos: Generalidades.* https://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf

Alcívar, C., Domenech, G. y Ortíz, C. (2015). La seguridad jurídica frente a los delitos informáticos. *Avances*, 10(12), 41-57.

Biblioteca y Archivo Central del Congreso de la Nación. Ley n.° 5994. https://www.bacn.gov.py/leyes-paraguayas/9900/ley-n-5994-aprueba-la-convencionsobre-la-ciberdelincuencia-y-el-protocolo-adicional-al-convenio-sobreciberdelincuencia-relativo-a-la-penalizacion-de-actos-de-indole-racista-y-xenofobacometidos-por-medio-de-sistemas-informaticos

Biblioteca del Congreso Nacional, BCN (2019). Convenio sobre la Ciberdelincuencia: Convenio de Budapest. Disponible en: https://www.bcn.cl/obtienearchivo?id=repositorio/10221/26882/1/Convenio_de_Bud apest_y_iberdelinciencia_n_Chile.pdf (junio, 2020).

Código Penal del Paraguay Ley n.° 1.160/97. http://www.oas.org/juridico/spanish/cyb_par_cod_penal.pdf

Gómez Perals, M. (1994). "Los Delitos Informáticos en el Derecho Español", Informática y

Derecho n.º 4, UNED, Centro Regional de Extremadura, III Congreso Iberoamericano de Informática y Derecho 21-25 septiembre 1992. Editorial Aranzadi.

Ministerio Público. República del Paraguay. Unidad Especializada de Delitos Informáticos. https://ministeriopublico.gov.py/unidad-especializada-de-delitos-informaticos-

Ministerio de Tecnologías de la Información y Comunicación. Convención contra el Ciberdelito. https://www.senatics.gov.py/noticias/paraguay-se-adhiere-laconvencion-contra-el-ciberdelito

MARKEDATA. (2022). *Alertan sobre intento de fraude por phishing nuevamente dentro del país. Asunción*: El análisis en tus manos.

Organización de los Estados Americanos. Departamento de Cooperación Jurídica. http://www.oas.org/juridico/spanish/cyb_par.htm

Rodríguez Flores, María Eugenia (2013). América Latina, ¿Debe crear un sistema de normas armonizadas para el cibercrimen? Trabajos de Investigación en Políticas Públicas, n.° 16, 2013. Departamento de Economía de la Universidad de Chile. Disponible en: http://www.econ.uchile.cl/uploads/ublicacion/9ba7739a0ac26598402dab53c990c58e49fc259a.pdf (julio, 2020).

Sequera, M. y Samaniego, M. (2018). *Cibercrimen: desafíos de la armonización de la Convención de Budapest en el sistema penal paraguayo*. https://creativecommons.org/licenses/by/4.0/deed.es

Tellez Valdés, J. (1999). Los delitos informáticos. Editorial Temis.