Ius Comitiãlis
ISSN: 2594-1356
iuscomitialis@uaemex.mx
Universidad Autónoma del Estado de México
México

Elizalde Castañeda, Rodolfo Rafael; Flores Ramírez, Héctor Hugo; Castro Lorzo, Edwin Misael
Los delitos cibernéticos en Chile, México y Colombia. Un estudio de Derecho Comparado
Ius Comitiãlis, vol. 4, núm. 8, 2021, Julio-Diciembre, pp. 252-276
Universidad Autónoma del Estado de México
México

Número completo
Más información del artículo
Página de la revista en redalyc.org

Los delitos cibernéticos en Chile, México y Colombia. Un estudio de Derecho comparado

Cyber crimes in Chile, Mexico and Colombia. A comparative law study

Rodolfo Rafael Elizalde Castañeda[1]
Héctor Hugo Flores Ramírez[2]
Edwin Misael Castro Lorzo[3]

Ius Comitiālis / Año 4, Número 8 / julio - diciembre 2021 / pp. 252-276 / ISSN: 2594-1356
Recepción: 18 de agosto de 2021 / Aceptación: 29 de noviembre de 2021

Resumen: El objetivo de este artículo fue investigar y analizar los delitos cibernéticos vigentes en Chile, México y Colombia, con el fin, primero, de estudiar sus ordenamientos jurídicos tendientes a regular estas nuevas formas delictivas; segundo, conocer cuáles son las semejanzas y diferencias que guardan los delitos cibernéticos en esos tres países; y, por último, determinar si en los inicios de la tercera década del siglo XXI, los tres países han adecuado su marco constitucional y legal a los términos establecidos en el Convenio sobre la Ciberdelincuencia 2001, celebrado en Budapest.

Palabras clave: Delitos cibernéticos; medios electrónicos; ciberespacio; sistemas informáticos; Derecho informático.

Abstract: The objective of this article was to investigate and analyze current cybercrimes in Chile, Mexico and Colombia, in order, first, to study their legal systems aimed at regulating these new criminal forms; second, to know what are the similarities and differences between cybercrimes in those three countries; and finally, to determine whether at the beginning of the third decade of the 21st century, the three countries have adapted their constitutional and legal framework to the terms established in the 2001 Convention on Cybercrime, celebrated in Budapest.

Key words: Cybercrimes; electronic media; cyberspace; information systems; computer law.

https://orcid.org/0000-0001-8680-3581. / *Correo electrónico: rodolfoelizaldecas@yahoo.com.mx*

[1] Facultad de Derecho, Universidad Autónoma del Estado de México. Toluca, Estado de México.

https://orcid.org/0000-0001-6857-4017. / *Correo electrónico: hectorhugofloresramirez@gmail.com*

[2] Facultad de Derecho, Universidad Autónoma del Estado de México. Toluca, Estado de México.

https://orcid.org/0000-0002-8354-3312. / *Correo electrónico: edwinmisaelcastrolorzo@gmail.com*

[3] Facultad de Derecho, Universidad Autónoma del Estado de México. Toluca, Estado de México.

Esta obra está bajo licencia Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International (CC BY-NC-SA 4.0)

Rodolfo Rafael Elizalde Castañeda/*https://orcid.org/0000-0001-8680-3581./Correo electrónico: rodolfoelizaldecas@yahoo.com.mx*
Héctor Hugo Flores Ramírez/*https://orcid.org/0000-0001-6857-4017./Correo electrónico: hectorhugofloresramirez@gmail.com*
Edwin Misael Castro Lorzo / *https://orcid.org/0000-0002-8354-3312. / Correo electrónico: edwinmisaelcastrolorzo@gmail.com*

INTRODUCCIÓN

Ha transcurrido medio siglo desde que la República de Chile, los Estados Unidos Mexicanos y la República de Colombia comenzaron a tipificar las conductas relacionadas con los delitos cibernéticos: Chile, en 1970, con la Ley N° 17.336; México reforma el Código Penal Federal con fecha 07 de noviembre de 1996; mientras que Colombia, en 1989, lo hace mediante el Decreto 1360, con el cual se reglamenta la inscripción del soporte lógico (software) en el Registro Nacional de Derecho de Autor. Como profundizaremos más adelante, los mencionados países han creado legislaciones para tipificar las conductas relacionadas con los delitos cibernéticos, pero surge una cuestión: ¿qué tanto han avanzado en las reformas constitucionales y legales sobre dicha materia? Para ello necesitamos un referente, por lo que consideramos que pudiera servirnos de parámetro el Convenio creado por el Consejo de Europa sobre Ciberdelincuencia, celebrado en Budapest en 2001. Se trata de un acuerdo internacional para combatir el crimen organizado transnacional, específicamente los delitos informáticos y su principal objetivo es crear una legislación penal sustantiva y adjetiva aplicable en todos los Estados Partes, o sea, se trata de un nexo obligado para sumar esfuerzos internacionales con la idea de fortalecer el Estado moderno constitucional de Derecho para combatir la ciberdelincuencia, sobre todo porque este es el único convenio internacional que existe sobre la materia. Por ello, en los inicios de la tercera década del siglo XXI, proponemos estudiar comparativamente las referidas reformas a la luz de dicho convenio.

En los tres países motivo de este artículo existen diversos estudios que se han realizado en materia de delitos cibernéticos y/o informáticos, tal es el caso de Chile con Sebastián Becker y Pablo Viollier (2020) y su artículo "La Implementación del Convenio de Budapest en Chile: un Análisis a Propósito del Proyecto Legislativo que Modifica la Ley 19.223"; de la misma manera, Verónica Barrios y Andrea Vargas (2018) y su artículo "Convenio sobre la Ciberdelincuencia: Convenio de Budapest"; en México, tenemos a Hiram Piña (2019) y su artículo, "Cibercriminalidad y ciberdelincuencia en México"; asimismo, María del Consuelo Argüelles (2016) y su artículo "Retos de la legislación informática en México"; también tenemos en Colombia a Yenifer Dávila (s.f.), y su artículo, "Delitos Cibernéticos en el Derecho Colombiano y desde la Perspectiva del Derecho Comparado"; pese a la variedad de artículos, no encontramos un estudio que involucre exclusivamente a los tres países mencionados y, menos aún, que se realice un análisis comparativo de cada una de las reformas constitucionales y legales vigentes sobre delitos cibernéticos; tampoco se encontró un estudio sobre el avance que han tenido respecto a la protección de derechos cibernéticos en torno al Convenio de Budapest hasta este momento del siglo XXI. Esto sería suficiente para justificar doctrinal y jurídicamente un trabajo como el que aquí se propone, pues los resultados que arroje seguramente servirán para que los operadores jurídicos de los tres países abonen a su cultura jurídica sobre la temática.

Las preguntas que orientaron este análisis son: ¿Cuáles son las reformas constitucionales y legales sobre los delitos cibernéticos en los ordenamientos jurídicos vigentes? ¿Cuáles son las semejanzas y diferencias que guarda la regulación de los delitos cibernéticos? ¿Chile, México y Colombia han adecuado al Convenio de Budapest su marco constitucional y legal en materia de delitos cibernéticos en los inicios de la tercera década del siglo XXI? Los métodos utilizados fueron: analítico, sintético, normativo, bibliográfico y hemerográfico, basado sobre todo en el derecho comparado.

I. ALGUNAS IDEAS CONCEPTUALES

En este apartado se definirán algunos de los términos que servirán como preámbulo del análisis y la comparación entre las diversas reformas constitucionales y legales tendientes a regular los Delitos Cibernéticos en Chile, México y Colombia.

a. Delitos Cibernéticos
De acuerdo con André Santos y Ricardo Magno (2020), el delito cibernético:

> Se configura cuando se manifiestan comportamientos delictivos practicados en el ciberespacio, en los que la esencia del daño no podría haber ocurrido en ningún otro espacio. Desde esta perspectiva, cualquier comportamiento delictivo que se produzca en el espacio o el entorno cibernético es admitido como delito cibernético, incluyendo los tipos de delitos ejecutados tradicionalmente sin necesidad de ser materializados en el entorno virtual, pero que efectivamente hoy también evolucionaron a la dimensión tecnológica... (p. 89).

b. Medios Electrónicos
Al respecto del tema, Javier Esteinou y Alma Alva (2011) establecen que:

> Los medios electrónicos han permanecido como instancias prácticamente autónomas de la verdadera regulación social y se han desarrollado como instituciones sin límites que las acoten, convirtiéndose en poderes fácticos que desafían y rebasan a los poderes públicos y sociales constituidos formalmente a través de largos procesos civilizados de la historia de México. Así, se han convertido en poderes facticos o poderes reales independientes, impunes y prepotentes muy poderosos que retan, golpean y subordinan a los otros poderes públicos y sociales ya establecidos a lo largo de muchas décadas... (p. 96).

c. Ciberespacio
De acuerdo con Rodrigo Ardissom de Souza (2018) el ciberespacio es:

> La posibilidad de encuentros de los sujetos, de la creación de comunidades en un lugar específico, en la estructura de una red que potencialmente no tiene jerarquías, un encuentro de sujetos que aunque no compartan la misma ubicación tienen la posibilidad de compartir experiencias al instante (p. 7).

d. Sistemas Informáticos

De conformidad con el artículo 1, del Convenio sobre la Ciberdelincuencia, adoptado en Budapest (2001), por sistema informático se entenderá, "todo dispositivo aislado o conjunto de dispositivos interconectados o relacionados entre sí, siempre que uno o varios de ellos permitan el tratamiento automatizado de datos en ejecución de un programa" (p. 3).

e. Derecho Informático

De igual manera, Horacio Fernández (2014) define al derecho informático como:

> El conjunto de principios y normas que regulan los efectos jurídicos nacidos de la interrelación entre el derecho y la informática. Y que la informática es una ciencia que estudia métodos, proceso y técnicas, con el fin de almacenar, procesar y transmitir informaciones y datos en formato digital. (p. 1)

II. CONVENIO SOBRE LA CIBERDELINCUENCIA

El Convenio sobre la Ciberdelincuencia fue creado por el Consejo de Europa en 2001 y entró en vigor hasta el 2004, enfocándose plenamente en la ciberdelincuencia a nivel internacional. En él se establece que:

> Es necesario para prevenir los actos que pongan en peligro la confidencialidad, la integridad y la disponibilidad de los sistemas, redes y datos informáticos, así como el abuso de dichos sistemas, redes y datos, garantizando la tipificación como delito de dichos actos. (p. 2)

Hasta la fecha, ha sido ratificado por 65 países, entre ellos Chile y Colombia, mientras que México mantiene un estatus de "observador". Uno de los objetivos, de acuerdo con el Boletín N°. 12.192-25 emitido por el Presidente de la República de Chile, Sebastián Piñera Echenique, dirigido al Senado (2018) es:

> El desarrollo de una política criminal común frente a la ciberdelincuencia, mediante la homologación de los conceptos fundamentales y del tratamiento de la legislación penal, sustantiva y procesal, así como del establecimiento de un sistema rápido y eficaz de cooperación internacional. (p. 2)

En el Convenio se estipulan 9 delitos cibernéticos, que deben ser incorporados al derecho interno de cada país que se adhiera al mismo, Estos delitos son:

> Art. 2. Acceso ilícito. ...el acceso deliberado e ilegitimo a todo o parte de un sistema informático...
> Art. 3. Intercepción ilícita. ...intercepción deliberada e ilegítima por medios técnicos de datos a un sistema informático...

Art. 4. Ataques a la integridad de datos. ...todo acto deliberado e ilegítimo que dañe, borre, deteriore, altere o suprima datos informáticos...
Art. 5. Ataques a la integridad del sistema. ...la obstaculización grave, deliberada e ilegítima del funcionamiento de un sistema informático mediante la introducción, trasmisión, daño, borrado, deterioro, alteración o supresión de datos informáticos...
Art. 6. Abuso de los dispositivos. ...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 la comisión de cualquiera de los delitos previstos en los artículos 2 a 5 del presente Convenio;

ii. una contraseña, código de acceso o datos informáticos similares que permitan acceder a todo o parte de un sistema informático,

Art. 7. Falsificación informática. ...la introducción alteración, borrado o supresión deliberados o ilegítimos de datos informáticos que genere datos no auténticos...
Art. 8. Fraude informático. ...los actos deliberados e ilegítimos que causen perjuicio patrimonial a otra persona...

a. la introducción, alteración, borrado o supresión de datos informáticos;

b. Cualquier interferencia en el funcionamiento de un sistema informático...

Art. 9. Delitos relacionados con pornografía infantil (a través de un sistema informático).
Art. 10. Delitos relacionados con infracciones de la propiedad intelectual y de derechos afines (a través de un sistema informático).

Cabe resaltar que una de las características del multicitado Convenio es que es no autoejecutable, es decir, requiere de modificaciones en su derecho interno, acorde con sus propios términos, tal como se establece en el artículo 2, donde se determina que "Cada Parte adoptará las medidas legislativas y de otro tipo que resulten para tipificar como delito en su derecho interno el acceso deliberado e ilegítimo a la totalidad o a una parte de un sistema informático...". Lo cual requiere un gran esfuerzo de las legislaturas de cada país para poder llevar a cabo las adecuaciones en favor de resguardar los bienes jurídicos de sus gobernados.

III. MARCO REGULATORIO DE LOS DELITOS CIBERNÉTICOS EN CHILE, MÉXICO Y COLOMBIA

a. Chile

Marco Constitucional

La Constitución Política de la República de Chile (1980), publicada en el Diario Oficial de la República de Chile, en su artículo 19, estipula en el número 4° que "La Constitución asegura a todas las personas... El respeto y protección de sus datos personales", mientras que en el número 5° establece que "La Constitución asegura a todas las personas... la inviolabilidad del hogar y de toda forma de comunicación privada". Pese a que se encuentran reconocidos estos derechos relacionados con el derecho cibernético, la Constitución de Chile carece de legitimidad ya que su origen data de un golpe de Estado llevado a cabo el 11 de septiembre de 1973 en contra del gobierno de Salvador Allende. A ese respecto, Rafael Amézquita (2020) señala:

> Una de las graves problemáticas de la constitución vigente es que, durante la dictadura, funcionó como instrumento jurídico para justificar violaciones de derechos humanos, la perpetuación en el poder de los grupos militares y de derecha, la persecución política a opositores y la instauración del principio de subsidiariedad. (pp. 70-71)

De la misma manera, es preciso mencionar que actualmente los chilenos están haciendo grandes esfuerzos e incluso movilizaciones a fin de crear una nueva constitución que permita el regreso al Estado de Derecho y la protección de los Derechos Humanos.

Marco Legal

Aquí se analizarán brevemente los siguientes ordenamientos: Ley N° 17.336, promulgada en 1970; Ley 19.223, promulgada en 1993; Ley N° 19.927, promulgada en 2004; y, a nivel internacional, el Convenio de Budapest, suscrito en fecha de 2017 por medio del Decreto 83, emitido por el Ministro de Relaciones Exteriores, publicados todos en el Diario Oficial de la República de Chile.

Ley N° 17.336

Cuando Chile comenzó en 1970 a tipificar los delitos cibernéticos consideró que en la información cibernética los bienes jurídicos a proteger son bienes inmateriales o intangibles, lo cual se ve plasmado en el artículo 67 bis de la citada Ley N° 17.336, sobre la propiedad intelectual, tendiente a proteger los derechos que adquieren los autores en el ámbito literario, artístico y científico. El delito cibernético recae directamente en la distribución o venta de las obras del autor sin su autorización, ya que los artículos 17 y 20 otorgan a los titulares del derecho de autor de manera exclusiva las facultades de utilizar o difundir sus obras, ya sea total o parcialmente, inclusive realizar una transferencia de la misma por medio de una autorización a terceros; por lo cual si se difunde o modifica alguna obra sin permiso del autor (en este caso se tiene que llevar a cabo por medios electrónicos, como lo son páginas de internet o redes sociales), en caso de no darle el debido reconocimiento por autoría, se configuraría el delito cibernético contra la propiedad intelectual, conforme al artículo número 18 de la precitada Ley.

Ley N°. 19.223 de 1991

El 16 de julio de 1991 se presentó el Proyecto de Ley N° 19.223 o Ley que Tipifica Figuras Penales Relativas a la Informática ante la Cámara Alta del Poder Legislativo, dicha ley se integra por solo 4 artículos, de los cuales se resalta su enfoque en dos conductas ilícitas con la utilización de medios electrónicos para su comisión: el sabotaje y el espionaje informático. El sabotaje informático como conducta ilícita cibernética se plasmó en sus artículos 1 y 3, y sucede cuando se genera una afectación a algún sistema de información, puede tratarse de daños a sus partes o componentes; se estipula que la conducta ilícita cibernética se concentra exclusivamente en los datos o información que contenga un sistema de tratamiento de información, tal y como lo corrobora Susana Hiplan (2019), esto puede ser "desde la placa madre hasta un simple puerto USB, tanto como de un bien intangible, el cual corresponde a la información y los datos que en aquel sistema se encuentren almacenados" (p. 25). En los artículos 2 y 4 se aborda el espionaje informático, donde se especifica que se castigará cuando alguien se apodere indebidamente y difunda información contenida en un sistema de tratamiento informático.

Con lo anterior, podemos vislumbrar que la Ley que nos ocupa se enfoca concretamente en los sistemas de información, dejando a un lado figuras como el fraude, robo de identidad y la pornografía infantil, entre otros. Siguiendo la misma postura, Susana Hiplan (2019) considera que con dicha ley se creó:

> Una ley simple y escueta que establece cuatro tipos penales que buscan sancionar el sabotaje al funcionamiento al sistema informático, el espionaje a estos sistemas y la revelación de información obtenida desde un sistema sin la autorización para hacerlo. Se tipifican, de igual modo, conductas que atenten contra la protección de los datos contenidos en los sistemas informáticos, y es esta tipicidad objetiva la que trae aparejadas las penas más altas, por considerarse los peligros relativos a la obtención y manejo de la información almacenada los potencialmente más dañosos. (p. 12)

Para la época de los noventa cabe resaltar, sin embargo, que dicha ley estaba a la vanguardia jurídica, considerando que en esa época este tema era completamente nuevo, en donde las herramientas tecnológicas, como lo es la Internet, apenas se comenzaban a divisar.

Ley N°. 19.927 de 2004

La Ley N°. 19.927 fue publicada en el Diario Oficial con fecha 14 de enero del 2004 y se le conoció como *Ley sobre la Pedofilia*, con la que se llevó a cabo una serie de modificaciones al Código Penal Chileno (1874), en materia de pornografía infantil, por lo cual a continuación se hará mención de los puntos más relevantes que trajo consigo; asimismo, es preciso señalar que en esa época se comenzó a introducir el término *Pornografía Infantil*; es decir, difundir cualquier tipo de video en los que se realicen actos sexuales o de exhibicionismo corporal protagonizado por menores de edad a través de diferentes medios electrónicos. Los puntos relevantes que trajo consigo esta

ley son los siguientes:

> I. Respecto al artículo 361 tiene una modificación consistente en aumentar la pena del delito de violación, en correlación con el artículo 374 bis, cuando se lleva a cabo la comercialización, importación, exportación o exhibición de material pornográfico mediante cualquier soporte, en donde entran páginas de internet o redes sociales; además se tipifica la conducta de la persona que almacene materiales sexuales. La pena aumentó de cinco años y un día a quince años.
> II. En el artículo 366 quinquies, se agregó "que aquel que participare en la producción de material pornográfico, en cuya elaboración se hubieren utilizado menores de dieciocho años". Además de la producción también se castiga al que abusivamente realice una acción sexual distinta al acceso carnal con una persona mayor de catorce años, esto, en el artículo 366, castigando también a aquella persona que, sin realizar una acción sexual, solo para su excitación o de un tercero, obligaré al menor a ver y escuchar videos pornográficos, esto con respecto al artículo 366 quáter. Estableciendo además la definición de material pornográfico: "cuya elaboración hubieren sido utilizados menores de dieciocho años, toda representación de éstos dedicados a actividades sexuales explícitas, reales o simuladas, o toda representación de sus partes genitales con fines primordialmente sexuales" lo anterior en relación con el artículo 366 quinquies y 374 bis.
> III. En los artículos 367 y 367 bis se estableció que aquellas personas que promuevan o faciliten la prostitución de menores de edad para satisfacer los deseos de otro y realice acciones tendientes a facilitar la entrada y salida de personas que ejerzan la prostitución en el país.

Con lo anterior se castiga a quienes participen en material pornográfico, comercializarlo, difundirlo, exportarlo o exhibirlo por medios electrónicos, en cuya creación o difusión de contenido sexual participen personas menores de 18 años, a los cuales van a obligar a participar en actos sexuales o exhibicionismo para la obtención de una remuneración económica, ya que los menores de edad son personas desprotegidas.

Chile y el Convenio de Budapest

La República de Chile se adhirió al Convenio de Budapest el 20 de abril de 2017, el cual entró en vigor, para el país, el 01 de octubre de 2017, por medio del Decreto 83, emitido por el Ministro de Relaciones Exteriores y publicado en el Diario Oficial, con ello se comprometían a llevar a cabo modificaciones en sus leyes respecto a los delitos cibernéticos, esto mediante el ya citado Boletín 12.192-25 (2018), en el que se establece:

> El proyecto de ley deroga la ley N° 19.223, con el objeto de establecer una ley especial que contenga de manera integral las nuevas formas delictivas surgidas a partir del desarrollo de la informática. De esta manera se pretende llenar los vacíos o dificultades que ha tenido nuestro ordenamiento penal en la persecución de ciertas conductas que, incluso, no eran concebibles a la época de dictación de la ley N° 19.223. (p. 7)

Como se vio previamente, Chile comenzó a legislar en materia de delitos cibernéticos antes de la celebración del multicitado convenio, ejemplo de ello son la Ley 17.336 (1970) sobre la propiedad intelectual, como se hizo mención *supra* en su artículo 79, se encuentra relacionada con el artículo 10 (Delitos relacionados con infracciones de la propiedad intelectual y de derechos afines) del Convenio de Budapest y de la Ley 19.223 (1991) que tipifica Figuras Penales Relativas a la Informática, que en sus artículos tipifica el Sabotaje y Espionaje Informático, en donde el primero guarda relación con los artículos 4 (Ataques a la integridad de los datos) y 5 (Ataques a la integridad del sistema); mientras que el segundo se involucra con los artículos 2(Acceso Ilícito) y 3 (Intercepción Ilícita) del Convenio de Budapest. De acuerdo con Juan Lara, Martínez y Viollier (2014), "cuando la legislación chilena habla de «delitos informáticos» lo hace en referencia a la protección mediante el derecho penal de los datos y sistemas informáticos" (p. 109), que de acuerdo con la teoría del bien jurídico protegido se establecerían como delitos simples y que de acuerdo con Claus Roxin (1997) "solo protegen a un bien jurídico" (p. 337), dejando a un lado la regulación de delitos cibernéticos orientados a la protección de bienes jurídicos compuestos, tales como: la propiedad, la vida, pornografía infantil, fraude, entre otros.

Pese a que Chile aún no se había adherido al Convenio de Budapest, creo la Ley 19.927 publicada en el Diario Oficial de fecha 14 de enero del 2004 sobre Pedofilia, con la que se modificó el Código Penal Chileno, en el cual, en sus artículos 366 quinquies y 374 bis, referentes a la reproducción, difusión, adquisición, posesión, exportación e importación de pornografía infantil por medios electrónicos, ambos se relacionan con el artículo 9-Delitos relacionados con la pornografía infantil del Convenio de Budapest; en este caso, el bien jurídico de los delitos cibernéticos/informáticos queda como el medio/herramienta para su comisión: de conformidad con la teoría del bien jurídico protegido se establecerían como delitos compuestos, y, parafraseando a Claus Roxin (1997) los delitos compuestos protegen varios bienes jurídicos.

Si bien Chile se adhirió al mencionado Convenio cuando ya regulaba las referidas conductas cibernéticas, aún falta realizar modificaciones en términos del Convenio sobre la Ciberdelincuencia, tales como: Abuso de los dispositivos, Falsificación Informática y Fraudes Informáticos; lo cual se observa en la Ley N° 19.223, que sigue vigente, incluso cuando el pasado 6 de octubre de 2021 se conformó una Comisión Mixta (compuesta por Senadores y Diputados) para analizar el proyecto de ley que moderniza las normas sobre delitos informáticos con el objetivo de derogarla; sin embargo, dicho proyecto aún no se ha aprobado, tal como se corrobora en la página web oficial del Senado de la República de Chile (2021).

b. México

Marco Constitucional

Es la Constitución Política de los Estados Unidos Mexicanos (1917), donde se encuentran plasmados la Libertad de Expresión y el Derecho a la Información, en sus artículos 6 y 7, respectivamente; el primero, consiste en que "toda persona tiene derecho al libre acceso a información plural y oportuna... y difundir información e ideas de toda

índole... El Estado garantizará el derecho de acceso a las tecnologías de la información"; en el segundo se establece que "es inviolable la libertad de difundir opiniones, información e ideas, a través de cualquier medio". De acuerdo con lo anterior, emerge la Tesis Aislada *Flujo de Información en Red Electrónica (Internet) Principio de Restricción Mínima Posible,* en México. Suprema Corte de Justicia de la Nación (Tesis 2ª. CII/2017 (10ª.) de 16 de junio de 2017), en donde se reconoce que en el orden jurídico nacional y en el derecho internacional de los derechos humanos existe el principio relativo al flujo de información por Internet, el cual debe restringirse lo mínimo posible con la finalidad de proteger la libertad de expresión y el derecho a la información, dado que le corresponde al Estado garantizarlos; en circunstancias excepcionales y limitadas, se tipifican conductas cibernéticas previstas en la ley para proteger otros derechos humanos, de lo contrario, se estarían vulnerando la libertad de expresión y el derecho a la información.

Marco Legal

México comenzó a vislumbrar temas concernientes a delitos cibernéticos mediante la reforma al Código Penal Federal (1931) con fecha 07 de noviembre de 1996, por la cual se adicionó, entre otros artículos, el artículo 211 bis, en el que se plasmó concretamente el delito de Revelación de Secretos y que tiene relación con el espionaje informático: "A quien revele, divulgue o utilice indebidamente o en perjuicio de otro información o imágenes obtenidas en una intervención de comunicación privada...", es decir, el bien jurídico protegido se enfoca directamente en los sistemas de información y en aquellos datos que se puedan obtener de los mismos.

Posteriormente, el 17 de mayo de 1999 se adicionó al Código Penal Federal el Título Noveno, que se denominó "Revelación de Secretos y Acceso Ilícito a Sistemas y Equipos de Informática", además de llevarse a cabo la adición de un segundo capítulo en el cual se establecieron siete nuevos tipos penales referentes a Equipos Informáticos:

> CAPÍTULO II, Acceso ilícito a sistemas y equipos de informática
> Artículo 211 bis 1.- Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática, protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa...
> Artículo 211 bis 2.- Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática del Estado, protegidos por algún mecanismo de seguridad, se le impondrán de uno a cuatro años de prisión y de doscientos a seiscientos días multa...

Con dicha reforma se protegieron los bienes jurídicos de las personas contra las conductas de sabotaje y espionaje informáticos, únicamente en los citados artículos 211 bis y 211 bis 1, mientras que el Estado protegió sus sistemas de información, el de sus instituciones públicas y el del sistema financiero mexicano en los artículos 211 bis 2 al 211 bis 7. Aunque no se encuentren en un capítulo específico, en México se alude a los delitos comunes o tradicionales que para su comisión se utilizan herramientas o medios tecnológicos, tales conductas son: Delitos en materia de Derechos de

autor, en el artículo 424 bis; Pornografía Infantil, en los artículos 202 al 202 bis; Violación a la Intimidad Sexual en los artículos 199 Octies al 199 Diecies, todos del Código Penal Federal.

Cabe resaltar que México aún no ha tipificado y adecuado delitos respecto a los parámetros internacionales establecidos en el convenio sobre ciberdelincuencia como lo son: robo de identidad, suplantación de (identidad) personas, software malicioso, hurto por medios electrónicos, suplantación de sitios web para capturar datos personales y transferencia no consentida de activos. Por lo cual, resulta necesario que amplíe el catálogo de delitos cibernéticos en relación con dicho convenio internacional, dado que se mantiene como observador a la fecha.

México y el Convenio de Budapest

México históricamente ha firmado diversos tratados internacionales en diferentes materias, en específico, en la temática de los derechos humanos. En cada tratado ha tenido la obligación de reformar o crear legislaciones correspondientes, para todo lo anterior tenemos como ejemplo la reforma en materia de derechos humanos publicada en el Diario Oficial de la Federación con fecha 10 de junio de 2011 la cual modificó la manera de protección de los derechos humanos de todas las personas del territorio nacional, teniendo como consecuencia, la reforma constitucional respecto a los artículos 1, 3, 11, 15, 18, 29, 33, 89, 97, 102 apartado B y 105; sin embargo, en materia de delitos cibernéticos se ha abstenido de formar parte del Convenio de Budapest, teniendo, como ya se mencionó supra, un estatus de observador, de acuerdo con el Punto de Acuerdo presentado por la senadora Silvana Beltrones Sánchez, por el que exhorta a las autoridades del Ejecutivo Federal para que se concluya la evaluación al marco jurídico vigente que permitiría cumplir cabalmente con las obligaciones contenidas en el Convenio sobre la Ciberdelincuencia (Convenio de Budapest) para la adhesión al mismo, ante la comisión de relaciones exteriores (2020):

> En el año 2006, el entonces Observador Permanente Adjunto de México hizo la solicitud formal para la adhesión de nuestro país al Convenio sobre la Ciberdelincuencia. El 31 de enero de 2007, el Comité de Ministros del Consejo de Europa, hizo la invitación conducente. No obstante, la adhesión de México al Convenio de Budapest aún no ha sido ratificada por el Ejecutivo Federal. (p. 13)

Pese a que México fue invitado a ser parte del mencionado convenio, tomó la decisión de mantenerse al margen de este, teniendo como consecuencia que el Código Penal Federal solo contemple figuras jurídicas como son: sabotaje, espionaje, pornografía, delitos en materia de derechos de autor y violación a la intimidad, dejando fuera delitos como fraude y suplantación de personas físicas o jurídico colectivas, entre otros, dado que no ha modificado sus ordenamientos jurídicos. En este contexto y de acuerdo con Víctor Ballinas y Andrea Becerril (2021):

> El Senado de la república exhortó al gobierno mexicano a concluir la etapa de evaluación del marco jurídico vigente para que México se adhiera a la Convención sobre Ciberdelincuencia o convenio de Budapest, ya que tiene más

de 10 años analizándolo para proceder a su ratificación. (párr. 1)

Siguiendo la línea anterior y, como ejemplo, se tiene el Dictamen con Punto de Acuerdo relativo al Convenio de Budapest sobre Ciberdelincuencia (2019), emitido por la Cámara de Diputados del H. Congreso de la Unión, donde exhorta al titular de la Secretaría de Relaciones Exteriores a impulsar el instrumento de adhesión para que México forme parte del multicitado convenio, argumentando lo siguiente:

> México ha utilizado el mecanismo de adhesión en nueve tratados impulsados por el Consejo de Europa, incluyendo el Convenio Europeo de Información sobre Derecho Extranjero (ratificado en 2003); el Convenio de Derecho Penal sobre la Corrupción (firmado en 2002), y el Convenio del Consejo de Europa sobre los Delitos Relacionados con los Bienes Culturales (ratificado en 2018), entre otros, los cuales ya han sido ratificados por el Senado mexicano. (p. 10)

En el mismo orden de ideas se encuentra la Proposición con Punto de Acuerdo que Exhorta al Ejecutivo Federal a enviar al Senado el Convenio de Budapest sobre Ciberdelincuencia suscrito por la Senadora Alejandra Soto (2019) en el que se invita al Ejecutivo Federal a iniciar los trabajos necesarios para la adhesión de México al convenio de Budapest. También se debe resaltar que México, al igual que Chile, comenzó a legislar en materia de delitos cibernéticos antes de la creación del convenio, específicamente con las reformas al Código Penal Federal de 1996 y de 1999, por las cuales adicionó el artículo 211 bis y el Capítulo II, Acceso Ilícito a Sistemas y Equipo de Informática, respectivamente; el primero de los mencionados guarda relación con el artículo 3. Intercepción Ilícita del Convenio sobre la Ciberdelincuencia; mientras que el Capítulo II tiene relación con los artículos 2. Acceso ilícito, 4. Ataques a la integridad de los datos y 5. Ataques a la integridad de sistemas, del Convenio sobre la Ciberdelincuencia, siendo el bien jurídico a proteger, únicamente, los sistemas informáticos y la información contenida en ellos, tomando a los delitos cibernéticos como un fin y no como un medio, ya que no se ve afectado algún otro bien jurídico de delitos tradicionales.

México, al adherirse al Convenio sobre Ciberdelincuencia de Budapest, se obligará a adecuar sus ordenamientos jurídicos en términos del convenio; sin embargo, pese a que México mantiene un estatus de "observador", ha ido más lejos en la regulación de esa temática: es el caso del delito de Pornografía de Personas de Menores de dieciocho años, regulado en el artículo 202 del Código Penal Federal, que guarda relación con el artículo 9. Delitos relacionados con la pornografía infantil del Convenio de Budapest; de la misma manera, el artículo 424 bis, fracción II, de los delitos en materia de Derechos de autor del mismo Código, establece: "A quien fabrique con fin de lucro un dispositivo o sistema cuya finalidad sea desactivar los dispositivos electrónicos de protección de un programa de computación", tiene relación con el artículo 10. Delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines del citado Convenio de Budapest.

Cabe destacar que los últimos avances en materia de regulación sobre delitos cibernéticos fueron el 1° de junio de 2021 con la "Ley Olimpia", publicada en el Diario

Oficial de la Federación, la cual trajo consigo un entramado de reformas en materia de delitos cibernéticos al Código Penal Federal y a la Ley General de Acceso de las Mujeres a una Vida Libre de Violencia (2007). En el caso del Código Penal, se adicionó el Capítulo II, Violación a la Intimidad, al Título Séptimo bis "delitos contra la Indemnidad de Privacidad de la Información Sexual", cuya finalidad es la de tipificar todas aquellas conductas que divulguen contenido íntimo sexual de una persona que tenga la mayoría de edad sin su consentimiento, esto puede ser en cualquier tipo de plataforma digital o red social. Por otra parte, la reforma realizada a la Ley General de Acceso de las Mujeres a una Vida Libre de Violencia cuya finalidad, de acuerdo con Jesika Velázquez (2020), es "reconocer y sancionar la violencia digital y la violencia mediática contra las mujeres, figuras que serán aplicables en todo el país" (párr. 10). Hay que destacar que es una innovación por parte del Estado mexicano, puesto que en los parámetros del convenio de Budapest solo se sanciona el delito de pornografía con menores de edad, mientras que, con el delito de Violencia a la Indemnidad Sexual, se protege a toda persona que tenga la mayoría de edad y a quienes se divulgue contenido íntimo sexual sin su consentimiento; dicho bien jurídico a proteger está comprendido en el Convenio de Budapest, puesto que todas las personas, mayores o menores de edad, son susceptibles de padecer la difusión de su contenido íntimo sexual sin consentimiento.

Ahora bien, cabe señalar que México es "una república... compuesta por estados libres y soberanos en todo lo concerniente a su régimen interior" (Art. 40, CPEUM), de esta manera, tanto la federación como sus estados están facultados para legislar, debido a la división de poderes y del sistema de pesos y contra pesos del sistema que lo conforma, algunos estados se han adelantado en la regulación de los delitos cibernéticos como sucede en el estado de México, la Ciudad de México, estado de Colima, entre otros, con la Ley Ingrid, que de acuerdo con la Secretaría de Gobernación (2020), en su Ficha Técnica señala:

> La "Ley Ingrid" al igual que la "Ley Olimpia" no se refiere a una ley como tal, sino a un conjunto de reformas legislativas que buscan evitar la exposición de las personas ante los medios para proteger la intimidad y dignidad de las víctimas y sus familiares, combatir la violencia mediática de género y su normalización; sancionando a las personas y servidores públicos que realicen dichas conductas. (p. 1)

En ese mismo orden de ideas tenemos al estado de Jalisco, con la reforma a su Código Penal (1982) registrada el 01 de noviembre de 2021, en su artículo 143 quater, que tipifica el delito de suplantación de identidad por cualquier medio.

c. Colombia

Marco Constitucional

En la Constitución Política de la República de Colombia (1991), publicada en el Diario Oficial de la República de Colombia, en relación con los derechos cibernéticos, tiene su fundamento en el artículo 15, el cual plasma que todas las personas tienen derecho a la

protección de datos personales, en donde el Estado debe garantizar tal derecho; asimismo, establece que se respetará la libertad de recolección, tratamiento y circulación de datos, además de que todas las formas de comunicación privada son inviolables. De la misma manera, en su artículo 20 se garantiza la libertad de expresión y de difusión. Siendo estos los dos artículos tendientes a garantizar la seguridad cibernética de los gobernados.

Marco Legal

Colombia comenzó a legislar en temas concernientes a delitos cibernéticos mediante el Decreto 1360 de 1989, publicado en el Diario Oficial de la República de Colombia, con el cual se reglamenta la inscripción del soporte lógico (software) en el Registro Nacional de Derecho de Autor, que sirvió como fundamento normativo para resolver aquellas reclamaciones por violación de tales derechos, propios de los desarrolladores de software. A partir de esa fecha se comenzó a tener acervo jurídico para proteger la producción intelectual de estos nuevos creadores de aplicativos y soluciones informáticas. Pero fue hasta 2009 que se promulgó la "Ley de Delitos Informáticos" o "Ley 1273", publicada en el Diario Oficial de la República de Colombia, por medio de la cual se modifica el Código Penal Colombiano (2000), y cuyo objetivo es la protección de datos de información y datos contenidos en sistemas informáticos. De manera general, en dicha ley se tipifican los siguientes delitos cibernéticos:

En el Artículo 269A del Código Penal Colombiano se establece el delito de acceso abusivo a un sistema informático, conducta ilícita que requiere la utilización de herramientas tecnológicas, nombrada espionaje informático, sucede cuando un individuo o grupo de individuos especializados en sistemas informáticos se introducen a los mismos con la finalidad de obtener información o bases de datos que sean útiles para cambiar por recursos económicos o hacerse de toda aquella información que sea de carácter vital, tanto para personas físicas como jurídico colectivas, que respecto a estas últimas, cuando se trata de información indispensable para el ejercicio y desarrollo de sus actividades laborales . Lo anterior en concordancia con el grupo de investigación Seguridad y Delitos informáticos (SEGUDELIN) (2010) que establece lo siguiente:

> Cuando el pirata informático o hacker aprovecha la vulnerabilidad en el acceso a los sistemas de información, o las deficiencias en los procedimientos de seguridad informática establecidos por las organizaciones, para extraer beneficios económicos o para indagar o demostrar la capacidad y recursos que ofrece la tecnología de la información. (p. 54)

En el Artículo 269B del mismo Código Colombiano (2000) se tipifica la figura del sabotaje informático, el cual consiste en impedir u obstaculizar el funcionamiento o el acceso normal a un sistema informático o datos de información contenidos en él. El objetivo de los ciberdelincuentes es despojar a los propietarios de los sistemas informáticos respecto a sus cuentas personales de correo electrónico o de sus redes sociales, en donde existen demasiados datos, configurando a su vez otro delito: el de extorsión, que ocurre cuando los delincuentes cibernéticos obtienen recursos econó-

micos ilícitos al presionar con amenazas a los propietarios para poder regresarles sus sistemas informáticos o redes sociales, esto tratándose de las personas físicas. La intercepción de datos informáticos es una figura jurídica que se implementó en el referido Código Penal Colombiano derivado de la "Ley 1273", en su artículo 269C:

> La intercepción deliberada e ilegítima por medios 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 datos informáticos.

Respecto a lo anterior, se denota que dicha conducta cibernética tiene como finalidad la intercepción por parte del ciberdelincuente a un sistema de información denominado de "origen" con el objetivo de modificar, obtener y obstruir la información emitida por el mismo, repercutiendo directamente en la confidencialidad tanto de personas físicas como jurídico colectivas, teniendo íntima relación con el artículo 269A, dado que en ambos artículos se pretende proteger la información y los datos contenidos con carácter de reservado en el sistema informático tanto de empresas como de los individuos. De igual manera, el artículo 269D consistente en el daño informático nos habla de "aquellas personas que, sin estar facultadas para ello, destruyan, dañen, borren, deterioren, alteren o supriman datos informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos"; se puede establecer que consiste en el sabotaje informático en concordancia con el ya citado artículo 269B.

En la referida ley se introduce el delito de malware, en el artículo número 269E, es cuando el ciberdelincuente produce, adquiere, vende envía, distribuye o introduce programas, mejor conocidos como virus, a los sistemas informáticos que desea para generar un daño irreversible; dichos programas pueden ser utilizados directamente para la obtención de bases de datos, ya que es posible entrar a los softwares de las personas jurídico-colectivas o personas físicas.

El artículo 269F respecto a la conducta ilícita de violación de datos personales, mejor conocido como Hackeo o Hacking informático, consiste en que el ciberdelincuente acceda sin ningún consentimiento a algún sistema informático o red social para la obtención de datos, en este caso se tratan de datos personales, aunado a lo anterior, Yenifer Bechara, Alan Mosquera y Edwar Ledezma (2020) consideran que el artículo está "orientado a proteger los derechos fundamentales de la persona como dignidad humana y libertad ideológica". (p. 37)

El último artículo del primer capítulo, 269G, consiste en un término actual e innovador para cometer delitos: el *Phishing*, que en el Código Penal Colombiano es denominado como suplantación de sitios web para capturar datos personales, lo cual se relaciona de manera directa con el artículo 269J del segundo capítulo de dicha ley, el cual hace referencia a "la transferencia no consentida de activos, generando manipulación de información bancaria con el ánimo de lucro, esto, sin el consentimiento del propietario de dicha información". Por último, en el artículo 269I del segundo capítulo

se incorpora la conducta ilícita de hurto por medios informáticos y semejantes, el cual consiste en:

> Aquellas personas que superando medidas de seguridad informáticas realicen dicha conducta manipulando un sistema informático, teniendo como consecuencia que la persona que se introduzca sin consentimiento alguno pueda apoderarse de una cosa mueble ajena, con el propósito de obtener provecho para sí o para otro.

Colombia y el Convenio de Budapest

El 24 de julio de 2018 la República de Colombia, por medio de su Congreso, aprueba la Ley 1928 (2018), con la cual aprueba el Convenio sobre la Ciberdelincuencia, sin embargo, uno de los requerimientos para poder adherirse a dicho convenio es presentar el instrumento de adhesión ante el Consejo de Europa en Estrasburgo, ante ello, de acuerdo con el mismo Consejo de Europa (2019):

> El 3 de enero de 2018, la Sra. María Ángela Holguín Cuellar, Ministra de Relaciones Exteriores de Colombia, solicitó una prórroga del plazo de adhesión de Colombia al Convenio sobre la Ciberdelincuencia (RCDE Nº 185), hasta el 12 de septiembre de 2020, a fin de disponer del tiempo necesario para completar el proceso interno de adhesión. (párr. 2)

De esta manera, Colombia presentó su instrumento de adhesión en fecha 16 de marzo de 2020, entrando en vigor el 01 de julio de 2020. No obstante, aun cuando Colombia no estaba adherido al Consejo de Europa, por medio de la Ley 1273 publicada en año de 2009 se adoptaron los términos del Convenio sobre la Ciberdelincuencia en la legislación nacional, y de acuerdo con el Consejo de Europa (2021), en la contestación de la solicitud para adherirse al Convenio, las adecuaciones que se hicieron son las siguientes:

Tabla 1: *Que contiene algunas disposiciones del Convenio de Budapest en relación con la Ley 1273 de la república de Colombia*

Convenio de Budapest	Equivalente en la Legislación Nacional de Colombia
Art. 2. Acceso ilícito	Art. 269ª. Acceso abusivo a un sistema informático (Ley 1273)
Art. 3. Interceptación ilícita	Art. 269C. Interceptación de datos informáticos (Ley 1273)
Art. 4. Ataques a la integridad de datos	Art. 269D. Daño Informático (Ley 1273)
Art. 5. Ataques a la integridad del sistema	Art. 269D- Daño Informático (Ley 1273)
Art. 6. Abuso de dispositivos	Art. 269E. Uso de software malicioso Art. 269G. Suplantación de sitios web para capturar datos personales (Ley 1273)
Art. 8. Fraude informático	Art. 269I. Hurto por medios informáticos y semejantes Art. 269J. Transferencia no consentida de activos (Ley 1273)
Art. 9. Delitos relacionados con la pornografía infantil	Art. 218. Pornografía con personas menores de 18 años (Ley 1273) Art. 219A. Utilización o facilitación de medios de comunicación para ofrecer servicios sexuales de menores (Código Penal)

Art. 10. Delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines	Art. 272. Violación a los mecanismos de protección de los derechos patrimoniales de autor y otras defraudaciones. (Código Penal)

Fuente: Elaboración propia con información tomada del Convenio de Budapest y la Ley 1273.

Ahora bien, aunque los delitos establecidos en los artículos 269B y 269F de la Ley 1273 no están expresamente contemplados por el Convenio de Budapest, consideramos que sí tienen una relación muy estrecha: el artículo 269B se vincula con el artículo 5-Ataques a la integridad del sistema, respecto a la obstaculización deliberada e ilegítima del funcionamiento de un sistema informático; mientras que el artículo 269F guarda relación con el artículo 2-Acceso Ilícito, derivada de la intención de obtener datos informáticos u otra intención delictiva, con la sustracción de datos personales establecida en la legislación de Colombia. Asimismo, se detectó que aquí aún falta por legislar en la materia de falsificación informática.

IV. ANÁLISIS COMPARATIVO DE LOS DELITOS CIBERNÉTICOS EN CHILE, MÉXICO Y COLOMBIA

A continuación, se hará un análisis comparado en la legislación de los referidos países, tomando como base la Ley 17.336, la Ley 19.223 y la Ley 19.927 publicadas en el Diario Oficial de la República de Chile, el 02 de octubre de 1970, el 07 de junio de 1993 y el 14 de enero de 2004, respectivamente. Asimismo, el Código Penal Federal mexicano publicado en el DOF el 14 de agosto de 1931, y la Ley 1273 de 2009 publicada el 05 de enero de 2009, en el Diario Oficial de la República de Colombia.

Tabla 2*: Relación de la legislación de Chile, México y Colombia, para determinar las semejanzas y diferencias entre los antecitados ordenamientos sobre los delitos cibernéticos*

Chile			México			Colombia		
Delito	**Bien Jurídico Tutelado**	**Legislación**	**Delito**	**Bien Jurídico Tutelado**	**Legislación**	**Delito**	**Bien Jurídico Tutelado**	**Legislación**
Contra la Propiedad Intelectual	Obras de dominio ajeno protegidas por esta ley, inéditas o publicadas	Artículo 79° de la Ley de Propiedad Intelectual, Ley 17.336	**Revelación de secretos**	Información o imágenes obtenidas en una intervención de comunicación privada	Artículo 211 bis del Código Penal Federal	**Acceso Abusivo a un Sistema Informático**	Sistema informático protegido o no con una medida de seguridad	Artículo 269A Ley 1273 de 2009

Sabotaje Informático	Sistema de tratamiento de información o sus partes o componentes	Artículos 1° y 3° de la Ley que tipifica Figuras Penales Relativa a la Informática, Ley 19.223	**Acceso ilícito a sistemas y equipos de informática**	Información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad	**Artículo 211 bis 1 del Código Penal Federal**	**Obstaculización Ilegítima de Sistema Informático o Red de Telecomunicación**	Sistema informático, los datos informáticos allí contenidos, o a una red de telecomunicaciones	Artículo 269B Ley 1273 de 2009
Espionaje Informático	La información contenida en un sistema de tratamiento de información o sus partes o componentes	Artículo 2° y 4° de la Ley que tipifica Figuras Penales Relativa a la Informática, Ley 19.223	**Acceso ilícito a sistemas y equipos de informática del Estado**	Información contenida en sistemas o equipos de informática del Estado, protegidos por algún mecanismo de seguridad	**Artículos del 211 bis 2 y 211 bis 3 del Código Penal Federal**	**Interceptación de Datos Informáticos**	Datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático	Artículo 269C Ley 1273 de 2009
Pornografía Infantil	La libertad e intimidad sexual	Artículo 366 quinquies de la Ley de Delitos de Pornografía Infantil, Ley 19.227	**Acceso ilícito a sistemas y equipos de informática de las instituciones que integran el sistema financiero**	Información contenida en sistemas o equipos de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad	Artículos del 211 bis 4 al 211 bis 7 del Código Penal Federal	**Daño Informático**	Datos informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos	Artículo 269D Ley 1273 de 2009
			Violación a la intimidad sexual	La intimidad sexual	Artículo 199 Octies del Código Penal Federal	**Uso de Software Malicioso**	Software u otros programas de computación	Artículo 269E Ley 1273 de 2009
			Pornografía infantil	La intimidad sexual	Artículo 202° del Código Penal Federal	**Violación de Datos Personales**	Datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes	Artículo 269F Ley 1273 de 2009

						Suplantación de Sitios Web para Capturar Datos Personales	Datos Personales	Artículo 269G Ley 1273 de 2009
						Hurto Por Medios Informáticos y Semejantes	Sistema informático, una red de sistema electrónico, telemático u otro medio semejante	Artículo 269I Ley 1273 de 2009
						Transferencia no Consentida de Activos	Cualquier activo	Artículo 269J Ley 1273 de 2009
						Pornografía Infantil	La libertad e intimidad sexual	Art. 218 de la Ley 1273 y Art. 219A del Código Penal
						Violación a los mecanismos de protección de los derechos patrimoniales de autor y otras defraudaciones	Obras de carácter literario, artístico, científico, cinematográfico, audiovisual o fonograma	Art. 272 del Código Penal

Fuente: Elaboración propia con información tomada de las leyes *supra* mencionadas.

Como se desprende de la Tabla 2, las semejanzas que se encontraron de los delitos cibernéticos entre Chile, México y Colombia son: el sabotaje informático, el espionaje informático y los delitos contra la propiedad intelectual y la pornografía infantil, en donde, incluso en el contenido de sus artículos, respectivamente, se encuentran bastantes similitudes. Chile no contiene dentro de sus legislaciones algún delito cibernético que lo diferencie de México y Colombia, esto porque se está trabajando en el proyecto que reforma a la Ley 19.223, para así poder adecuar su derecho interno a los términos de lo establecido en el Convenio de Budapest, dado que dicha ley (como ya se hizo mención en el cuerpo del presente trabajo) solo contempla los delitos cibernéticos concernientes al sabotaje y espionaje informático, además de los delitos contra la propiedad intelectual y la pornografía infantil, mientras que Colombia y México cuentan en sus ordenamientos jurídicos con delitos cibernéticos diferentes a los establecidos en la legislación chilena. En efecto, en México se crea una figura jurídica que lo diferencia de Chile, Colombia y el propio Convenio, puesto que

estos solo contemplan la pornografía infantil; lo anterior no obstante que, como ya se refirió, mantiene un estatus de observador ante el Convenio de Budapest, derivado de la reforma a la Ley Olimpia con la que introdujo el delito de violación a la intimidad sexual.

Por su parte, Colombia es el país que más sobresale con la regulación de los delitos cibernéticos, frente a Chile y México, pues enuncia delitos tales como: uso de software malicioso, violación de datos personales, suplantación de sitios web para capturar datos personales, hurto por medios electrónicos y semejantes y transferencias no contenciosas de artículos; no obstante, en términos de lo establecido por el Convenio, aún le falta por introducir a su legislación el delito de Fraude informático. Por lo anterior, Colombia es el país que más adecuaciones ha realizado en términos de lo establecido en el Convenio de Budapest, esto en concordancia con la Exposición de Motivos del Proyecto de Ley 1928 (2018), la cual señala:

> Por medio de la Ley 1273 del 2009 se adoptan lineamientos del Convenio de Budapest celebrado en el año 2001. La decisión, de proferir las leyes internas en concordancia al Convenio sobre la Ciberdelincuencia, fue tomada por considerarse de vital importancia que los desarrollos normativos incluyeran esas directrices de la legislación europea... (p. 30).

REFLEXIONES FINALES

En este ejercicio académico se logró el objetivo de investigar y analizar los delitos cibernéticos regulados por Chile, México y Colombia, al amparo de sus respectivos ordenamientos constitucionales y legales. Asimismo, por en la Tabla II se indicaron los avances de cada uno de esos países en el tema, estableciendo sus semejanzas y diferencias. También se determinó el progreso que hasta el momento han logrado esos países en la regulación de lo mencionado, para lo cual tomamos como parámetro los compromisos contemplados por el Convenio de Budapest sobre la ciberdelincuencia. No obstante que Chile, México y Colombia han avanzado en la regulación sobre el tema de la ciberdelincuencia, los dos primeros no han hecho propiamente las adecuaciones a su respectivo marco constitucional y legal en términos de los parámetros establecidos en el Convenio sobre Ciberdelincuencia, pues Chile apenas el 6 de octubre de 2021 conformó una Comisión Mixta para analizar el proyecto de ley que modernice su legislación en esa materia. Por lo que se refiere a México, aún no se adhiere al multicitado Convenio y, en cuanto a Colombia, el Convenio entró en vigor desde el 1 de julio de 2020, aunque desde la citada Ley 1273 del 2009 adoptó algunos lineamientos del multicitado Convenio sobre ciberdelincuencia.

REFERENCIAS

1. Amézquita, R. (31 de octubre de 2020). El problema constitucional, derechos humanos y la necesidad de una Convención Constitucional en Chile. *Derechos fundamentales a debate,* Comisión Estatal de Derechos Humanos Jalisco, pp. 68-104. http://cedhj.org.mx/revista%20DF%20Debate/articulos/revista_No14/ADEBATE-14-art3.pdf

2. Ardissom de Souza, R. (2018). De las redes al ciberespacio. *Revista Digital Universitaria,* 2(19), pp. 1-11. Recuperado de http://www.revista.unam.mx/wp-content/uploads/v19_n2_a2.pdf

3. Argüelles, M. (2016). Retos de la legislación informática en México. *Computación y Sistemas, Instituto Tecnológico de Zacatecas,* 4(20), pp. 827-831. Recuperado de http://www.scielo.org.mx/pdf/cys/v20n4/1405-5546-cys-20-04-00827.pdf

4. Ballinas, V. y Becerril, A. (15 de septiembre de 2021). Urgen a que México firme el Convenio de Budapest. *La Jornada.* Recuperado de https://www.jornada.com.mx/notas/2021/09/15/politica/urgen-a-que-mexico-firme-el-convenio-de-budapest/

5. Barrios, V., y Vargas, A. (2018). Convenio sobre la Ciberdelincuencia: Convenio de Budapest. *Biblioteca del Congreso Nacional de Chile*, pp. 1-12. Recuperado de http://bcn.cl/2mq07

6. Bechara, Y., Mosquera, A. y Ledezma, E. (2020). *Análisis Jurídico de la Ley 1273 del 2009 y el Surgimiento y Expansión del Delito de Hurto y Semejantes por Medios Informáticos* [tesis de licenciatura, Facultad de Derecho de la Universidad Cooperativa de Colombia]. Repositorio UCC. Recuperado de https://repository.ucc.edu.co/bitstream/20.500.12494/19788/3/2020_analisis_delitos_informaticos.pdf

7. Becker, S. y Viollier, P. (2020). La Implementación del Convenio de Budapest en Chile: un Análisis a Propósito del Proyecto Legislativo que Modifica la Ley 19.223. *Revista de Derecho,* (248), pp. 75-112. Recuperado de https://scielo.conicyt.cl/scielo.php?script=sci_abstract&pid=S0718-591X2020000200075&lng=es&nrm=iso

8. Código Penal de la República de Chile (12 de noviembre de 1874). Diario Oficial de la República de Chile, Congreso de la república de Chile. Recuperado de https://www.bcn.cl/leychile/navegar?idNorma=1984&idVersion=2021-02-03&idParte=10131189

9. Código Penal de la República de Colombia (24 de julio de 2000). Diario Oficial de la República de Colombia, Congreso de la República de Colombia. Recuperado de http://www.secretariasenado.gov.co/senado/basedoc/ley_0599_2000.html

10. Código Penal Federal (14 de agosto de 1931). Diario Oficial de la Federación, Congreso de los Estados Unidos Mexicanos Recuperado de http://www.diputados.gob.mx/LeyesBiblio/pdf/CPF.pdf

11. Código Penal para el Estado Libre y Soberano de Jalisco (2 de noviembre de 1982). Congreso del Estado de Jalisco. Recuperado de https://transparencia.info.jalisco.gob.mx/sites/default/files/Código%20Penal%20para%20el%20Estado%20Libre%20y%20Soberano%20de%20Jalisco%20(1).pdf

12. Constitución Política de la República de Chile (1980). Diario Oficial de la República de Chile. Recuperado de http://extwprlegs1.fao.org/docs/pdf/chi127261.pdf

13. Constitución Política de la República de Colombia (1991). Diario Oficial de la República de Colombia. Recuperado de http://www.secretariasenado.gov.co/index-.php/constitucion-politica

14. Constitución Política de los Estados Unidos Mexicanos (1917). Diario Oficial de la Federación. Recuperado de http://www.diputados.gob.mx/LeyesBiblio/pdf/1_280521.pdf

15. Convenio sobre la Ciberdelincuencia (23 de noviembre de 2001). Serie de Tratados Europeos, Consejo de Europa (185). Recuperado de https://www.oas.org/juridico/english/cyb_pry_convenio.pdf

16. Dávila, Y. (s.f.). Delitos Cibernéticos en el Derecho Colombiano y desde la Perspectiva del Derecho Comparado. *Artículo de Investigación de la Universidad Católica de Colombia*, pp. 1-33. Recuperado de https://repository.ucatolica.edu.co/bitstream/10983/24446/1/2111214-Davila-SuanchaYC-delitos-inform%C3%A1ticos-en-derecho-colombiano-Articulo.pdf

17. Diario Oficial de la República de Colombia (23 de junio de 1989). Decreto 1360 de 1989. Por el cual se Reglamenta la Inscripción del Soporte Lógico (Software) en el Registro Nacional del Derecho de Autor. Recuperado de https://www.funcionpublica.gov.co/eva/gestornormativo/norma_pdf.php?i=10575

18. Diario Oficial de la República de Chile (28 de agosto de 2017). Decreto 83. Por el cual se Promulga el Convenio sobre Ciberdelincuencia. Ministerio de Relaciones Exteriores de la República de Chile. Recuperado de https://www.bcn.cl/leychile/navegar?idNorma=1106936

19. Diario Oficial de la Federación (01 de junio de 2021). Decreto. Por el cual se adicionan diversas disposiciones a la Ley General de Acceso de las Mujeres a una Vida Libre de Violencia y al Código Penal Federal. Recuperado de https://www.dof.gob.mx/nota_detalle.php?codigo=5619905&fecha=01/06/2021

20. Diario Oficial de la Federación (10 de junio de 2011). Decreto. Por el cual se modifica la denominación del Capítulo I del Título Primero y reforma diversos artículos de la Constitución Política de los Estados Unidos Mexicanos. Recuperado de http://www.dof.gob.mx/nota_detalle.php?codigo=5194486&fecha=10/06/2011

21. Esteinou, J. y Alva, A. (2011). *Los medios electrónicos de difusión y la sociedad de la información.* Dirección General del Acervo Histórico Diplomático, Secretaría de Relaciones Exteriores.

22. Diario Oficial de la República de Colombia (24 de julio de 2018). Exposición de motivos del proyecto de Ley 1928 por medio de la cual se aprueba el Convenio sobre la Ciberdelincuencia, adoptado el 23 de noviembre de 2001. Recuperado de http://www.suin-juriscol.gov.co/imagenes//31/07/2018/1533072070593_Anexo%202%20Ley%201928.pdf

23. Fernández, H. (2014). *Manual de Derecho Informático.* Buenos Aires, Argentina: Abeledo Perrot.

24. Grupo de Investigación Seguridad y Delitos Informáticos (SEGUDELIN) (2010). Delitos informáticos y entorno jurídico vigente en Colombia: CUAD. CONTAB., 11(28), pp. 41-66. Recuperado de http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S0123-14722010000200003

25. Cámara de Diputados de los Estados Unidos Mexicanos (2019). Dictamen con Punto de Acuerdo. Relativo al Convenio de Budapest sobre Ciberdelincuencia. Comisión de Relaciones Exteriores. Recuperado de http://www5.diputados.gob.mx/index.php/esl/content/download/168058/838814/file/9e_Art_72_Fr_IX_LVotpropoBudap.pdf

26. Hiplan, S. (2019). La Ley 19.223 a 26 Años de su Promulgación [tesis de licenciatura, Facultad de Derecho de la Universidad de Chile]. Repositorio UChile. Recuperado de https://repositorio.uchile.cl/bitstream/handle/2250/173119/La-ley-N%c2%b019223-a-26-a%c3%b1os-de-su-promulgacion.pdf?sequence=1&isAllowed=y

27. Lara, J., Martínez, M. y Viollier, P. (2014). Hacia una regulación de los delitos informáticos basada en la evidencia. *Revista Chilena de Derecho y Tecnología,* 1(3), pp. 101-137. Recuperado de https://rchdt.uchile.cl/index.php/RCHDT/article/view/32222/34151

28. Diario Oficial de la República de Chile (02 de octubre de 1970). Ley 17.336. Por la cual se expide la Ley de Propiedad Intelectual. Congreso de la República de Chile. Recuperado de https://www.bcn.cl/leychile/navegar?idNorma=28933

29. Diario Oficial de la República de Chile (07 de junio de 1993). Ley 19.223 por la cual se expide la Ley que Tipifica Figuras Penales Relativas a la Informática. Congreso de la República de Chile. Recuperado de https://www.bcn.cl/leychile/navegar?idNorma=30590&buscar=ley%2B19223

30. Diario Oficial de la República de Chile (14 de enero de 2004). Ley 19.927. Por la cual se expide la Ley que Modifica el Código Penal, El Código de Procedimiento Penal y El Código Procesal Penal en Materia de Delitos de Pornografía Infantil. Congreso de la República de Chile. Recuperado de https://www.bcn.cl/leychile/navegar?idNorma=220055

31. Diario Oficial de la Republica de Colombia (24 de julio de 2018). Ley 1928. Por medio de la cual se aprueba el Convenio sobre la Ciberdelincuencia, adoptado el 23 de noviembre de 2001, en Budapest. Congreso de la República de Colombia. Recuperado de http://www.secretariasenado.gov.co/senado/basedoc/ley_1928_2018.html

32. Diario Oficial de la Federación. (01 de febrero de 2007). Ley General de Acceso de las Mujeres a una Vida Libre de Violencia. Congreso de los Estados Unidos Mexicanos. Recuperado de http://www.diputados.gob.mx/LeyesBiblio/pdf/LGAMVLV_010621.pdf

33. Diario Oficial de la República de Colombia (05 de enero de 2009). Ley 1273 de 2009. Por medio de la cual se Modifica el Código Penal, se crea un nuevo bien jurídico tutelado –denominado "De la Protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones. Congreso de la República de Colombia. Recuperado de https://www.enticconfio.gov.co/images/stories/normatividad/Ley_1273_de_2009%20.pdf

34. México. Suprema Corte de Justicia de la Nación (16 de junio 2017). Tesis 2ª. CII/2017 (10ª.). Flujo de información en red electrónica (internet). Principio de restricción mínima posible. Semanario Judicial de la Federación.

35. Piña, L. H. R. (2019). Cibercriminalidad y ciberseguridad en México. *Revista Ius Comitiãlis,* 4(2), pp. 47-69. Recuperado de https://iuscomitialis.uaemex.mx/article/view/13203

36. Portal del Consejo de Europa (2019). Convenio sobre la Ciberdelincuencia (ETS Nº 185) –Solicitud de Colombia de prórroga del plazo de adhesión. Consejo de Europa. Comité de Ministros. Recuperado de https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=090000168078b843

37. Portal del Consejo de Europa (2021). Convenio del Consejo de Europa sobre la Ciberdelincuencia (ETS Nº 185) –*Solicitud de la República de Colombia para ser invitada a adherirse. Consejo de Europa.* Comité de ministros. Recuperado de https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805c104d

38. Roxin, C. (1997). *Derecho Penal, Parte General, Tomo I, Fundamentos. La Estructura de la Teoría del Delito.* España: Civitas.

39. Santos, A. y Teixeira, R. (2020). *Delitos Cibernéticos Nociones Básicas.* Brasil: SEGEN.

40. Presidencia de la República de Chile (2018). Boletín Nº 12.192-25. Proyecto de ley, iniciado en mensaje de S. E. el Presidente de la República, que establece normas sobre delitos informáticos, deroga la ley Nº 19.223 y modifica otros cuerpos legales con el objeto de adecuarlos al convenio de Budapest. *MENSAJE Nº 164-366/.* Recuperado de https://alertas.directoriolegislativo.org/wp-content/uploads/2019/08/12192-25.pdf

41. Senado de la República de Chile (06 de octubre de 2021). *Proyecto que moderniza normas sobre delitos informáticos será analizado por una Comisión Mixta.* Chile: Senado de la República de Chile. Recuperado de https://www.senado.cl/proyecto-que-moderniza-normas-sobre-delitos-informaticos-sera-analizado

42. Senado de la República de los Estados Unidos Mexicanos (10 de septiembre 2019). Proposición con Punto de Acuerdo que Exhorta al Ejecutivo Federal a Iniciar, a través de un Proceso de Múltiples Partes Interesadas, los trabajos necesarios para la adhesión de México al Convenio sobre La Ciberdelincuencia, o Convenio de Budapest. Ciudad de México. México: Senado de la República LXIV Legislatura. Recuperado de http://sil.gobernacion.gob.mx/Archivos/Documentos/2019/09/asun_3907851_20190918 _1568820339.pdf

43. Velázquez, J. (09 de diciembre de 2020). *Ley Olimpia.* Instituto de Investigaciones Jurídicas de la Universidad Nacional Autónoma de México. Recuperado de https://revistas.juridicas.unam.mx/index.php/hechos-y-derechos/article/view/15277/16356