Tribunal
Revista en Ciencias de la Educación y Ciencias Jurídicas

ISSN: 2959-6513 - ISSN-L: 2959-6513
Volumen 1 No. 2 / Julio - diciembre 2021
Páginas 104 - 121

Tipificación de nuevos delitos informáticos

Classificationof new computercrimes

Classificação dos novos crimes informáticos

Loredana Castiglion Basagoitia
loredanita6@gmail.com
https://orcid.org/0000-0002-8348-3620
Universidad Privada del Valle, Sucre, Bolivia

http://doi.org/10.59659/revistatribunal.v.1i2.11

Recibido abril 2021 / Arbitrado en mayo 2021 / Aceptado en junio 2021 / Publicado julio 2021

Resumen

A nivel mundial los delitos informáticos evolucionan de manera acelerada, causando vacíos legales que obstaculizan el dictamen de sanciones. En este contexto, el objetivo de este artículo fue establecer la necesidad de la tipificación de nuevos delitos informáticos en el Código Penal Boliviano. Se efectuó el análisis normativo y doctrinal, tanto internacional como nacional, con énfasis en las legislaciones boliviana, argentina y colombiana. Como resultado se evidenció que existe un vacío legal en Bolivia en lo que respecta a la tipificación de delitos informáticos. Asimismo, existen países vecinos, como es el caso de Argentina, que ya están actualizando sus normas. Resalta la necesidad de incorporar nuevos delitos informáticos en los arts 363 (bis), 363 (ter) y siguientes del Código Penal, asimismo se deberá modificar la Ley de Servicios Financieros. Finalmente se concluye que estas actualizaciones normativas deberán ir acompañadas de educación ciudadana.

Palabras clave:

Delitos informáticos; Derecho comparado; Derecho penal; Vacío legal; Internet; Redes sociales

Abstract

Globally, cybercrime evolves rapidly, causing loopholes that hamper the issuance of sanctions. In this context, the objective of this article was to establish the need for the classification of new computer crimes in the Bolivian Penal Code. The normative and doctrinal analysis was carried out, both international and national, with emphasis on Bolivian, Argentine and Colombian legislation. As a result, it was evidenced that there is a legal vacuum in Bolivia about the classification of computer crimes. Likewise, there are neighboring countries, such as Argentina, that are already updating their regulations. It highlights the need to incorporate new computer crimes into articles 363 (bis) and 363 (ter) and following of the Bolivian Penal Code, and the Financial Services Law must also be modified. Finally, it is concluded that these normative updates must be accompanied by citizenship education.

Keywords:

Cybercrime; Comparative law; Criminal law; Legal gap; Internet; Social media

Resumo

Globalmente, os crimes de computador estão evoluindo rapidamente, causando brechas legais que impedem a emissão de sanções. Nesse contexto, o objetivo deste artigo foi estabelecer a necessidade de tipificação dos novos crimes informáticos no Código Penal boliviano. Foi realizada a análise normativa e doutrinária, tanto internacional quanto nacional, com ênfase na legislação boliviana, argentina e colombiana. Como resultado, ficou evidenciado que existe um vácuo jurídico na Bolívia quanto à tipificação dos crimes informáticos. Da mesma forma, existem países vizinhos, como a Argentina, que já estão atualizando suas normas. Destaca a necessidade de incorporar novos crimes informáticos nos artigos 363.º bis, 363.º ter) e seguintes do Código Penal, devendo igualmente ser alterada a Lei dos Serviços Financeiros. Por fim, conclui-se que essas atualizações regulatórias devem ser acompanhadas de educação cidadã.

Palavras-chave

Crimes informáticos; lei comparativa; Direito Penal; vazio jurídico; Internet; Redes sociais

INTRODUCCIÓN

Las sociedades, en su constante desarrollo, se enfrentan a diferentes conflictos que dan lugar a nuevas normas creadas para regular la conducta humana y el nuevo escenario, para así poder crear un ambiente de armonía. Es así como desde la edad moderna el mundo se enfrenta a un dilema llamado tecnología y desde la edad contemporánea al internet que, si bien produce efectos positivos en diferentes áreas, favorece una serie de problemas que afectan a la sociedad, sin barreras geográfica o culturales. Diferentes países alrededor del mundo se han preocupado por la facilidad de comunicación entre desconocidos y los riesgos que esto implica (García-Piña, 2008; Ojeda-Pérez et al., 2010).

A partir del año 1969, tras el surgimiento del internet, se identificaron fallas como el primer virus fue creado en 1988 accidentalmente mediante una falla en su código eque intentaba averiguar las contraseñas de otras computadoras bajo una rutina de búsqueda (Loredo & Ramírez, 2013). Actualmente existe una serie de ataques informáticos y otros usos indebidos del internet y las redes virtuales; paulatinamente los países van adaptando normativa legal para frenar y castigar hechos ilícitos en este ámbito. Algunos países se adecúan de manera más ágil que otros.

En el caso boliviano, el internet llegó en 1989 e inicialmente fue de uso exclusivamente académico, mientras se extendía en el país, en otros países ya estaban lidiando con ataques informáticos significativos tales como el ciberterrorismo (Gómez, 2016);en la actualidad el internet se ha vuelto indispensable en la vida cotidiana, así como facilitó la comunicación también generó riesgos y actos de mala fe que no son penalizados. El Código Penal Boliviano (1997) está desactualizado siendo que los delitos informáticos que se encuentran comprendidos no son suficientes para lograr una protección jurídica a la sociedad actual. La ley que introdujo los delitos informáticos fue la Ley N° 1768 del 10 de marzo de 1997(Código Penal Boliviano, 1997), en el título de “delitos informáticos” y sus artículos 363 (bis) y 363 (ter).La última ley que modificó esta parte fue la Ley N° 393 del 21 de agosto de

2013, al añadir a los delitos financieros en el artículo 363 (quater). Entre 2013 y 2021 las modalidades de delitos contempladas en la legislación internacional han incorporado una serie de nuevas prácticas que, naturalmente, no están registradas en el Código Penal de Bolivia.

En este país se presentan más casos relacionados a las redes sociales, aunque se puede contar con la acción de protección a la privacidad, ésta no es suficiente para lograr abarcar la cantidad de delitos que se vienen suscitando. La normativa legal y las autoridades no se encuentran actualizadas y capacitadas. En el marco de esta problemática, el objetivo de este estudio fue establecer la necesidad de la tipificación de nuevos delitos informáticos en el Código Penal Boliviano (1997), además de capacitar a las autoridades frente a esta nueva modalidad.

MÉTODO

Con un enfoque sociocrítico y alcance descriptivo, se abordó la importancia de la tipificación de nuevos delitos informáticos en Bolivia, concentrando el análisis en el ámbito penal, para así proponer formas de prevención y protección ante ciertos ataques.

El estudio se desarrolló en cuatro apartados: [1] base teórica referente a delitos informáticos; [2] derecho comparado; [3] marco legal en Bolivia; [4] propuesta de ley. Mediante el derecho comparado se analizaron las legislaciones de Argentina, Colombia y Chile.

La fundamentación normativa y legal interna se respalda en los siguientes documentos: Código Penal Boliviano Ley No 1768 (1997); Ley 19.223 (1993); Ley 548 Código Niño Niña Adolescente (2014); Ley No 393 de Servicios Financieros (2013) y la Sentencia Constitucional Plurinacional 0819/2015-S3 (2015). El derecho comparado se estableció mediante el análisis de las siguientes normas: Colombia, Ley N 1273 (2009); Argentina, Ley 26904 (2013); Chile, Ley 19223 (1993). Finalmente, se buscó sustento internacional en: el Acuerdo para la Represión de la Circulación de Publicaciones Obscenas (1910); el Convención Americana sobre

derechos humanos (1969); el Convenio de Budapest (Consejo de Europa, 2001); el Convenio para la Represión de la Circulación y el Tráfico de Publicaciones Obscenas (1923).

RESULTADOS

El abordaje se presenta en cuatro apartados: base teórica referente a delitos informáticos; derecho comparado; marco legal en Bolivia; propuesta de ley.

Delitos informáticos

Los delitos informáticosson acciones antijurídicas que se ejecutan mediante vías informáticas; con la tecnología como medio, como objeto o como bien jurídico protegido (Galán, s.f.). Intervienen las nuevas tecnologías de la información, como ser las redes sociales, aplicaciones para celulares, computadoras, tablets, etc, y las diferentes páginas web; la definición de delitos informáticos tiende a ampliarse, puesto que en algunos países hacen una diferencia entre delitos informáticos y delitos computacionales según el fin que persiguen cada uno.

Los delitos informáticos reconocidos por foro de seguridadde las naciones unidas (ONU, 2015) son:manipulación de los datos de entrada;manipulación de programas;manipulación de los datos de salida;fraude efectuado por manipulación informática;falsificaciones informáticas; sabotaje informático; virus; gusanos; bomba lógica o cronológica; acceso no autorizado a sistemas o servicios; hackeo y; reproducción no autorizada de programas informáticos de protección legal.

La Organziación de las Naciones Unidas (ONU), en su 13° congreso sobre la Prevención del Delito y Justicia Penal del 12 al 19 de abril del 2015, trató el tema de la ciberdelincuencia considerando que en el manual mencionado solo se había tratado a los delitos informáticos. Aclaran:

> En 1994, en el Manual de las Naciones Unidas sobre Prevención y Control de Delitos Informáticos se señaló que el potencial de la delincuencia informática es tan amplio como el de los propios sistemas internacionales de telecomunicaciones. Como era de esperar, la palabra "Internet" aparecía solo una vez en el Manual y la palabra "ciberdelincuencia" no se utilizó; sin embargo, las conclusiones demostraron una gran visión de futuro. Si bien el manual centró su atención en el concepto de "delito informático", es bien sabido que hoy en día la "ciberdelincuencia" recurre efectivamente a las tecnologías globalizadas de la información y las comunicaciones, en particular a Internet, para la comisión de actos delictivos de alcance transnacional.
>
> Con la evolución de la terminología se han realizado esfuerzos para formular una definición académica del término "ciberdelincuencia". Un enfoque moderno de la cuestión consiste en reconocer que la ciberdelincuencia no es necesariamente un término jurídico técnico, sino más bien un término genérico para referirse a un conjunto de hechos cometidos en contra o a través del uso de datos o sistemas informáticos. Otros enfoques se centran en los delitos contra la información computadorizada o el uso de recursos de información con fines ilícitos. (ONU, 2015, p.. 6).

También hace referencia a actos que se encuentran comprendidos dentro de lo que es la ciberdelincuencia, y puntualiza en que si bien un delito informático puede tener como objeto el ataque a un servidor, también se utiliza como instrumento para llegar a cometer otros ilícitos.

> Los actos comprendidos habitualmente en la categoría de “ciberdelincuencia” son aquellos en los que los datos o sistemas informáticos son el objeto contra el que se dirige el delito, así como los actos en que los sistemas informáticos o de información forman parte integrante del modus operandi del delito. Algunos ejemplos de los primeros son los delitos contra la confidencialidad, la integridad y la disponibilidad de los datos o sistemas informáticos, como el acceso ilegal a datos o sistemas informáticos (a veces denominados delitos cibernéticos “principales”). Algunos ejemplos de los segundos son el uso de datos o sistemas informáticos para estafar, robar o causar daño a otras personas, así como los delitos relacionados con contenidos informáticos o de Internet, como los discursos de incitación al odio, la pornografía infantil, los delitos relacionados con la identidad y laventa por Internet de mercancías ilícitas. (ONU, 2015, p.7).

Por otra parte, temas como la pornografía infantil causan controversia. La pornografía virtualinfantil crea contenidos sexuales con imágenes no reales, como dibujos y animaciones de menores. Fomenta el consumo de otros materiales que sí lo hacen y provoca problemas al perseguir la pornografía infantil, legal y judicialmente.

Según elinforme sobre pornografía infantil en internet de ANESVAD,en el mundo existen más de 4 millones de sitios de internet que contienen material de sexo con menores y que cada día se crean 500 nuevos(Tellez, 2008). El mismo informe señala que la mayor base de datos de pornografía infantilcuenta con 3 millones de fotografías diferentes,a esto se suman los videos, relatos y otros modos de pornografía infantil. (Tellez, 2008).

Diferencia entre delitos informáticos y delitos computacionales

En el delito informático se emplea para su comisión un sistema automático de procesamiento de datos o de transmisión de datos; en cambio, delito computacional es toda conducta llevada a cabo mediante el uso de tecnología de la información que daña bienes jurídicos ya contemplados en el ordenamiento jurídico penal (Acurio Del Pino, 2016). Si bien existe una pequeña diferencia, ambos van en conjunto ya que persiguen un mismo fin, la diferencia radica en el modo de llegar a éste, un delito informático puede estar dentro de un delito computacional.

Tratados internacionalesque contemplan la seguridad informática

El tema de "delitos informáticos" es reciente, por ello varios juristas expresaron su preocupación ante el vacío legal existentes en la legislación de varios países, por ello se creó el Convenio de Budapest (Consejo de Europa, 2001) que trata la ciber delincuencia, exigiendo a países latinoamericanos a formar parte de este convenio y adecuar sus legislaciones para que puedan estar actualizados ante estas nuevas amenazas, en su preámbulo indica:

> Conscientes de los profundos cambios provocados por la digitalización, la convergencia y la globalización continuas de las redes informáticas; Preocupados por el riesgo de que las redes informáticas y la información electrónicas sean utilizadas igualmente para cometer delitos y de que las pruebas relativas a dichos delitos sean almacenadas y transmitidas por medio de dichas redes; Reconociendo la necesidad de cooperación entre los Estados y el sector privado en la lucha contra la ciberdelincuencia, así como la necesidad

> de proteger los intereses legítimos en la utilización y el desarrollo de las tecnologías de la información;Estimando que la lucha efectiva contra la ciberdelincuencia requiere una cooperación internacional reforzada, rápida y eficaz en materia penal (Consejo de Europa, Convenio sobre la Ciberdelincuencia, 2001, preámbulo).

Bolivia no firmó este convenio, sin embargo, hay países que han comprendido en sus leyes delitos informáticos y se dedicaron a actualizar sus normas.

Por otra parte, la Convención Americana Sobre Derechos Humanos San José de Costa Rica (CASDH, 1969), en su artículo 13 trata libertad de pensamiento y de expresión, por cualquier medio y la limita para evitar el libertinaje, puesto que si bien reconoce la libertad de buscar, difundir y recibir información de toda índole y sin reconocer fronteras, también pone un límite explicando que dicha información no puede dañar la reputación de otras personas, dañar sus derechos, así como el orden público y la moral.

El acuerdo para la represión de la circulación de publicaciones obscenas (1910), en su protocolo modificatorio (1949) expone:

> Los Estados partes en el presente protocolo, considerando que en virtud del Acuerdo para la Represión de la Circulación de Publicaciones Obscenas, firmado en París el 4 de mayo de 1910, el Gobierno de la República Francesa estaba investido de ciertas funciones; considerando que dicho gobierno ha ofrecido espontáneamente traspasar a las Naciones Unidas las funciones que ejerce en virtud de dicho acuerdo; y considerando que es conveniente que en adelante sean éstas asumidas por las Naciones Unidas.

Es aquí donde en tres artículos se hace una explicacion sobre como los países firmantes deben actuar para la prevencion de publicaciones obscenas, el nombrar una autoridad para centralizar la información que pudiera facilitar la averiguacion de material ya sea escritos, dibujos, imágenes u objetos para su respectivo decomiso, y realizar informes sobre los mismos.

Derecho comparado

Son 51 países los que ya firmaron el convenio de Budapest (Consejo de Europa, 2001), y adecuaron su legislación para brindar seguridad informática desde la perspectiva del derecho. Esta lista incluyea Argentina, Chile, República Dominicana, Costa Rica, Panamá y Paraguay. Trata delitos informáticos tales como:

Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos: Interceptación ilícita; Ataque a la integridad de los datos; ataques a la integridad del sistema; Abuso de los dispositivos Delitos informáticos; falsificación informática; fraude informático; delitos relacionados con el contenido; delitos relacionados con la pornografía infantil; delitos relacionados con infracciones de la propiedad intelectual y los derechos afines; tentativa y complicidad; responsabilidad de las personas jurídicas y; sanciones y medidas.

A continuación, se analiza el tratamiento de los derechos informáticos en el derecho comparado.

Argentina

En Argentina, la Ley de Delitos Informáticos 26.388 (2008), modifica, sustituye e incorpora figuras típicas a artículos, con el objeto de regular las nuevas tecnologías como medios de comisión de delitos previstos, fue promulgada de hecho el 24 de junio del 2008 para modificar e incorporar nuevas figuras en su código penal comprende: Distribución y tenencia con fines de distribución de pornografía infantil; Violación de correos electrónicos; Acceso ilegítimo a sistemas informáticos; Daño informático y distribución

de códigos maliciosos; Interrupción de comunicaciones o DoS (sistema operativo de discos) (Arocena, 2012).

Posteriormente se puso en vigencia la Ley de Grooming 26.904 (2013), que incorpora un artículo bajo el título que corresponde a los "Delitos contra la integridad sexual" que dice:

ARTICULO 1º — Incorpórase como artículo 131 del Código Penal el siguiente:

> 'Artículo 131: Será penado con prisión de seis (6) meses a cuatro (4) años el que, por medio de comunicaciones electrónicas, telecomunicaciones o cualquier otra tecnología de transmisión de datos, contactare a una persona menor de edad, con el propósito de cometer cualquier delito contra la integridad sexual de la misma (Ley de grooming 26.904, 2013, p. 1).

Siendo que Argentina incluso es uno de los países que se adhieren al Convenio de Budapest desde el 22 de noviembre del 2017.

Colombia

En Colombia se promulgó la Ley 1273 de 2009, para añadir al código penal un nuevo título sobre "la protección de la información y de los datos" que contiene dos capítulos, que son: de los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos y; de los atentados informáticos y otras infracciones.

Esta ley comprende delitos tales como el hurto por medios informáticos y semejantes, transferencia no consentida de activos, acceso abusivo a un sistema informático, interceptación de datos informáticos, daño informático violación de datos personales, entre otros. Tipifica de igual forma la suplantación de sitios web para capturar datos personales, lo que se conoce como "phishing" que

es un estafador que se hace pasar por una empresa de confianza a través de técnicas de ingenería social mediante una comunicación oficial o un correo electrónico, para luego sustraer información de datos personales, información financiera, credenciales de acceso, para lograr esto utiliza diferentes medios de prop.ación tales como: correos electrónicos, redes sociales, mensajes, llamadas telefónicas e infección por medio de un malware.

Chile

Chile en 1993 ya había promulgado la Ley 19223 (1993) que sanciona los delitos informáticos, luego en 2001 firmó el tratado de Budapest ya que se consideró esencial para la actualización normativa del país, ante los nuevos riesgos que fueron surgiendo a través de los años.

Marco legal boliviano

En el Código Penal Boliviano (1997) en el Título XII Delitos Contra la Propiedad, en el Capítulo XI Delitos Informáticos, se encuentran tipificados dos delitos informáticos, que se exponen a continuación.

363 bis (Manipulación informática) El que con la intención de obtener un beneficio indebido para sí o un tercero, manipule un procesamiento o transferencia de datos informáticos que conduzca a un resultado incorrecto o evite un proceso tal cuyo resultado habría sido correcto, ocasionando de esta manera una transferencia patrimonial en perjuicio de tercero, será sancionado con reclusión de uno a cinco años y con multa de sesenta a doscientos días.

363 ter (Alteración, Acceso y Uso Indebido de Datos Informáticos) El que sin estar autorizado se apodere, acceda, utilice, modifique, suprima o inutilice, datos almacenados en una computadora o en cualquier soporte informático, será sancionado con prestación de trabajo hasta un año o multa hasta doscientos días (ley 10426 Código Penal).

Posteriormente se fueron añadiendo otros, sin embargo, éstos se refieren únicamente al tema financiero. En la Ley 393 de servicios financieros de 21 de agosto del 2013 en el art 491se incorpora lo siguiente:

363 quater (Delitos Financieros) Comete delito financiero la persona natural o jurídica a través de su representante legal, que por acción u omisión incurra en alguna de las tipificaciones delictivas detalladas a continuación […]

- c) Apropiación Indebida de Fondos Financieros. El que sin autorización y mediante la utilización de medios tecnológicos u otras maniobras fraudulentas, se apoderare o procurare la transferencia de fondos, ya sea para beneficio suyo o de terceros incurrirá en privación de libertad de cinco(5)a diez (10) años y multa de cien (100) a quinientos (500) días.Cuando el ilícito sea cometido por un empleado de la entidad financiera aprovechando de su posición o del error ajeno, la pena se agravará en una mitad. […] (Ley 393 de Servicios Financieros).

El Código Niño, Niña y Adolescente (2014) tiene contemplado en su artículo 151 los tipos de violencia en el sistema educativo en su parágrafo primero en su inciso G:

A efectos del presente Código, se consideran formas de violencia en Sistema Educativo:

- Violencia Cibernética en el Sistema Educativo. Se presenta cuando una o un miembro de la comunidad educativa es hostigada u hostigado, amenazada o amenazado, acosada o acosado, difamada o difamado, humillada o humillado, de forma dolosa por otra u otras personas, causando angustia emocional y preocupación, a través de correos electrónicos, videojuegos conectados al internet, redes sociales, blogs, mensajería instantánea y mensajes de texto a través de internet, teléfono móvil o cualquier otra tecnología de información y comunicación.
- II. Los tipos de violencia descritos en el presente Artículo, serán considerados infracciones mientras no constituyan delitos

(Ley 548 Código niño, niña adolescente, 2014, art 151).

Se constata que la norma dice que, ya que los tipos de violencia no constituyen en delito se los considerará como infracciones, de esa manera ante el vacío legal existente en el Código Penal se están tomando como infracciones conductas que deben ser tipificadas ya que pueden derivar en otros delitos de gravedad.Con base en encuestas realizadas a la población, se listan los principales actos desleales informáticos que no se consideran actualmente como delitos y que causan daño en la sociedad, que son: (1) Contenido no apropiado a redes sociales y páginas de internet, relacionado con la pornografía, contenido violento o que incite a la violencia; (2) Desvío de fondos, cuando un funcionario de una empresa legítima hace un traspaso de fondos a una empresa ilegítima; (3) Creación de contenidos y retos que inciten al daño físico o al suicidio, sucede que para ganar popularidad los "influencers" crean retos de este tipo; (4) Hackeo de cuentas personales; (5) Emplear redes sociales y/o páginas de internet para fines de trata y tráfico de personas; (6) Utilización de redes sociales y/o páginas de internet para realizar compra y ventas de productos ilícitos y; (7) Suplantación de identidad.

Asimismo, se detectó necesidad de educar a la sociedad sobre los riesgos en redes sociales para que, por ejemplo, los jóvenes no hagan caso a retos que ponen en peligro su seguridad física y su vida.

Por otra parte, si bien Bolivia aún no recibe amenazas de terrorismo cibernético,es necesario considerar su incorporación en el Código Penal. Las empresas privadas se están digitalizando, las empresas estatales también. Por ejemplo, se está trabajando en una infraestructura informática para el manejos de los servicios básicos, y existe el riesgo hakeode esta infraestructura, en este caso se podría dejar sin agua o sin luz a una ciudad entera o incluso a todo el país, afectando hospitales, clínicas, laboratorios, estaciones de policía y bomberos.

DISCUSIÓN

"Dada la alta tecnología de la informática y su constante […] progreso, tanto las legislaciones de orden penal como los medios de investigación […] resultan insuficientes" (Correo del Sur, 2015). De lo anterior se destacan carencias que impiden la ejecución del proceso penal. Tanto la legislación penal como los medios de investigación se encuentran desactualizados por lo que la sociedad al intentar denunciar estos hechos, no se logra llevar adelante el proceso por el vacío existente.

"En condiciones ideales: los autores serán identificados y llevados a juicio; los tribunales dispondrán sanciones adecuadas; los potenciales autores de ataques contra los sistemas de información recién un mensaje. Sin embargo, los vacíos jurídicos pueden impedir cooperación policial y judicial" (Tellez, 2008).

"A futuro, la aproximación de las legislaciones a nivel internaciones mejorará, pues esta cooperación garantiza que se cumpla la exigencia de doble incriminación, permitiendo la colaboración internacional a nivel judicial en el marco de una investigación penal en la que se haya constituido un delito en dos o más países" (Tellez, 2008). Entonces, se requiere cooperación internacional, ya que estos delitos pueden cometerse desde cualquier ordenador en el mundo, sin embargo, al no tener delitos tipificados en el Código Penal, se están limitando los medios para hacer justicia.

Respecto a los delitos de pornografía infantil: la Sentencia Constitucional Plurinacional 0819/2015-S3 de 10 de agosto del 2015 trata del caso de la divulgación de un video íntimo que se tomó sin el conocimiento de la víctima teniendo relaciones sexuales luego de una serie de amenazas, siendo la víctima extorsionada, se procedió a la acción de protección a la privacidad pidiendo que se eliminara el video de las redes sociales y de la página en la que había sido publicado, en una parte de los fundamentos jurídicos del fallo dice "el Estado no cuenta con normas adecuadas para la protección de datos de carácter personal ni con políticas públicas claras en la materia, pese a que la era digital actual

así lo demanda, donde el acceso a la información fue el puntal de su propia evolución"(Sentencia Constitucional Plurinacional 0819/2015-S3, 2015, fundamentos jurídicos del fallo, párrafo 10). Si bien en éste caso se procedió a la acción de protección a la privacidad, es evidente el vacío legal existente en el actual Código Penal.

CONCLUSIONES

Se identificó la necesidad de educar a los ciudadanos respecto a: los delitos informáticos tipificados en el Código Penal boliviano (1997) y la acción de protección a la privacidad; esto permitirá quela población pueda hacer uso de estas normas para defender sus derechos. Sin embargo, se identificó también que si bien el Código Penal hace alusión a los delitos informáticos (artículo 363 bis y 363 ter), su abordaje ni es exhaustivo ni suficiente para brindar seguridad jurídica, ya que la realidad ha cambiado y ahora existen nuevos riesgos informáticos. Por tanto, existe un vacío legal que genera inseguridad. Se evidencia la necesidad de modificar esta Ley para incorporar el tratamiento de nuevos delitos.

Se evidenció que los países vecinos han actualizado sus normas penales para responder a la realidad social que enfrentan, incorporando leyes modificatorias. Si bien hay mucho por avanzar en el tema, países como Chile y Argentina ya han tipificado delitos informáticos significativos.

Asimismo, se identificó la necesidad de contar con cooperación internacional para la prevención, identificación y penalización de delitos informáticos. Se dan casos en los que las personas que sufren acoso mediante redes no pueden seguir un proceso porque el hecho fue cometido por un sujeto que se encuentra en otro país. En estos casos no procede realizar una investigación ya que Bolivia no tiene tratados o convenios internacionales que se relacionen con el tema.

La propuesta va dirigida en el sentido que las personas se sientan más seguras al momento de usar el internet, tomando conocimiento de que, si ocurriera algo que atente contra su

seguridad física y psicológica, puedan realizar una denuncia con la seguridad de que sus derechos se encuentran protegidos específicamente en la norma establecida, y que las autoridades tengan la base necesaria para hacer justicia.

REFERENCIAS

Acuerdo para la Represión de la Circulación de Publicaciones Obscenas (1910). París. Acuerdo para la Represión de la Circulación de Publicaciones Obscenas y su Protocolo de 1949. Obtenido de https://www.dipublico.org/10685/acuerdo-para-la-represion-de-la-circulacion-de-publicaciones-obscenas-paris-4-de-mayo-de-1910/

Acurio Del Pino, S. (2016). Delitos informáticos: generalidades. Recuperado de http://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf

Arocena, G. A. (2012). La regulación de los delitos informáticos en el Código Penal argentino: Introducción a la Ley Nacional núm. 26.388. Boletín mexicano de derecho comparado, 45(135), 945-988

CASDH (7 al 22 de noviembre de 1969). Convención Americana sobre derechos humanos suscrita en la Conferencia Especializada Interamericana sobre Derechos Humanos. B-32. San José, Costa Rica

Código penal boliviano (1997). Ley No 1768 del 10 de marzo de 1997. Actualizado 2014. Bolivia

Consejo de Europa (2001). Convenio sobre la ciberdelincuencia [Convenio de Budapest]. Consejo de Recuperado de: http://www.oas.org/juridico/english/cyb_pry_convenio. pdf.

Convenio para la Represión de la Circulación y el Tráfico de Publicaciones Obscenas (1923). Ginebra. Convenio para la Represión de la Circulación y el Tráfico de Publicaciones Obscenas y su Protocolo de 1947.

Correo del sur. (30 de junio de 2015). Obtenido de https://correodelsur.com/opinion/20150630_delitos-informaticos.html

Galán, A. (s.f.). iuris now. Obtenido de https://iurisnow.com/es/delitos-informaticos/ gandini, i., Isaza, a., & delgado, a. (s.f.). DELTA asesores. Obtenido de https://www.deltaasesores.com/ley-de-delitos-informaticos-en-colombia/

García-Piña, C. A. (2008). Riesgos del uso de

internet por niños y adolescentes. Estrategias de seguridad. Acta pediátrica de México, 29(5), 272-278

Gómez T., N. (diciembre 2016). Historia de Internet en Bolivia. Bolivia digital, 15 miradas acerca de Internet y sociedad en Bolivia P. 31 – 59. ISBN 978-99974-62-22-0. Vicepresidencia del Estado / Centro de Investigaciones Sociales. La Paz, Bolivia

Ley 19.223 (28 de mayo de 1993). tipifica figuras penales relativas a la informática. Ministerio de Justicia. Santiago de Chile

Ley 548 Código Niño Niña Adolescente. (17 de julio de 2014). Asamblea Legislativa Plurinacional. Estado Plurinacional de Bolivia. Recuperado de: https://siteal.iiep.unesco.org/sites/default/files/sit_accion_files/siteal_bolivia_0248.pdf

Ley N 1273 de 2009. Colombia. Extraído de: https://www.sic.gov.co/recursos_user/documentos/normatividad/Ley_1273_2009.pdf

LeyN° 26904 (2013). Se incorpora la figura de 'Grooming' o 'Ciberacoso' sexual al art. 131 del Código Penal Tipo: LEY Número: 26904 Emisor: Poder Legislativo Nacional Fecha B.O.: 11-dic-2013 Localización: Nacional Cita: LEG59568. Buenos Aires, Argentina.

Ley No 393 de Servicios Financieros (21 de agosto de 2013). Bolivia

Loredo G., J. A., & Ramírez G., A. (2013). Delitos informáticos: su clasificación y una visión general de las medidas de acción para combatirlo. Celerinet, 44-51.

Ojeda-Pérez, J. E., Rincón-Rodríguez, F., Arias-Flórez, M. E., & Daza-Martínez, L. A. (2010). Delitos informáticos y entorno jurídico vigente en Colombia. Cuadernos de Contabilidad, 11(28), 41-66.

ONU (abril de 2015). 13° congreso de las nociones unidas sobre prevención del delito y justicia penal. Obtenido de https://www.unodc.org/documents/congress/Documentation/A-CONF.222-12_Workshop3/ACONF222_12_s_V1500666.pdf

Sentencia Constitucional Plurinacional 0819/2015-S3 (10 de agosto de 2015). Tribunal Constitucional Plurinacional de Bolivia, SALA TERCERA. Magistrado Relator Dr. Ruddy José Flores Monterrey, Acción de protección de privacidad. Expediente: 06499-2014-13-APP del departamento de La Paz. Sucre, Bolivia

Tellez, J. (2008). Derecho Informático. En J. Tellez, Derecho Informático (p.. 206). Mc Graw Hill Educación