Artículo de reflexión

LA MODIFICACIÓN DEL CÓDIGO PENAL BOLIVIANO EN LA INCORPORACIÓN DE NUEVOS DELITOS INFORMÁTICOS

AMENDMENT OF THE BOLIVIAN PENAL CODE TO INCLUDE NEW CYBERCRIME OFFENSES

VERENA CONSTANTINA AREQUIPA REJAS
https://orcid.org/0009-0006-4846-4455
arequipa1239@gmail.com

RESUMEN:

El dinámico avance tecnológico ha reconfigurado profundamente la dinámica social, remodelando la forma en que las personas interactúan y se relacionan en la era moderna. La relación entre personas y las Tecnologías de la Información y Comunicación (TIC) se ha vuelto cada vez más profunda e influyente en la sociedad contemporánea. Las TIC, que influyen dispositivos como computadoras, teléfonos, internet y redes sociales, han transformado la forma en que vivimos, trabajamos y nos relacionamos. Por un lado, estas nuevas tecnologías han ampliado el acceso a la información y han facilitado la comunicación instantánea y global entre personas de todo el mundo.
Sin embargo, este progreso vertiginoso ha venido acompañado de desafíos legales sin precedentes, como la proliferación de delitos informáticos, que plantean interrogantes fundamentales. Frente a esta compleja convergencia entre derecho, tecnología y sociedad, es imperativo que los sistemas legales se adapten y evolucionen para abordar de manera efectiva estos retos emergentes. Esto implica la creación de leyes y regularizaciones actualizadas dirigidas a los ciberdelitos. Al establecer un marco legal claro y robusto, se fomenta un entorno en línea más seguro y se disuade a los posibles de cometer delitos informáticos.

Palabras clave: Delitos Informáticos, Tecnologías de la Información y Comunicación (TIC), Dinámica Social, Desafíos Legales, Derecho, Tecnología y Sociedad, Progreso Tecnológico, Actualización.

ABSTRACT:

The dynamic technological advancement has profoundly reconfigured social dynamics, reshaping how people interact and relate in the modern era. The relationship between individuals and Information and Communication Technologies (ICT) has become increasingly deep and influential in contemporary society. ICT, which encompasses devices such as computers, phones, internet, and social media, has transformed the way we live, work, and relate. On one hand, these new technologies have expanded access to information and facilitated instant and global communication among people worldwide.
However, this rapid progress has been accompanied by unprecedented legal challenges, such as the proliferation of cybercrimes, which pose fundamental questions. Faced with this complex convergence of law, technology, and society, it is imperative that legal systems adapt and evolve to effectively address these emerging challenges. This implies the creation of updated laws and regulations aimed at cybercrimes. By establishing a clear and robust legal framework, a safer online environment is promoted and potential offenders are discouraged from committing cybercrimes.

Keywords: Computer Crimes, Information and Communication Technologies (ICT), Social Dynamics, Legal Challenges, Law, Technology, and Society, Technological Progress, Update.

Copyright: © 2024 by the authors. Submitted for open access publication under the terms and conditions of the Creative Commons Attribution (CC BY) license

Revisado: 10/09/2024. **Aceptado:** 17/10/2024.
Citado: Arequipa Rejas, V. C. LA MODIFICACIÓN DEL CÓDIGO PENAL BOLIVIANO EN LA INCORPORACIÓN DE NUEVOS DELITOS INFORMÁTICOS. *Juris Studia,* 1(2), 83–100
https://doi.org/10.52428/12345678.v1i1.1087

1. INTRODUCCIÓN

En el tejido social, el ser humano destacaba por su capacidad cognitiva, creativa y social. Sin embargo, la llegada de las Nuevas Tecnologías de la Información y comunicación (NTIC) se desató una revolución. Este cambio redefinió las interacciones humanas y, a su vez, introdujo nuevos desafíos, como la ciberdelincuencia. En este análisis se exploró como estas transformaciones afectaron la experiencia humana y los paradigmas sociales.

Partiendo de la siguiente interrogante: ¿Es necesario modificar la norma sustantiva penal boliviana aplicando los nuevos tipos penales de los delitos informáticos?

Cuyo objeto fue:

Proponer la incorporación de nuevos tipos penales que regulen los delitos informáticos en el Código Penal boliviano.

2. MÉTODO

Los métodos que se utilizaron en el desarrollo del presente trabajo son diversos y abarcan diferentes enfoques para abordar la complejidad del tema. A continuación, se detallan estos métodos:

- ***Método Descriptivo :*** Consiste en especificar las propiedades y características de grupos, personas u objetos, así como de fenómeno sometidos a análisis. En este caso se analizará como la sociedad se desenvuelve en el espacio del Internet mediante el uso de las Nuevas Tecnologías de la Información y Comunicación, así como la perpetración de delitos informáticos.
- ***Método Cualitativo:*** Tiene por objeto evaluar la eficacia del orden normativo teórico en relación con problemas sociales concretos. Se explora la efectividad del Código Penal Boliviano en el ámbito de la informática y la tecnología, y su es suficiente para regular y sancionar los delitos cometidos a través de las Tecnologías de la Información y Comunicación.
- ***Método Detallado:*** Se utilizará para observar la conducta de la sociedad ante el uso o el abuso de las Nuevas Tecnologías de Información y Comunicación, que conducen a actividades ilícitas no sancionadas debido a la falta de conocimiento sobre la identificación de los tipos penales en la legislación de Bolivia.
- ***Método Inductivo:*** Propone partir de un postulado específico para llegar a una norma general y tomar una decisión. Este enfoque puede ser útil para extraer conclusiones generales a partir de observaciones específicas sobre el teme de los delitos cibernéticos y su regulación.
- ***Método Jurídico Propositivo:*** Se caracteriza por evaluar las deficiencias de los sistemas o normas existentes con el fin de proponer o aportar posibles soluciones. Este método puede ser útil para identificar lagunas en la legislación actual y proponer enmiendas o nuevas regulaciones para abordar los desafíos emergentes en el ámbito de la cibercriminalidad.

Revista JURIS STUDIA Diciembre de 2024
ISSN Digital: 2075-8944 ISSN Impreso: 2075-8936 / DOI 10246451213131212
Copyright: © 2024 by the authors. Submitted for open access publication under the terms and conditions of the Creative Commons Attribution (CC BY) license

3. DESARROLLO

A lo largo de la historia, la humanidad ha experimentado diversas etapas de desarrollo tecnológico que han culminado en el nivel actual de innovación. El impacto de las revoluciones industriales ha traído consigo grandes transformaciones a nivel social y mundial. Desde la invención de la rueda hasta el surgimiento de las computadoras, y en particular, la herramienta tecnológica del internet, han marcado hitos importantes en este viaje evolutivo.

3.1 HISTORIA DEL INTERNET

El internet surge a raíz de la confrontación entre Estados Unidos y la Unión Soviética durante la Guerra Fría, un conflicto que se extendió desde 1947 hasta 1991. En este contexto de rivalidad tecnológica y militar, Estados unidos creo en 1958 la Agencia de Proyectos de Investigaciones Avanzadas (ARPA, por sus siglas en ingles).

ARPA comenzó a desarrollar una teoría revolucionaria: dividir la información en pequeños bloques que pudieran ser transmitidos independientemente a través de una red de computadoras en su destino final.

En 1969, ARPA lanzo ARPANET, la primera red de computadoras basadas en esta tecnología. ARPANET permitió la conexión entre instituciones académicas y de investigación, facilitando la colaboración y el intercambio de información de manera sin precedentes. Inicialmente, ARPANET tenía un propósito militar, buscando asegurar las comunicaciones en caso de un ataque, pero su éxito pronto atrajo el interés de comunidad científica y académica.

Con el tiempo, ARPANET dejó de ser de interés exclusivamente militar y fue desmantelada 1990. Sin embargo, su legado continuo, y la tecnología y los principios desarrollados durante su existencia sentaron las bases para el surgimiento del internet tal como lo conocemos hoy.

3.2 INTERNET

Considerada como una red global de computadoras interconectadas que permite la transmisión y el intercambio de información a través de diversos protocolos de comunicación. Funciona como una infraestructura descentralizada, que utiliza la conmutación de paquetes para enviar datos de manera eficiente entre múltiples dispositivos y redes. A través del internet, los usuarios pueden acceder a una vasta cantidad de recursos y servicios, como páginas web, correo electrónico, redes sociales, transmisión de multimedia, comercio electrónico y muchas otras aplicaciones. Es una herramienta esencial para la comunicación, la educación, el entrenamiento y los negocios en la sociedad contemporánea.

3.3 TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN (TIC)

Las Tecnologías de la Información y la Comunicación (TIC) son un conjunto de herramientas, recursos y sistemas tecnológicos diseñados para gestionar, procesar, almacenar, recuperar y transmitir información de manera eficiente. Estas tecnologías incluyen tanto dispositivos físicos, como computadoras, teléfonos móviles y equipos de redes, como aplicaciones y servicios digitales, tales como software, bases de datos, internet, redes sociales, y plataformas de comunicación y colaboración en línea.

ISSN Digital: 2075-8944 ISSN Impreso: 2075-8936 / DOI 10246451213131212
Copyright: © 2024 by the authors. Submitted for open access publication under the terms and conditions of the Creative Commons Attribution (CC BY) license

Las TIC son fundamentales en la modernización de diversos sectores, incluyendo la educación, la salud, los negocios, el gobierno y el entretenimiento, ya que facilitan la comunicación, la toma de decisiones informadas, la innovación y la eficiencia operativa. Al integrar estas tecnologías, las organizaciones y los individuos pueden acceder a un flujo constante de información, conectarse con otros usuarios y recursos globales, y mejorar la productividad y la calidad de vida.

3.4 CIBERESPACIO

El ciberespacio está de moda, debido a el desarrollo de las tecnologías de la información y comunicación (TICs), ha abierto nuevos potenciales para relaciones entre los Estados y los individuos, así como para el desarrollo económico y social; lamentablemente, las TICs también pueden utilizarse para fines que no son enteramente pacíficos.

El ciberespacio, proviene del término inglés "cyberspace" llego al español como "ciberespacio", así se denomina al entorno artificial que se desarrolla a través de herramientas informáticas, es el ámbito de información que se encuentra implementado dentro de los ordenadores y de las redes digitales de todo el mundo. Es también un tema recurrente en la ciencia ficción. Es visual, inexistente desde el punto de vista físico donde las personas o sujetos, públicas o privadas desarrollan comunicaciones a distancia, exponen sus competencias, generan interactividad para diversos propósitos (Wikipedia, s.f.)

El ciberespacio tiene una variedad de características que lo convierten en un escenario ideal para la comisión de diferentes delitos, resultando en una variedad e complejidades, como lo demuestran los siguientes puntos:

- Diversidad y fragmentación regulatoria en relación con los tipos de delitos
- Identificar al autor y determinar el lugar del crimen.
- Procedimientos técnicos de investigación y ámbito de competencia para perseguir hechos ilícitos.
- Necesidad de recurrir a conocimientos técnicos, especialmente relacionadas con la informática forense.
- Debilidades en los mecanismos de ciberseguridad y preservación de evidencia.

3.5 CIBERCRIMINALIDAD

El rápido avance de la tecnología y su uso cotidiano en la vida del ser humano no está exento de nuevos problemas que la ley debe abordar. Se cree que la cuestión de la cibercriminal es particularmente importante en esta área porque los delitos ocurren más rápido, son más números y más sofisticados. El cibercrimen se entiende como un fenómeno delictivo en el ciberespacio, es decir que el cibercrimen son los delitos que se realizan en el ciberespacio.

La cibercriminalidad trata de un acto que infringe la ley que se comete usando las tecnologías de la información y la comunicación (TIC) para atacar las redes, sistemas, datos, sitios web y la tecnología o para facilitar un delito, la ciberdelincuencia o cibercriminalidad se diferencia de los delitos comunes, pues se pueden cometer con menos esfuerzo y más facilidad y velocidad que los delitos comunes, debido a que estos delitos son dependientes de los medios informáticos, es decir todo delito que solo se puede cometer usando computadoras, redes computarizadas u otras formas tecnologías de la información y comunicación (UNODC, 2020).

Revista JURIS STUDIA Diciembre de 2024
ISSN Digital: 2075-8944 ISSN Impreso: 2075-8936 / DOI 10246451213131212
Copyright: © 2024 by the authors. Submitted for open access publication under the terms and conditions of the Creative Commons Attribution (CC BY) license

3.6 SOCIEDAD DE LA INFORMACIÓN

La sociedad de la información, comienza por la fuerte relación de las personas con aparatos tecnológicos, este término describe una etapa de desarrollo social y económico en la cual la creación, distribución, y manipulación de la información se convierten en las principales actividades económicas, sociales y culturales. En esta sociedad, las tecnologías de la información y la comunicación (TIC) juegan un papel central al facilitar el acceso, procesamiento y transmisión de datos a gran escala.

En la sociedad de la información, el conocimiento y la información son considerados recursos estratégicos, esenciales para la innovación, el crecimiento económico y el bienestar social. Esta transformación afecta diversos aspectos de la vida, incluyendo la educación, el trabajo, la política, la cultura y las relaciones personales.

La sociedad de la información se caracteriza por una mayor conectividad global, el surgimiento de nuevas formas de comunicación y colaboración, y la democratización del acceso a la información. Sin embargo, también plantea desafíos, como la brecha digital, la protección de la privacidad y la gestión de la sobrecarga de información.

¿Quiénes forman parte de la sociedad de la información?

Forman parte todas las personas, consideradas en este ambiente artificial del ciberespacio como los usuarios. Los usuarios son individuos o entidades que interactúan con sistemas, dispositivos o servicios tecnológicos para llevar a cabo diversas tareas y actividades. En el contexto de las tecnologías de la información y la comunicación (TIC), los usuarios pueden desempeñar múltiples roles y pueden variar significativamente en términos de sus necesidades, habilidades y objetivos.

3.7 DELITOS INFORMÁTICOS

Los delitos informáticos son las acciones que contravienen la ley, poseen características típicas y son imputables, llevadas a cabo en el ámbito digital, el espacio cibernético o la red internet. El anonimato y la disponibilidad de información personal en entornos digitales han ampliado considerablemente el alcance de los perpetradores delictivos, lo que ha resultado en un aumento exponencial de los delitos informáticos y las amenazas a la seguridad. Además de estos, existen otras acciones delictivas que, aunque no califican estrictamente como delitos, se clasifican como ciberataques y se integran dentro del espectro de la delincuencia informática. (Wikipedia, 2023)

Otro concepto es que el delito informático es todo acto o conducta ilícita e ilegal que pueda ser considerada como criminal, dirigida a alterar, socavar, destruir, o manipular, cualquier sistema informático o alguna de sus partes competentes, que tenga como finalidad causar una lesión o poner en peligro un bien jurídico cualquiera. (Del Pino, 2016)

¿quiénes comenten estas fechorías?

Delincuentes informáticos, ciberdelincuentes, que puede ser cualquier persona que tenga en su poder un aparato tecnológico con acceso a internet. Es decir que el sujeto activo en el campo de la informática se caracteriza por la utilización de algún soporte tecnológico (celulares, computadoras, Tablet, etc.) o el manejo de las nuevas tecnologías de la información y la comunicación (Internet, redes sociales, etc.).Las personas que comenten los “Delitos Informáticos” son aquellos sujetos activos impropios, es decir

ISSN Digital: 2075-8944 ISSN Impreso: 2075-8936 / DOI 10246451213131212
Copyright: © 2024 by the authors. Submitted for open access publication under the terms and conditions of the Creative Commons Attribution (CC BY) license

que cualquier persona puede llegar a cometer el acto ilícito por medio de la tecnología, a través de toda la información que ofrece la herramienta del internet, la información adquirida muchas veces no se le utiliza de forma positiva, sino también negativa.

De forma positiva es que el usuario adquiera información y amplíe sus conocimientos mediante las diversas plataformas del internet, de forma negativa, es que el usuario con intenciones maliciosas busca y adquiere información para cometer o causar daño a otra persona natural o jurídica por medio de las Tics. Los sujetos activos desarrollan habilidades para el manejo de los sistemas informáticos y generalmente se encuentran en lugares estratégicos donde se manipula información de carácter sensible, o bien son hábiles en el uso de los sistemas informatizados.

3.8 INGENIERÍA SOCIAL

Ingeniería social son las diferentes técnicas de manipulación que usan los ciberdelincuentes para obtener información privada de los usuarios. El primero en usar el término "Ingeniería Social" en el ámbito de la seguridad informática fue el hasta hoy reconocido como el mejor hacker del mundo, Kevin Mitnick, quien señala que la Ingeniería Social se refiere a la aplicación de técnicas, que los hackers utilizan para engañar a un usuario autorizado de sistemas informáticos de una compañía para que revele información o para lograr que de forma insospechada realice acciones que creen un hueco de seguridad que pueda ser explotado (Argentina.gob.ar., 2020).

El propósito del atacante que emplea tácticas de ingeniería social es aprovechar la vulnerabilidad del usuario, considerado el componente más susceptible dentro de la estructura organizacional. La audacia del atacante determina si recurre a herramientas tecnológicas o a interacciones directas para adquirir la información requerida.

Los canales que utilizan los ciberdelincuentes para los ataques de ingeniería social son:

- ✓ llamadas telefónicas
- ✓ aplicaciones de mensajería instantánea
- ✓ correos electrónicos
- ✓ redes sociales

Los métodos que emplean los ciberdelincuentes para cometer sus ataques son:

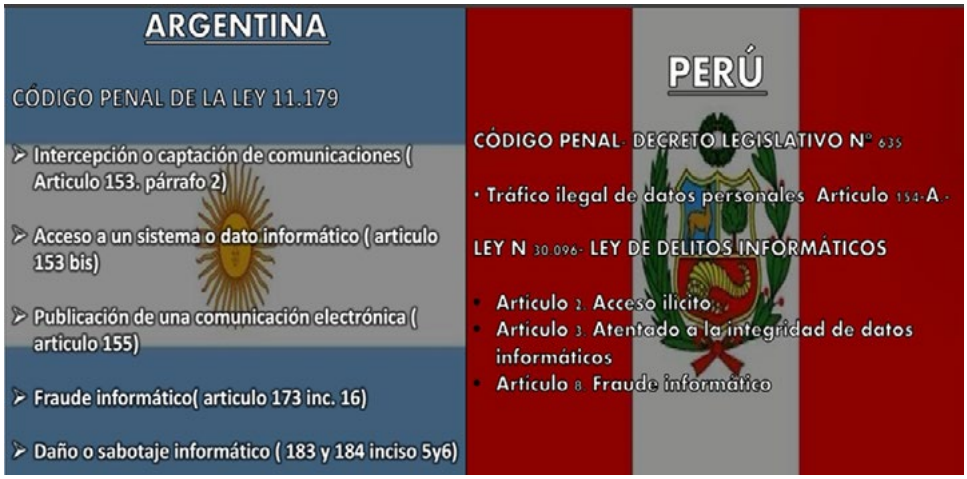
- ✓ Hacerse pasar por algún miembro de la familia, un conocido o un compañero de trabajo.
- ✓ Ofrecer a la víctima premios o promociones únicas y limitadas a cambio de sus datos.
- ✓ Hacerse pasar por el técnico de la empresa o por la persona responsable de sistemas.
- ✓ Invitar a completar formularios para ganar un premio o un producto.
- ✓ Ofrecer actualizaciones de navegadores o aplicaciones a través de páginas falsas (Argentina.gob.ar., 2020).

4. LEGISLACIÓN COMPARADA

Los países como Argentina y Perú han realizado grandes esfuerzos por adaptar sus normas a la realidad tecnológica de su sociedad. Como podemos observar en el presente cuadro, ambos países han tipificado los delitos informáticos en sus códigos penales.

Revista JURIS STUDIA Diciembre de 2024
ISSN Digital: 2075-8944 ISSN Impreso: 2075-8936 / DOI 10246451213131212
Copyright: © 2024 by the authors. Submitted for open access publication under the terms and conditions of the Creative Commons Attribution (CC BY) license

Sin embargo, este trabajo recopiló y seleccionó los artículos relacionados con los tipos penales que se planean incorporar. Lo que destaca de ambas legislaciones es que cuentan con una normativa específica dedicada identificar y sancionar los delitos cometidos por medios digitales. Por ejemplo, Perú cuenta con la Ley 30.096 de Delitos Informáticos.



Fuente: Elaboración propia

4.1 LEGISLACIÓN BOLIVIANA

En el año 2019, se llevó a cabo una Asamblea de las Naciones Unidas titulada “Lucha contra las nuevas tecnologías de la información y la comunicación con fines delictivos”. Esta reunión tenía como objetivo que los países miembros emitieran un informe sobre su relación con estas tecnologías. En el caso de Bolivia, se destacaron cuatro puntos importantes y preocupantes.

El Estado Plurinacional de Bolivia afirmó que, a la par del desarrollo tecnológico informático, los delincuentes encontraban formas innovadoras de cometer fraudes y otros delitos que iban más rápido que los códigos penales. Frente a un fenómeno en alza, se imponía la necesidad de prevención y protección, que era deber de todos: Estados, empresas, organizaciones, ciudadanía. En este sentido, las innovaciones tecnológicas planteaban múltiples desafíos para las instituciones encargadas de mantenerlas:

a) **La falta de conciencia y conocimiento** por parte de la población respecto del uso de las tecnologías de la información y las comunicaciones. Esa carencia hacía que las personas fueran más vulnerables a delitos de diferente índole. Un desafío conexo seria como elaborar políticas adecuadas para mejorar los conocimientos acerca del buen uso de esas tecnologías.
b) **La existencia de un vacío legal** producto del desconocimiento o de la inaplicabilidad de las legislaciones actuales a los nuevos delitos para cuya comisión se utilizaban las tecnologías de la información y las comunicaciones. Era necesario, por lo tanto, revisar y actualizar la legislación.

ISSN Digital: 2075-8944 ISSN Impreso: 2075-8936 / DOI 10246451213131212
Copyright: © 2024 by the authors. Submitted for open access publication under the terms and conditions of the Creative Commons Attribution (CC BY) license

c) **La necesidad de modificar las estrategias de investigación y respuestas tradicionales**, a los delitos mediante la utilización de nuevos métodos, había cuenta de evolución de los delitos en los que se emplean a las tecnologías de la información y las comunicaciones.

d) **La necesidad de ser parte de convenios internacionales** de cooperación sobre investigación, aseguramiento y obtención de pruebas en materia de ciberdelincuencia. Varios países de América Latina formaban parte ya de convenios y habían progresado en el desarrollo de sus capacidades tecnológicas de la información y comunicaciones.

En base a este informe, podemos verificar en la siguiente imagen los delitos informáticos que tiene nuestro país.

Fuente: Elaboración propia

La situación legal en Bolivia respecto a los delitos informáticos muestra una limitación en la tipificación y regulación de estas conductas. Actualmente, solo se cuenta con dos tipos penales específicos: el Artículo 363 Bis y 363Ter. Sin embargo, estos son considerados demasiado tradicionales y no se ajustan adecuadamente a la realidad social y tecnológica del país. Su contenido se percibe como general y poco claro.

Es esencial recordar que una norma debe cumplir con principios fundamentales como la taxatividad, certeza y reserva de ley, los cuales son vitales para proteger los derechos fundamentales y garantizar la seguridad jurídica. Además, el derecho es dinámico y debe adaptarse a los cambios sociales y tecnológicos para satisfacer necesidades y resolver conflictos.

Los avances tecnológicos generan la necesidad de revisar y actualizar la legislación en materia de delitos informáticos. Es fundamental que la normativa sea lo suficiente flexible y precisa para abordar adecuadamente las conductas delictivas en el ámbito digital y garantizar una aplicación efectiva de la justicia. Por lo tanto, se hace imperativo que se realice reformas legales que reflejen de manera adecuada la realidad tecnológica y social del país.

Revista JURIS STUDIA Diciembre de 2024
ISSN Digital: 2075-8944 ISSN Impreso: 2075-8936 / DOI 10246451213131212
Copyright: © 2024 by the authors. Submitted for open access publication under the terms and conditions of the Creative Commons Attribution (CC BY) license

INFORME DEL OBSERVATORIO DE DELITOS INFORMÁTICOS DE BOLIVIA (ODIB)En 2023

Bolivia experimento **3768 casos de delitos cibernéticos**, con los departamentos de La Paz, Santa Cruz, Cochabamba y El Alto los más afectados. Las víctimas se distribuyeron en **55% mujeres, 40% hombres, 5% otros.** El fraude o estafa informático fue el delito principal

La ODIB realizó una encuesta sobre el panorama digital en Bolivia

Preguntas	Totalmente en desacuerdo	En desacuerdo	Desconoce	De acuerdo	Totalmente de acuerdo
1. El Estado boliviano cuenta con leyes específicas que abordan el cibercrimen y protegen a las víctimas	39%	40%	7%	10%	5%
2. Las leyes existentes en Bolivia son lo suficientemente amplias y actualizadas para abarcar una amplia gama de actividades delictivas en el ámbito digital.	38%	41%	5%	11%	5%
3. El Estado boliviano cuenta con agencias gubernamentales dedicadas específicamente a combatir el cibercrimen.	43%	47%	5%	4%	2%
4. Se han asignado suficientes recursos, tanto humanos como financieros, para combatir el cibercrimen en Bolivia.	44%	44%	2%	5%	5%
5. Bolivia tiene la infraestructura tecnológica y las capacidades técnicas necesarias para detectar, investigar y responder eficazmente a los delitos informáticos.	52%	45%	2%	1%	1%

Tabla 1 *Tabla resumen de preguntas y respuestas de la encuesta realizada (selección múltiple)*

Preguntas	SI	NO	Desconoce
6. ¿Cree usted que las campañas de concienciación pública sobre los riesgos del cibercrimen son suficientes en Bolivia?	2%	90%	8%
7. ¿Considera importante incluir la educación en seguridad cibernética en los programas escolares y universitarios en Bolivia?	92%	1%	8%
8. ¿Ha recibido orientación y apoyo adecuados en caso de ser víctima de delitos informáticos en Bolivia?	5&	84%	10%

Tabla 2 *Tabla resumen de preguntas y respuestas de la encuesta realizada (falso o verdadero)*

Fuente: Elaboración propia

Revista JURIS STUDIA Diciembre de 2024
ISSN Digital: 2075-8944 ISSN Impreso: 2075-8936 / DOI 10246451213131212
Copyright: © 2024 by the authors. Submitted for open access publication under the terms and conditions of the Creative Commons Attribution (CC BY) license

CASOS TIPIFICADOS COMO ESTAFA

Se han registrado 192 casos de rechazo cerrado, todos relacionados con delitos tecnológicos. Los legisladores se basan en el **artículo 304** de la normativa penal procesal, el cual permite al fiscal rechazar denuncias cuando el hecho no ocurrió, no es un delito tipificado o el imputado no participo, así como cuando la investigación no proporciona suficientes elementos para fundamentar la acusación.

Fuente: Elaboración propia

En resumen, mediante encuestas y ejemplos de casos, se busca demostrar que Bolivia enfrenta desafíos considerables en la implementación efectiva del derecho informático. Esto evidencia que aún hay un largo camino por recorrer en cuanto a la aplicación de normativas y la protección de las víctimas en el ámbito digital.

6. PROPUESTA

Se hicieron modificaciones necesarias a la Ley 1768 de 10 de marzo de 1997 Código Penal Boliviano, mediante un Proyecto de Ley, con nuevos tipos penales en relación a delitos informáticos.

NUEVOS DELITOS INFORMÁTICOS

Se seleccionaron e identificaron los siguientes delitos informáticos porque son aquellos que impactan significativamente a nuestra sociedad, considerando los métodos y medios utilizados para realizarlos en el ámbito digital. Estos delitos son relevantes por su creciente incidencia y complejidad en un mundo cada vez más interconectado y dependiente de la tecnología. La selección de estos delitos se basa en su capacidad para causar daño económico, violaciones a la privacidad, perjuicio a la seguridad informática y otros efectos nocivos en individuos y organizaciones.

a) **PHISHING**

- **Origen**
  Esta palabra proviene del término fishing que significa pescar. Se identifica con esta palabra porque la intención de esta estafa es “pescar” a usuarios de internet para que releven información susceptible. (Leyes, 2022).

Revista JURIS STUDIA Diciembre de 2024
ISSN Digital: 2075-8944 ISSN Impreso: 2075-8936 / DOI 10246451213131212
Copyright: © 2024 by the authors. Submitted for open access publication under the terms and conditions of the Creative Commons Attribution (CC BY) license

- **Definición**
  Se puede definir al phishing como la suplantación de identidad, proceso por el cual una persona es contactada por email con un mensaje que invita a la persona a ingresar, mediante un enlace (link) a una página o sitio web muy convincente por alguien que simula ser una institución legítima para obtener datos privados, tales como datos bancarios, contraseñas, datos personales etc. Luego esta información obtenida de forma fraudulenta es utilizada para acceder a las cuentas personales de las víctimas y causar pérdidas económicas o suplantación de identidad (Leyes, 2022).

- **Objetivo**
  El phishing intenta captar diferentes tipos de información, entre ellas, destacamos la información personal (dirección de correo, número de documento de identidad, datos de contacto, etc.), la información financiera (número de tarjetas de crédito, números de cuentas, información sobre el banco, etc.) y datos sobre credenciales de acceso (redes sociales, cuentas de correo, etc.) (Leyes, 2022).

b) **VISHING**

- **Origen**
  Esta palabra nace de la unión de voice y phishing, es decir, engloba a aquellos ataques de phishing que involucran una voz, ya sea robótica o humana. En estas, los atacantes pueden llegar a la víctima mediante llamadas telefónicas masivas (Ciudadanía, 2021).

- **Definición**
  Es un tipo de fraude basado en la ingeniería social y en la suplantación de identidad. Se efectúa mediante llamadas telefónicas, donde el atacante suplanta la identidad de una empresa, organización o incluso de una persona de confianza, con el objetivo de obtener información personal de sus víctimas (Ciudadanía, 2021).

- **Objetivo**
  El phishing y el vishing persiguen el mismo objetivo, el de obtener información delicada de usuarios que podría emplearse para robo de identidad, obtener beneficios financieros o apoderarse de cuentas (Ciudadanía, 2021).

c) **SMISHIG**

- **Origen**
  El smishing proviene de la combinación de las palabras SMS (mensajes) y Pishing, mensajes que son enviados desde cualquier red social (WhatsApp, Facebook, Instagram, etc.) (Castillo, 2023).

- **Definición**
  El smishing es un ataque estrechamente relacionado que también usa números de teléfonos móviles, no obstante, en lugar de un correo de voz, el smishing emplea mensajes de texto para engañar a los usuarios. El smishing se basa principalmente en que los usuarios confíen en mensajes de texto. Estos

Copyright: © 2024 by the authors. Submitted for open access publication under the terms and conditions of the Creative Commons Attribution (CC BY) license

mensajes suelen prometer premios en metálico, cupones o amenazar con cancelar cuentas si el usuario no autentica y restablece sus credenciales. (Castillo, 2023).

- **Objetivo**
  Al igual que el phishing el smishing tiene como objetivo de robar información privada, realizar una estafa o incluso recibir algún monto económico. Obtener información personal, como por ejemplo claves o datos bancarios. También se envían mensajes para vender productos que no existen o avisos de premios que se ha ganado en un sorteo (Castillo, 2023).

d) **DOXING**

- **Origen**
  El doxing es el termino procedente de la abreviación de documentos en inglés (dox) Es la traducción de "exponer dox" (una forma coloquial de referirse a documentos), en referencia a la recopilación de documentos o de información personal y su posterior publicación en línea para generar un daño (Castillo, 2023).

- **Definición**
  Doxing, es el acto de revelar intencional y públicamente información, es una forma de acoso que consiste en revelar en internet datos o documentos personales o, indirectamente, la identidad completa de una persona, sin su consentimiento (Castillo, 2023).

- **Objetivo**
  El objetivo es causar angustia, pánico o alarma a través de la información publicada como ser: números de teléfono de la persona a la que se dirige el ataque, dirección física o del lugar de trabajo, direcciones de correo electrónico u otra información de contacto, números de la seguridad social, datos de tarjetas de crédito, información de cuentas bancarias, cuentas de redes sociales, fotos personales. Tweets, publicaciones y estados. Información que contenga datos de salud, datos laborales. Antecedentes penales. Historiales de búsquedas en línea, Información sobre gustos y prioridades. Adolescentes, instituciones, jóvenes y personas adultas pueden ser víctimas de este accionar.

6. IDENTIFICACIÓN DEL NOMEN IURIS DE LOS NUEVOS DELITOS INFORMÁTICOS

Nomen Iuris es una expresión latina que se traduce como "nombre del derecho". En el contexto jurídico, se refiere a la denominación o término legal utilizado para identificar una institución jurídica, una figura legal, un concepto legal o cualquier elemento del sistema legal.

Revista JURIS STUDIA Diciembre de 2024
ISSN Digital: 2075-8944 ISSN Impreso: 2075-8936 / DOI 10246451213131212
Copyright: © 2024 by the authors. Submitted for open access publication under the terms and conditions of the Creative Commons Attribution (CC BY) license

Los delitos informáticos que se planeó incorporar a nuestra norma sustantiva penal, provienen de palabras en inglés, para que puedan ser añadidos a nuestra legislación se necesita su traducción o una denominación jurídica en idioma español, siempre y cuando no se cambie la esencia conceptual, debido a que la Constitución Política del Estado Plurinacional de Bolivia señala en su **artículo 5** lo siguiente: "Son idiomas oficiales de Estado el castellano y todos los idiomas de las naciones y pueblos indígena originario campesino". Por tanto, se identifica a los nuevos delitos informáticos con los siguientes términos basados en su significado:

INGLÉS	CASTELLANO
Pishing	Suplantación de Identidad Digital
Vishing	Engaño por Voz Virtual
Smishing	Manipulación por Red Social
Doxing	Exposición de Documentos Electrónicos

6.2 DESCOMPOSICIÓN DEL TIPO PENAL DE LOS NUEVOS DELITOS INFORMÁTICOS

Esta investigación, realizó la descomposición del tipo penal en referencia a los nuevos tipos penales de delitos informáticos:

SUPLANTACIÓN DE IDENTIDAD DIGITAL

Quien, utilizando medios tecnológicos, se haga pasar por una persona natural o jurídica e invite a otro a ingresar sus datos personales a un enlace, con la intención de obtener un beneficio indebido para sí o un tercero, será sancionado con privación de libertad de tres (3) a seis (6) años y con una multa de sesenta (60) a doscientos (200) días

Descomposición:

- **Sujeto Activo:** El sujeto activo es impropio, este delito puede ser cometido por cualquier persona imputable.
- **Sujeto Pasivo:** El sujeto pasivo es impropio este delito afecta a cualquier persona.
- **Verbo Rector:** Suplantar
- **Bien Jurídico:** Delitos contra la propiedad
- **Condición Sine Qua non:** Obtener un beneficio indebido
- **Elemento Subjetivo:** Doloso
- **Pena o Sanción:** privación de libertad de tres (3) a seis (6) años y con multa de sesenta (60) a doscientos (200) días.

ENGAÑO POR VOZ VIRTUAL

Quien, mediante medios tecnológicos, llama telefónicamente para adquirir datos personales con la intención de obtener un beneficio indebido para sí o para un tercero, será sancionado con privación de libertad de tres (3) a seis (6) años y multa de sesenta (60) a doscientos (200) días.

ISSN Digital: 2075-8944 ISSN Impreso: 2075-8936 / DOI 10246451213131212
Copyright: © 2024 by the authors. Submitted for open access publication under the terms and conditions of the Creative Commons Attribution (CC BY) license

Descomposición:

- **Sujeto Activo:** El sujeto activo es impropio, este delito puede ser cometido por cualquier persona imputable.
- **Sujeto Pasivo:** El sujeto pasivo es impropio este delito afecta a cualquier persona.
- **Verbo Rector:** Engañar
- **Bien Jurídico:** Delitos contra la propiedad
- **Condición Sine Qua non:** Llamadas telefónicas para la adquisición de datos personales
- **Elemento Subjetivo:** Doloso
- **Pena o Sanción:** privación de libertad de tres (3) a seis (6) años y con multa de sesenta (60) a doscientos (200) días.

MANIPULACIÓN POR RED SOCIAL

Quien, mediante la utilización de medios tecnológicos, envíe mensajes por cualquier red social con la intención de engañar y adquirir información personal ajena, con el fin de obtener un beneficio indebido para sí o para un tercero, será sancionado con privación de libertad de tres (3) a seis (6) años y con una multa de sesenta (60) a doscientos (200) días

Descomposición:

- **Sujeto Activo:** El sujeto activo es impropio, este delito puede ser cometido por cualquier persona imputable.
- **Sujeto Pasivo:** El sujeto pasivo es impropio este delito afecta a cualquier persona.
- **Verbo Rector:** Manipular, enviar
- **Bien Jurídico:** Delitos contra la propiedad
- **Condición Sine Qua non:** Adquirir información personal ajena
- **Elemento Subjetivo:** Doloso
- **Pena o Sanción:** privación de libertad de tres (3) a seis (6) años y con multa de sesenta (60) a doscientos (200) días.

EXPOSICIÓN DE DOCUMENTOS ELECTRÓNICOS

Si accediera a todo o en parte de un medio tecnológico, vulnerando medidas de seguridad, con el fin de exponer públicamente información de datos o documentos personales de personas naturales o jurídicas, ocasionando daño o perjuicio, la sanción será con privación de libertad de tres (3) a seis (6) años y con multa de sesenta (60) a doscientos (200) días.

Descomposición:

- **Sujeto Activo:** El sujeto activo es impropio, este delito puede ser cometido por cualquier persona imputable.
- **Sujeto Pasivo:** El sujeto pasivo es impropio este delito afecta a cualquier persona.
- **Verbo Rector:** Acceder
- **Bien Jurídico:** Delitos contra la propiedad
- **Condición Sine Qua non:** exponer públicamente información de datos o documentos personales
- **Elemento Subjetivo:** Doloso

Revista JURIS STUDIA Diciembre de 2024
ISSN Digital: 2075-8944 ISSN Impreso: 2075-8936 / DOI 10246451213131212
Copyright: © 2024 by the authors. Submitted for open access publication under the terms and conditions of the Creative Commons Attribution (CC BY) license

- **Pena o Sanción:** privación de libertad de tres (3) a seis (6) años y con multa de sesenta (60) a doscientos (200) días.

6.3 MODIFICACIÓN E INCORPORACIÓN EN LOS ARTÍCULOS 363BIS Y 363TER DEL CÓDIGO PENAL DE BOLIVIA

Artículo 363 BIS. - (MANIPULACIÓN INFORMÁTICA). *El que con la intención de obtener un beneficio indebido para sí o un tercero, manipule un procesamiento o transfiera datos informáticos que conduzcan a un resultado incorrecto o evite un proceso tal cuyo resultado habría sido correcto, ocasionando de esta manera una transferencia patrimonial en perjuicio de un tercero, incurrirá en alguna de las tipificaciones delictivas detalladas a continuación:*

a) ***Suplantación de Identidad Digital.*** *Quien, utilizando medios tecnológicos, se haga pasar por una persona natural o jurídica e invite a otro a ingresar sus datos personales a un enlace, con la intención de obtener un beneficio indebido para sí o un tercero, será sancionado con privación de libertad de tres (3) a seis (6) años y con una multa de sesenta (60) a doscientos (200) días*

b) ***Engaño por Voz Virtual****. Quien, mediante la utilización de medios tecnológicos, realice llamadas telefónicas para la adquisición de datos personales con la intención de obtener un beneficio indebido para sí o para un tercero, será sancionado con privación de libertad de tres (3) a seis (6) años y con una multa de sesenta (60) a doscientos (200) días.*

c) ***Manipulación por Red Social.*** *Quien, mediante la utilización de medios tecnológicos, envíe mensajes por cualquier red social con la intención de engañar y adquirir información personal ajena, con el fin de obtener un beneficio indebido para sí o para un tercero, será sancionado con privación de libertad de tres (3) a seis (6) años y con una multa de sesenta (60) a doscientos (200) días*

Artículo 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, ocasionando perjuicio al titular de la información, será sancionado con prestación de trabajo hasta un (1) año o multa hasta doscientos (200) días.*

Si accediera a todo o en parte de un medio tecnológico, vulnerando medidas de seguridad, con el fin de exponer públicamente información de datos o documentos personales de personas naturales o jurídicas, ocasionando daño o perjuicio, la sanción será con privación de libertad de tres (3) a seis (6) años y con multa de sesenta (60) a doscientos (200) días.

7. CONCLUSION

La incorporación de los delitos informáticos actuales, tales como ***la suplantación de identidad digital, el engaño por voz virtual, la manipulación por redes sociales y la exposición de documentos digitales,*** ayudara a identificar y sancionar los infractores, evitando que queden impunes. A pesar de que estos delitos son ampliamente cometidos a través de medios tecnológicos, no están tipificados en el Código Penal, el cual se considera general y tradicional, dificultando su adaptación a los problemas emergentes en el ámbito digital. Las autoridades han enfrentado y siguen enfrentando obstáculos para mantenerse al día con los avances tecnológicos, limitando su capacidad de respuesta. La burocracia y la lentitud en los procesos han obstaculizado la implementación efectiva de políticas informáticas, mientras que la desconexión entre las autoridades y la comunidad

ISSN Digital: 2075-8944 ISSN Impreso: 2075-8936 / DOI 10246451213131212
Copyright: © 2024 by the authors. Submitted for open access publication under the terms and conditions of the Creative Commons Attribution (CC BY) license

tecnológica han llevado a políticas poco reflexivas. Aunque los avances tecnológicos han brindado oportunidades, también han aumentado os riesgos para los derechos individuales. El sistema judicial boliviano ha carecido de conocimientos y recursos para abordar eficazmente los delitos informáticos, lo que destaca la importancia de la cooperación internacional para enfrentar este problema global.

Se ha recomendado fortalecer la legislación, capacitar a las fuerzas del orden, educar al público sobre seguridad cibernética y actualizar continuamente las medidas de prevención. Estas acciones buscan mejorar la capacidad del país para combatir los delitos informáticos en el futuro.

Referencias bibliográficas

LIBROS

Bacigalupo, E. (1999). *Derecho Penal Parte General.* España. Editorial Hammurabi.

Belloch, C. (2020). *Los recursos tecnológicos en logopedia*. Universidad de Valencia.

Cabanellas, G. (1979). *Diccionario jurídico elemental*. Argentina. Editorial Heliasta.

Castells, M. (2002). *Tecnologías de la información y la comunicación y desarrollo global.*

Cordova, M. M. (2014). *Derecho Informático*. Santa Cruz, Bolivia: Creative Commons.

Cuevas, J. I. F. (2003). *Sociedad de la Información y Cultura Mediática*.

De Asúa, J. (2003). *La Ley y el delito*. Editorial Porrúa.

Del Pino, S. D. (2016). Delitos informáticos: Generalidades.

Garcia, J. O. (2015). *Metodología de la Investigación Jurídica.* México. Editorial Maporrua.

Hernández, R., Fernández, C., Baptista, P. (2014). *Metodología de la Investigación*. México. McGraw - Hill.

Huerta, M. & Líbano, C. (1996). *Delitos Informáticos*. Editorial Cono Sur Ltda.

Muñoz, C. F. (2001). *Introducción al derecho penal*. Euros Editores

Ossorio, M. (s.f.). *Diccionario de Ciencias Juridicas, Politicas y sociales*. Editorial Heliasta.

Rivera S, J. (2004). *Jurisdicción constitucional. Procesos constitucionales en Bolivia*. Cochabamba. Kipus.

Romero, I. M. (2002). *Apuntes de Criminología*. La Paz.

Sevilla, R. M. Á. (s.f). *Resumen sobre Internet*. Universidad de Guadalajara.

Téllez, V.J. (2014). *Derecho Informático*. México. Editorial Mcgraw Hill Educación.

Revista JURIS STUDIA Diciembre de 2024
ISSN Digital: 2075-8944 ISSN Impreso: 2075-8936 / DOI 10246451213131212
Copyright: © 2024 by the authors. Submitted for open access publication under the terms and conditions of the Creative Commons Attribution (CC BY) license

Welzel, H. (2014). *Derecho penal alemán.*

Wolf, E. (2005). *Las categorías de la tipicidad: estudios previos sobre una doctrina general de la parte especial del derecho penal.*

Zapata, F., & Zapata, H. (2015). *Derecho procesal penal y procedimiento penal boliviano*. Cochabamba, Bolivia. Olimpo.

PÁGINAS WEB

Argentina.gob.ar. (diciembre de 2020) *¿Qué es la ingeniería social y cómo me protejo?* Argentina.gob.ar. https://www.argentina.gob.ar/justicia/convosenlaweb/situaciones/que-es-la-ingenieria-social-y-como-protegerte

Bahillo, L. (16 de mayo de 2023). *Historia de Internet: ¿cómo nació y cuál fue su evolución?* Marketing 4 Ecommerce. https://marketing4ecommerce.net/historia-de-internet/

Belloch, C. (7 de septiembre del 2013). *Internet*. Entornos virtuales de formación. https://www.uv.es/bellochc/pedagogia/EVA1.wiki?1

Castillo, C. (2023). *"Phishing", "vishing", "smishing", ¿qué son y cómo protegerse de estas amenazas?* BBVA. https://www.bbva.com/es/innovacion/phishing-vishing-smishing-que-son-y-como-protegerse-de-estas-amenazas/

Ciudadanía. (17 de noviembre de 2021). *¿Qué es el vishing?* Ciudadanía. https://www.incibe.es/ciudadania/blog/que-es-el-vishing

Guía de Formación Cívica. (s.f). Biblioteca del Congreso nacional de Chile. https://www.bcn.cl/formacioncivica/detalle_guia?h=10221.3/45670

Wikipedia. (s.f.). *Ciberespacio*. Wikipedia. https://es.wikipedia.org/wiki/Ciberespacio

LEYES, CÓDIGOS, CONSTITUCIONES, CONVENIOS, CONVENCIONES

Código Penal Boliviano. [CPB]. 10 de marzo de 1997. (Bolivia).

Código Penal Decreto Legislativo N 635. 16 de octubre de 2018. (Perú).

Constitución Política del Estado de Bolivia. 7 de febrero de 2009 (Bolivia).

Convenio de Budapest. 4 de junio de 2021.

Ley 11179 de 1921. Código Penal. 3 de noviembre de 1921. (Argentina).

Ley 30096 de 2013. Ley de delitos informáticos. 21 de octubre de 2013. (Perú).

ONU (2019). Lucha contra la utilización de las tecnologías de la información y las telecomunicaciones con fines delictivos.

ISSN Digital: 2075-8944 ISSN Impreso: 2075-8936 / DOI 10246451213131212
Copyright: © 2024 by the authors. Submitted for open access publication under the terms and conditions of the Creative Commons Attribution (CC BY) license

ARTÍCULOS CIENTÍFICOS

Crovi, D. D. (2002). Sociedad de la información y el conocimiento. Entre el optimismo y la desesperanza. *Revista Mexicana de Ciencias Políticas y Sociales*, 65(185), 13-33.

Crovi, D. D. (2005). La sociedad de la información: Una Mirada Desde La comunicación. *Ciencia*.

Domínguez, A., & Villalobos, G. (2019). *Hecho, acto negocio jurídico*. Unam.mx. https://archivos.juridicas.unam.mx/www/bjv/libros/8/3834/6.pdf

Figuera, S. C., Cedeño, C. B., Camacho, M. A. (2017). Métodos de Razonamiento Lógico-Jurídico aplicados a Decisiones Judiciales: La Jurisprudencia como Mecanismo de Poder Estatal. *Revista de la Facultad de Jurisprudencia*, 2, 168-194.

Gómez, T.N. (2016). Historia de Internet en Bolivia. *Bolivia Digital, 15 miradas acerca del Internet y sociedad en Bolivia*, 1, 31-59.

Martínez Sánchez, F. (1996). La enseñanza ante los nuevos canales de información. *Perspectivas de las nuevas tecnologías en la educación*. 101-119.

Mora, R. (2005). La historia de Internet en Bolivia. *Semanario Pulso.*

Quiroz, Á. R. (2023). Metodología para redactar un proyecto de investigación en la ciencia del derecho. *FIPCAEC,* 8(2).

Zarate, E. (2022). La denuncia penal y el procedimiento administrativo disciplinario en infracciones de tipo G53 en la oficina de inspectoría del Cusco, 2021.

Revista JURIS STUDIA Diciembre de 2024
ISSN Digital: 2075-8944 ISSN Impreso: 2075-8936 / DOI 10246451213131212
Copyright: © 2024 by the authors. Submitted for open access publication under the terms and conditions of the Creative Commons Attribution (CC BY) license