

DELITOS INFORMÁTICOS EN BOLIVIA: NECESIDAD DE UNA REGULACIÓN PENAL DESDE EL ENFOQUE CONSTITUCIONAL

JARRY XAVIER BEJARANO PICOLOMINI¹

ORCID: 0009-0000-7086-7732

Enviado: 10 de noviembre 2025

Aceptado: 20 de diciembre 2025

RESUMEN

Hoy en días nos encontramos con una evolución de la informática de forma exponencial, más aún con el impacto que está teniendo en diversas áreas de nuestro cotidiano vivir la inteligencia artificial. En este contexto el presente artículo pretende sumergir al lector a la concientización de los delitos Informáticos en Bolivia, aspecto que necesita de manera urgente ser regulado desde una perspectiva constitucional, para lograr lo anterior resaltaremos la necesidad de revisar la legislación comparada e los países vecinos de Chile y Perú, así como también la imperante necesidad de alinear a Bolivia con la realidad de nuestra región, siempre desde una perspectiva constitucionalista.

Palabras clave: Cibereducación, Ciberdelincuente, Hackers, Crackers - Sabotaje Informático, Malware, Browser, Cookie Delitos informáticos.

1 Doctorante en Derecho Constitucional y Democracia, Universidad Autónoma Gabriel Rene Moreno. Master en Administración de Empresas, Bussines School. Master en Derecho Penal y Procesal Penal, Escuela Superior de Leyes. Ingeniero de Sistemas, Universidad Católica Boliviana "San Pablo" – jarrybejarano@gmail.com

ABSTRACT

Today, we are witnessing an exponential evolution of computing, even more so given the impact artificial intelligence is having on various areas of our daily lives. In this context, this article aims to raise awareness of cybercrime in Bolivia, an area that urgently needs to be regulated from a constitutional perspective. To achieve this, we will highlight the need to review the comparative legislation of neighboring Chile and Peru, as well as the imperative to align Bolivia with the reality of our region, always from a constitutional perspective.

Keywords: Cybereducation - Cybercrime - Hackers - Crackers - Computer Sabotage - Malware - Browser - Cookie - Computer crimes.

INTRODUCCIÓN

En las últimas dos décadas, Bolivia ha experimentado un crecimiento sostenido en el acceso y uso de las Tecnologías de la Información y la Comunicación (TIC), impulsado por la expansión de la infraestructura digital, el acceso masivo a dispositivos móviles y el desarrollo de servicios en línea en sectores públicos y privados. Según datos del Instituto Nacional de Estadística (INE) y la Autoridad de Regulación y Fiscalización de Telecomunicaciones y Transportes (ATT), el número de usuarios de internet en el país ha aumentado exponencialmente, pasando de menos de un millón en 2005 a más de 11 millones en la actualidad, lo que representa una penetración superior al 90% en áreas urbanas y en crecimiento constante en regiones rurales.

El uso cotidiano de tecnologías digitales ha transformado diversas actividades sociales, económicas y gubernamentales. Hoy en día, gran parte de la población boliviana utiliza plataformas digitales para la educación, el trabajo, las transacciones comerciales, el entretenimiento y la interacción social. Asimismo, el Estado ha promovido la digitalización de servicios públicos mediante plataformas de trámites en línea, sistemas de facturación electrónica y gestiones administrativas virtuales.

Si bien los diversos ámbitos de interacción se ven favorecidos por la fluidez que le brinda esta nueva alternativa tecnológica, no obstante,

crecen los riesgos relacionados al uso de las tecnologías informáticas y de comunicación². La legislación boliviana actual carece de tipificaciones específicas y mecanismos eficaces para enfrentar la creciente ola de delitos informáticos, tales como fraudes electrónicos, suplantación de identidad digital, acceso no autorizado a sistemas, robo de datos personales, ciberacoso, entre otros. Esta situación evidencia una desconexión entre el desarrollo tecnológico y el marco jurídico penal, generando vacíos legales que limitan la capacidad del Estado para proteger los derechos fundamentales de los ciudadanos en el entorno digital.

Sin embargo, conforme al informe del doceavo Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal³, impera la necesidad de una reforma normativa si se considera que la Constitución Política del Estado reconoce y garantiza el derecho a la privacidad, la inviolabilidad de las comunicaciones, la seguridad de la información y el acceso a la justicia. Por tanto, el avance de las TIC en Bolivia exige una respuesta jurídica proporcional que articule una regulación penal moderna, eficaz y respetuosa del enfoque constitucional.

1. MARCO CONCEPTUAL Y DOCTRINAL

1.1. BIEN JURÍDICO TUTELADO

El bien jurídico tutelado en los delitos informáticos se concibe en los planos de manera conjunta y concatenada; en el primero se encuentra la información de manera general (información almacenada, tratada y transmitida mediante los sistemas de tratamiento automatizado de datos), y en el segundo plano, los demás bienes afectados a través de este tipo de delitos como son la indemnidad sexual, intimidad, etcétera. Respecto de la información deber ser entendido como el contenido de las bases y/o banco de datos o el producto de los procesos informáticos automatizados; por lo tanto, se constituye en un bien autónomo de valor económico. Y es la importancia del valor

2 AROCENA, Gustavo. La regulación de los delitos informativos en el Código Penal argentino. Introducción a la ley nacional 26388. En: Boletín Mexicano de Derecho Comparado, nueva serie. Año XLV. No. 135. México, 2012; pp. 945-988.

3 Véase: Informe del 12vo. Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal; p. 61.

económico de la información lo que ha hecho que se incorpore como bien jurídico tutelado⁴.

Sin embargo, creemos que la información se debe considerar de diferentes formas, y no solo como un valor económico, sino como un valor intrínseco de la persona por la fluidez y el tráfico jurídico, y por los sistemas que lo procesan o automatizan, los mismos que se equiparan a los bienes protegidos tradicionalmente, tales como el patrimonio (fraude informático), la reserva, la intimidad y confidencialidad de los datos (agresiones informáticas a la esfera de la intimidad), la seguridad o fiabilidad del tráfico jurídico probatorio (falsificación de datos o documentos probatorios), etcétera.

Por tanto, en este tipo de delitos no se puede establecer a la información como el único bien jurídico afectado, por ser el principal y el más importante; sino a un conjunto de bienes que son afectados⁵, debido a la característica de la conducta típica en esta modalidad delictiva que colisiona con diversos intereses colectivos. Es en ese sentido que coincidimos con María Luz Gutiérrez Francés, quien señala que es un delito pluriofensivo⁶, sin perjuicio de que uno de tales bienes este independientemente tutelado por otro tipo penal⁷.

1. 2. PERFIL DEL CIBERDELINCUENTE

El perfil del ciberdelincuente (sujeto activo) en esta modalidad delictual requiere que este posea ciertas habilidades y conocimientos detallados en el manejo del sistema informático⁸. Es en razón a esas cualidades que se les ha calificado a los sujetos activos como delincuentes de cuello

4 Cfr. GUTIERREZ FRANCÉS, María Luz. Atentados contra la información como valor económico de empresa. MAZUELOS COELLO y REYNA ALFARO. Delitos informáticos. DURAND VALLADARES. Los delitos informáticos en el Código Penal Peruano. URQUIZO OLAECHEA. Revista Peruana de Ciencias Penales. No. 11. Lima, 2002.

5 GONZÁLES DE CHAVES CALAMITA, María. El llamado 'delito informático'. En: Anales de la Facultad de Derecho de la Universidad de la Laguna. No. 21. España, 2004; pp. 44-65.

6 GUTIERREZ FRANCES, María. Fraude Informático y estafa. En: Centro de Publicaciones del Ministerio de Justicia. Madrid, 1991.

7 Por la ubicación sistemática de estos delitos dentro del Código Penal de 1991 y antes de la dación de la Ley penal especial 30096, el bien jurídico considerado era el patrimonio por las conductas dirigidas a dañar, alterar o destruir una base de datos. Véase GALVEZ VILLEGAS, Tomas y Walter DELGADO TOVAR. Derecho Penal Parte Especial. Tomo III. Lima: Jurista Editores, 2002; p.1207.

8 AZAOLA CALDERON, Luis. Delitos informáticos y Derecho penal. México: UBIJUS, 2010; p. 27.

blanco⁹, que tienen como características:

a) Poseer importantes conocimientos informáticos.

b) Ocupar lugares estratégicos en su centro laboral, en los que se maneja información de carácter sensible (se denominan delitos ocupacionales, ya que se comenten por la ocupación que se tiene y el acceso al sistema).

Para Marcelo Manson, los infractores de la ley penal en materia de delitos informáticos no son delincuentes comunes y corrientes, sino que, por el contrario, son personas especializadas en la materia informática¹⁰. Agrega que “las personas que cometen los delitos informáticos son aquellas que poseen ciertas características que no presentan el denominador común, esto es, habilidades para el manejo de los sistemas informáticos y que por su situación laboran en puestos estratégicos donde se maneja información sensible”.

Camacho Losa considera que el perfil de estas personas no coincide con el de un delincuente marginal, y caracteriza a los autores de estas infracciones como empleados de confianza de las empresas afectadas¹¹.

Vives Antón y Gonzales Cussac afirman que “sujeto activo puede ser tanto las personas legítimamente autorizadas para acceder y operar el sistema (operadores, programadores u otros), como terceros no autorizados que acceden a las terminales públicas o privadas”¹². Gutiérrez Francés y Ruiz Vadillo difieren de estos puntos de vista y sostienen que “el autor del delito informático puede serlo cualquiera, no precisando el mismo de determinados requisitos personales o conocimientos técnicos cualificados”¹³.

9 “Se le denomina así a la delincuencia informática debido a los estudios sobre criminalidad informática orientados en las manifestaciones en el ámbito económico patrimonial, donde la doctrina determinó que el sujeto activo del delito informático poseía un alto nivel socioeconómico”. AZAOLA CALDERON, Luis. Delitos informáticos y Derecho penal. Óp. cit.; pp. 27 y 28.

10 MANSON, Marcelo. Legislación sobre delitos informáticos. Referencia de 27 de diciembre del 2013. Disponible en web: <https://dl.dropbox.com/u//dl.legislacioncomparada.pdf>.

11 CAMACHO LOSA, Luis. El delito informático. Madrid: Gráficas Cóndor, 1987; pp. 83- 84.

12 VIVES ANTÓN, Tomás y José Luis GONZÁLES CUSSAC. Comentarios al código Penal 1995. Valencia: Tiront Blanch, 1996; p. 1238.

13 GUTIERRES FRANCES, María. Fraude informático y estafa. RUIZ VADILLO, Enrique. Tratamiento a la delincuencia informática. En AZAOLA CALDERON, Luis. Delitos informáticos y Derecho penal. Óp. cit.; p. 29.

Por nuestra parte, si bien consideramos que el sujeto activo puede ser cualquier persona (con conocimientos y habilidades en informática), compartimos parcialmente la postura de que el sujeto activo debe ocupar un puesto laboral que le permita acceder a información sensible. Sin embargo, no están excluidos los sujetos que sin ocupar algún cargo estratégico pueden ser sujeto activo por sus habilidades y conocimientos sobre la informática. Por ende, se trata de delitos de dominio.

A estos tipos de sujetos se les denomina de diferente manera dependiendo el modo como actúan y que conductas son las que realizan:

a) Hackers; Son personas dedicadas, por afición u otro interés, a violar programas y sistemas supuestamente impenetrables. Conocido como delincuente silencioso o tecnológico. Les gusta indagar por todas partes y conocer el funcionamiento de los sistemas informáticos. Son personas que realizan esta actividad como reto intelectual, sin producir daño alguno con la única finalidad de descifrar y conocer los sistemas informáticos.

Para Sieber los hackers son “personas que acceden sin autorización a un sistema de proceso de datos a través de un proceso de datos a distancia, no cometido con finalidades manipuladoras, fraudulentas, de espionaje, ni sabotaje, sino sencillamente como paseo por placer no autorizado”¹⁴. Morón Lerma define a los hackers como “personas que acceden o interfieren sin autorización, de forma subrepticia, a un sistema informático o redes de comunicación electrónica de datos y utilizan los mismos sin autorización o más allá de lo autorizado”¹⁵.

b) Crackers; Son personas que se introducen en sistemas remotos con la intención de destruir datos, denegar el servicio a usuarios legítimos y, en general, a causar problemas a los sistemas, procesadores o redes informáticas, conocidos como piratas electrónicos.

La característica que la diferencia de los hackers es que los crackers usan programas ya creados que pueden adquirir, normalmente vía internet;

14 (27) SIE BER, Ulrich. Criminalidad informática: peligro y prevención; p. 77. MIR PUIG, Santiago. Delincuencia informática.

15 (28) MORON LERMA, Esther. Internet y Derecho Penal: hacking y otras conductas ilícitas en la red. 2da edición. Navarra: Aranzadi; p. 51.

mientras que los hackers crean sus propios programas, tienen mucho conocimiento sobre los programas y conocen muy bien los lenguajes informáticos¹⁶. Por otra parte, Morant Vidal define a estos sujetos como “personas que se introducen en sistemas remotos con la intención de destruir datos, denegar el servicio a usuarios legítimos, y en general a causar problemas”¹⁷.

Alfonso Laso sostiene que el cracker “es la persona que, de manera intencionada, se dedica a eliminar o borrar ficheros, a romper los sistemas informáticos, a introducir virus, etcétera”¹⁸.

1. 3. AUMENTO DE LA DELINCUENCIA INFORMÁTICA EN EL PAÍS.

En 2023, Bolivia registró 3.768 casos de delitos cibernéticos, según el Observatorio de Delitos Informáticos de Bolivia (ODIB). Los delitos más comunes incluyen fraude o estafa informática, amenazas y grooming. Las regiones con mayor incidencia son La Paz, Santa Cruz y Cochabamba¹⁹.

Además, las estafas digitales aumentaron un 43% en el primer semestre de 2023 en comparación con el mismo período de 2022. Este incremento afecta a diversos grupos de la población, incluyendo comerciantes, estudiantes y adultos mayores²⁰.

Un informe del Centro S.O.S. Digital reveló que, entre junio de 2023 y mayo de 2024, 160 de las 210 personas que se contactaron con la línea de ayuda reportaron casos de violencia digital, siendo el abuso sexual relacionado con las TIC la forma más frecuente²¹.

16 (29) AZAOLA CALDERON, Luis. Óp. cit.; p. 32.

17 (30) MORANT VIDAL, Jesús. Protección penal de la intimidad frente a las nuevas tecnologías. Valencia: Práctica de Derecho, 2002; p. 44.

18 DE ALFONSO LASO, Daniel. El hackerin blanco. Una conducta ¿punible o impune? En Internet y derecho penal, Cuadernos de Derecho Judicial, Consejo General del poder Judicial. Madrid, 2001; pp.110-111.

19 Observatorio de Delitos Informáticos de Bolivia (ODIB). (2023). Informe estadístico anual sobre cibercriminalidad en Bolivia. La Paz: ODIB.

20 Agencia de Gobierno Electrónico y Tecnologías de Información y Comunicación (AGETIC). (2023). Reporte de estafas digitales en Bolivia 2023. La Paz: AGETIC.

21 Centro S.O.S. Digital. (2024). Informe sobre violencia digital en Bolivia (junio 2023 - mayo 2024). Santa Cruz: Fundación Internet Bolivia.

Estos datos reflejan una tendencia alarmante en el país, donde la rápida adopción de tecnologías digitales no ha sido acompañada por una legislación penal actualizada y efectiva para combatir los delitos informáticos.

1. 4. PROBLEMAS LEGALES ACTUALES: VACÍOS NORMATIVOS Y OBSOLESCENCIA DEL CÓDIGO PENAL.

El sistema jurídico penal boliviano enfrenta serias limitaciones para enfrentar los desafíos que plantea la criminalidad informática, principalmente debido a la existencia de vacíos normativos y a la obsolescencia del actual Código Penal. Promulgado en 1972, este cuerpo legal fue concebido en una época previa a la expansión de las tecnologías de la información y la comunicación, por lo que no contempla de manera expresa las nuevas modalidades delictivas que se cometen en entornos digitales.

Aunque en los últimos años se han realizado esfuerzos fragmentarios mediante leyes complementarias (como la Ley N.º 164 de Telecomunicaciones o algunas disposiciones de la Ley de Protección de Datos Personales en proyecto), Bolivia aún no cuenta con una legislación penal integral que tipifique delitos informáticos como el acceso no autorizado a sistemas informáticos, el sabotaje digital, el phishing, la suplantación de identidad digital, la interceptación de comunicaciones electrónicas, entre otros.

Esta ausencia de regulación específica impide a fiscales, jueces y policías aplicar con claridad la ley ante hechos delictivos en línea, generando inseguridad jurídica y afectando la tutela efectiva de los derechos fundamentales de las víctimas²². En muchos casos, la falta de una normativa clara obliga a los operadores de justicia a recurrir a analogías con tipos penales tradicionales, lo cual entra en tensión con el principio de legalidad penal²³.

22 De la Cuesta, J. L. (2014). Derecho penal y nuevas tecnologías. *Revista Electrónica de Ciencia Penal y Criminología*, 16, 1–34.

23 Silva Sánchez, J. M. (2000). *La expansión del Derecho penal: aspectos de la política criminal en las sociedades postindustriales*. Madrid: Civitas.

Además, el Código Penal actual no establece criterios técnicos ni doctrinales sobre la prueba digital, la cadena de custodia informática o los procedimientos adecuados para preservar y presentar evidencia tecnológica en juicio, lo que debilita las investigaciones y favorece la impunidad²⁴. Esta situación se agrava con la falta de capacitación especializada en ciberdelincuencia dentro de las instituciones del sistema de justicia penal. Por ejemplo, un informe de la UNODC señala que la mayoría de los países en desarrollo carecen de protocolos estandarizados para el manejo de evidencia electrónica y de recursos humanos con conocimientos técnico-jurídicos adecuados²⁵.

En consecuencia, la legislación penal vigente no solo es insuficiente frente a las amenazas que plantea el cibercrimen, sino que también se encuentra desalineada con los principios constitucionales de legalidad, seguridad jurídica y protección efectiva de los derechos, establecidos en la Constitución Política del Estado²⁶.

Esta desconexión entre la norma penal y la realidad digital evidencia la urgencia de una reforma normativa profunda que aborde de manera integral y con enfoque constitucional los delitos informáticos en Bolivia.

Los delitos informáticos constituyen un fenómeno jurídico y social en constante evolución. Según la ONU, se trata de actos delictivos cometidos mediante o contra sistemas informáticos, redes de comunicación o datos digitales²⁷.

La OEA, a través de su Grupo de Trabajo sobre Delito Cibernético, define estos delitos como conductas que vulneran la seguridad de la información, la integridad de los sistemas o los derechos de las personas mediante medios tecnológicos²⁸.

Desde la doctrina internacional, se reconocen dos grandes categorías:

24 Interpol. (2020). *Cybercrime: An Overview of Incidents and Threats*. Recuperado de <https://www.interpol.int/en/Crimes/Cybercrime>

25 UNODC. (2013). *Comprehensive Study on Cybercrime*. United Nations Office on Drugs and Crime.

26 Constitución Política del Estado Plurinacional de Bolivia (2009), Arts. 115-117.

27 United Nations. (2011). *Draft Comprehensive Study on Cybercrime*. United Nations Office on Drugs and Crime.

28 Organización de Estados Americanos (OEA). (2019). *Estrategia Integral para Combatir las Amenazas a la Seguridad Cibernética*.

1. **Delitos informáticos en sentido estricto**, que solo pueden cometerse mediante el uso de tecnología (por ejemplo, acceso ilícito a sistemas, sabotaje informático, interceptación de datos)²⁹.
2. **Delitos informáticos en sentido amplio**, que son delitos tradicionales cometidos con ayuda de herramientas digitales (por ejemplo, estafa, acoso, amenazas)³⁰.

La clasificación doctrinal puede dividirse además en:

- Delitos contra la confidencialidad, integridad y disponibilidad de datos y sistemas.
- Delitos relacionados con el contenido (pornografía infantil, incitación al odio).
- Delitos asociados al fraude y la manipulación informática³¹.

En cuanto a los principios del Derecho Penal aplicables al entorno digital, destacan:

- **Legalidad penal** (*nullum crimen, nulla poena sine lege*): exige tipos penales claros y previsibles, lo que se torna esencial frente a tecnologías cambiantes³².
- **Proporcionalidad y mínima intervención**: el Derecho Penal debe intervenir solo cuando otros mecanismos son insuficientes³³.
- **Culpabilidad y responsabilidad personal**: se requiere atribuir la conducta a un sujeto, lo cual es complejo en entornos anónimos o automatizados³⁴.

29 Arocena, G. (2012). La regulación de los delitos informáticos en el Código Penal argentino. *Boletín Mexicano de Derecho Comparado*, (135), 945–988.

30 Clough, J. (2015). *Principles of Cybercrime* (2nd ed.). Cambridge University Press.

31 Council of Europe. (2001). *Convention on Cybercrime* (ETS No. 185). Budapest.

32 Jakobs, G. (1997). *Derecho penal del enemigo*. Civitas.

33 Silva Sánchez, J. M. (2000). *La expansión del Derecho penal*. Madrid: Civitas.

34 Clough, J. (2015). *Principles of Cybercrime* (2nd ed.). Cambridge University Press.

- **Presunción de inocencia y debido proceso:** deben garantizarse en procedimientos digitales, especialmente en la recolección de evidencia electrónica³⁵.

El marco conceptual y doctrinal demuestra que los delitos informáticos no solo implican desafíos técnicos, sino también jurídicos y constitucionales, lo que exige una regulación penal específica, clara y alineada con los derechos fundamentales³⁶.

2. SITUACIÓN ACTUAL DE LA LEGISLACIÓN BOLIVIANA

El Código Penal boliviano de 1972, aunque ha sufrido algunas reformas parciales, no contempla de forma explícita los delitos informáticos. Su redacción refleja un paradigma pre-digital, incapaz de responder adecuadamente a conductas delictivas modernas vinculadas a sistemas de información, redes o datos personales³⁷.

En 2019, se presentó un anteproyecto de ley sobre delitos informáticos, que proponía tipificar figuras como el acceso ilícito, la manipulación de datos y el fraude informático. Sin embargo, el proyecto no prosperó en la Asamblea Legislativa, y desde entonces, no se han registrado avances significativos en la materia³⁸.

La ausencia de regulación específica ha generado un vacío normativo importante. Delitos como:

- Acceso ilícito a sistemas informáticos (hacking),
- Fraude digital (phishing, scam, suplantación de identidad),
- Ciberacoso (particularmente en redes sociales y contra mujeres),

35 De la Cuesta, J. L. (2014). Derecho penal y nuevas tecnologías. *Revista Electrónica de Ciencia Penal y Criminología*, 16, 1–34.

36 Council of Europe. (2001). *Convention on Cybercrime* (ETS No. 185). Budapest.

37 Romero, E. (2022). Vacíos normativos y delitos informáticos en Bolivia. *Revista Boliviana de Derecho Penal*, 12(2), 85-104.

38 Asamblea Legislativa Plurinacional de Bolivia. (2019). *Anteproyecto de Ley sobre Delitos Informáticos*.

- Pornografía infantil en línea (que actualmente se aborda solo desde figuras tradicionales), carecen de una respuesta penal clara y eficaz. Esta situación afecta la capacidad del sistema judicial para investigar, procesar y sancionar estas conductas, generando impunidad y revictimización³⁹.

En comparación, países vecinos como Chile, Argentina y Brasil han desarrollado legislaciones más actualizadas. Chile reformó su Código Penal para incluir delitos informáticos en 2022, y Argentina cuenta con una Ley de Delitos Informáticos desde 2008⁴⁰. Bolivia, en cambio, permanece rezagada, tanto en la tipificación como en el tratamiento procesal de la prueba digital.

Este retraso normativo compromete no solo la eficacia penal, sino también el cumplimiento de los compromisos internacionales asumidos por Bolivia en materia de derechos humanos y cooperación contra el cibercrimen⁴¹.

3. ANÁLISIS CONSTITUCIONAL

La Constitución Política del Estado (CPE) reconoce una serie de derechos fundamentales que se ven directamente afectados por la expansión de las tecnologías digitales y la falta de regulación penal específica. Entre ellos, destacan:

- Artículo 25 CPE: protege la inviolabilidad de las comunicaciones privadas, aplicable también a correos electrónicos, chats y redes sociales⁴².
- Artículos 21 y 66 CPE: reconocen el derecho a la dignidad, la honra, la imagen y la intimidad.
- Artículos 115 y 116 CPE: garantizan el debido proceso, la legalidad penal y la seguridad jurídica.

39 Fundación Internet Bolivia. (2023). Informe sobre delitos digitales y brecha normativa.

40 Ministerio de Justicia de Chile. (2022). Reforma al Código Penal para delitos informáticos.

41 ONU-DDHH. (2021). Lineamientos para una regulación penal compatible con derechos humanos.

42 Constitución Política del Estado Plurinacional de Bolivia (2009).

Frente al aumento de conductas delictivas en entornos digitales, la falta de normas específicas genera una omisión por parte del Estado en su deber de protección⁴³. Esta omisión legislativa puede ser considerada una forma de vulneración indirecta de derechos humanos, al no brindar herramientas adecuadas para investigar y sancionar hechos que afectan gravemente la vida privada, la integridad y la seguridad de los ciudadanos.

El principio de legalidad penal, consagrado constitucionalmente, exige que las conductas delictivas estén definidas con claridad, precisión y previsibilidad. En el ámbito digital, donde los comportamientos son novedosos y complejos, este principio requiere un esfuerzo especial del legislador para definir tipos penales modernos sin afectar garantías fundamentales⁴⁴.

Además, la jurisprudencia internacional, especialmente la de la Corte Interamericana de Derechos Humanos, ha sostenido que los Estados tienen la obligación positiva de proteger a las personas frente a amenazas tecnológicas, incluso si provienen de particulares. Este deber se refuerza por el bloque de constitucionalidad, que integra tratados internacionales como el Pacto Internacional de Derechos Civiles y Políticos y la Convención Americana sobre Derechos Humanos⁴⁵.

El derecho a la seguridad jurídica se ve también afectado. Sin normas claras sobre delitos informáticos, ni operadores del sistema penal ni los ciudadanos conocen con certeza los límites de la conducta permitida y la posible reacción estatal. Esto genera inseguridad jurídica y reduce la eficacia del sistema penal.

En resumen, la ausencia de regulación penal específica sobre delitos informáticos contradice directamente el mandato constitucional de proteger los derechos fundamentales, y pone en evidencia la necesidad urgente de una ley que garantice dicha protección bajo un enfoque constitucional, respetuoso de principios como legalidad, proporcionalidad, debido proceso y seguridad jurídica.

43 Corte IDH. (2015). Opinión consultiva OC-23/17.

44 Ferrajoli, L. (2001). *Derecho y razón*. Trotta.

45 Organización de Estados Americanos (OEA). (2019). *Estrategia Integral en Seguridad Cibernética*.

4. ARGUMENTOS A FAVOR DE UNA LEY ESPECÍFICA

La adopción de una ley penal específica sobre delitos informáticos en Bolivia se justifica por múltiples razones jurídicas, técnicas y sociales. En primer lugar, dicha ley permitiría una protección integral de los derechos digitales de las personas, especialmente de los más vulnerables (niños, mujeres, adultos mayores), quienes con mayor frecuencia sufren violencia, estafas o acoso en entornos digitales⁴⁶.

En segundo lugar, una ley especializada mejoraría significativamente la capacidad investigativa del Estado. Hoy, la falta de tipos penales y protocolos técnicos limita el accionar del Ministerio Público, la Policía y el sistema judicial en general, dificultando la preservación de evidencia digital, la cooperación internacional y la atribución de responsabilidades⁴⁷.

Asimismo, una norma penal especial permitiría establecer tipos penales precisos, procedimientos técnicos específicos y mecanismos de protección de derechos durante la investigación digital, todo ello en coherencia con los principios y garantías constitucionales.

La experiencia comparada demuestra que países que han implementado leyes específicas —como Chile con su Ley 21.459 (2022), Argentina con su Ley 26.388 (2008) o España con su Código Penal reformado— han mejorado sus capacidades para enfrentar el cibercrimen, garantizar el debido proceso y proteger a las víctimas⁴⁸.

Por tanto, Bolivia no solo requiere una ley específica, sino una que esté alineada con la Constitución Política del Estado, que respete el principio de legalidad, la proporcionalidad penal, y que esté articulada a estándares internacionales como el Convenio de Budapest sobre Ciberdelincuencia⁴⁹.

46 UNODC. (2013). *Comprehensive Study on Cybercrime*.

47 Interpol. (2020). *Cybercrime: An Overview of Incidents and Threats*.

48 Gutiérrez, M. (2021). *Derecho penal y cibercrimen comparado*. Editorial Jurídica.

49 Council of Europe. (2001). *Convention on Cybercrime (ETS No. 185)*. Budapest.

CONCLUSIONES Y RECOMENDACIONES

La presente investigación ha demostrado que Bolivia enfrenta una grave deficiencia normativa en materia de delitos informáticos. A pesar del avance de las TIC y el aumento de la criminalidad digital, el país carece de una legislación penal actualizada y específica. El Código Penal de 1972 resulta obsoleto frente a nuevas conductas delictivas como el fraude electrónico, el ciberacoso o la pornografía infantil en línea. Esta omisión legislativa no solo limita la respuesta penal, sino que también vulnera derechos fundamentales reconocidos en la Constitución Política del Estado.

Asimismo, se ha evidenciado que la falta de regulación penal clara compromete principios constitucionales esenciales como el de legalidad, debido proceso y seguridad jurídica. En este contexto, resulta urgente y necesario diseñar una ley penal específica que responda a los desafíos del entorno digital, siempre desde un enfoque constitucional y garantista.

Recomendaciones jurídicas

El futuro de la protección jurídica en el entorno digital depende de una respuesta legislativa integral, técnica y constitucionalmente sólida, con base a los siguientes temas de interés para la colectividad del estado boliviano.

- Tipificación penal clara de los delitos informáticos conforme a estándares internacionales.
- Creación de unidades especializadas en investigación digital dentro del Ministerio Público y la Policía Boliviana.
- Adhesión al Convenio de Budapest, como marco de cooperación internacional en la lucha contra el cibercrimen.
- Evaluar una posible reforma constitucional menor, si fuese necesario, para facilitar mecanismos de cooperación tecnológica y penal con otros Estados.

BIBLIOGRAFÍA

Agencia de Gobierno Electrónico y Tecnologías de Información y Comunicación (AGETIC).

2023 Reporte de estafas digitales en Bolivia 2023. La Paz: AGETIC.

CENTRO S.O.S. DIGITAL.

2024 Informe sobre violencia digital en Bolivia (junio 2023 - mayo 2024). Santa Cruz: Fundación Internet Bolivia.

OBSERVATORIO DE DELITOS INFORMÁTICOS DE BOLIVIA (ODIB).

2023 Informe estadístico anual sobre cibercriminalidad en Bolivia. La Paz: ODIB.

AROCENA, G.

2012 La regulación de los delitos informáticos en el Código Penal argentino. Boletín Mexicano de Derecho Comparado, (135), 945–988.

CLOUGH, J.

2015 Principles of Cybercrime (2nd ed.). Cambridge University Press.

Constitución Política del Estado Plurinacional de Bolivia.

2009

COUNCIL OF EUROPE.

2001 Convention on Cybercrime (ETS No. 185). Budapest.

DE LA CUESTA, J. L.

2014 Derecho penal y nuevas tecnologías. Revista Electrónica de Ciencia Penal y Criminología, 16, 1–34.

INTERPOL.

2020 Cybercrime: An Overview of Incidents and Threats. <https://www.interpol.int/en/Crimes/Cybercrime>

ORGANIZACIÓN DE ESTADOS AMERICANOS (OEA).

2019 Estrategia Integral para Combatir las Amenazas a la Seguridad Cibernética.

UNODC.

2013 Comprehensive Study on Cybercrime. United Nations Office on Drugs and Crime.

UNITED NATIONS.

2011 Draft Comprehensive Study on Cybercrime. UNODC.

ASAMBLEA LEGISLATIVA PLURINACIONAL DE BOLIVIA.

2019 Anteproyecto de Ley sobre Delitos Informáticos.

CLOUGH, J.

2015 Principles of Cybercrime (2nd ed.). Cambridge University Press.

COUNCIL OF EUROPE.

2001 Convention on Cybercrime (ETS No. 185). Budapest.

CORTE INTERAMERICANA DE DERECHOS HUMANOS.

2015 Opinión consultiva OC-23/17.

DE LA CUESTA, J. L.

2014 Derecho penal y nuevas tecnologías. Revista Electrónica de Ciencia Penal y Criminología, 16, 1-34.

FERRAJOLI, L.

2001 Derecho y razón. Madrid: Trotta.

FUNDACIÓN INTERNET BOLIVIA.

2023 Informe sobre delitos digitales y brecha normativa.

GUTIÉRREZ, M.

2021 Derecho penal y cibercrimen comparado. Editorial Jurídica.

JAKOBS, G.

1997 Derecho penal del enemigo. Civitas.

Ministerio de Justicia de Chile.

2022 Reforma al Código Penal para delitos informáticos.

ONU-DDHH.

2021 Lineamientos para una regulación penal compatible con derechos humanos.

ROMERO, E.

2022 Vacíos normativos y delitos informáticos en Bolivia. Revista Boliviana de Derecho Penal, 12(2), 85-104.

SILVA SÁNCHEZ, J. M.

2000 La expansión del Derecho penal. Madrid: Civitas.