Tesla Revista Científica, ISSN: 2796-9320
Vol. 4 Núm. 1 (2024), e369
https://doi.org/10.55204/trc.v4i1.e369

Área: Derecho
Artículo de revisión

Una comparación de la tipificación del ciberdelito en Sudamérica

A comparison of the classification of cybercrime in South America

Jorge Santiago Vallejo Lara [1] [0009-0007-1469-9296], Hillary Patricia Herrera Avilés [2] [0009-0003-1514-2247], Edwin Javier Ortega Campos [3] [0009-0005-6959-7970], Fredy Roberto Hidalgo Cajo [4] [0000-0001-6873-7250]

[1, 2, 4] Universidad Nacional de Chimborazo, Facultad de Ciencias Políticas y Administrativas. 060108. Riobamba - Chimborazo. Ecuador
{ jvallejo, hillary.herrera, fhidalgo }@unach.edu.ec
[3] Función Judicial, 180204. Ambato - Tungurahua. Ecuador, axl.ejoc.saou.272@gmail.com

CITA EN APA:
Vallejo Lara, J. S., Herrera Avilés, H. P., Ortega Campos, E. J., & Hidalgo Cajo, F. R. (2024). Una comparación de la tipificación del ciberdelito en Sudamérica. Tesla Revista Científica, 4(1), e369. https://doi.org/10.55204/trc.v4i1.e369

Recibido: 2024-03-25
Revisado: 2024-04-02 al 2023-04-27
Corregido: 2024-05-09
Aceptado: 2024-05-12
Publicado: 2024-05-16

TESLA
Revista Científica
ISSN: 2796-9320

Resumen: El análisis del ciberdelito por parte de juristas y expertos en seguridad informática ha resultado en la tipificación de conductas delictivas en muchas legislaciones del continente americano. A pesar de esto, aún no se ha realizado un estudio completo sobre la realidad del delito informático en esta región, lo que dificulta la identificación y sanción de ciertas conductas cibernéticas que deberían ser tratadas como delitos independientes. Ante esta necesidad, se realizó una investigación que identifica los delitos informáticos tipificados en países con avances significativos en la materia, con el fin de reconocer falencias y vacíos presentes en las legislaciones del continente americano. Este trabajo de investigación se basó en publicaciones académicas y en el análisis realizado por los autores, utilizando métodos teóricos y empíricos, así como técnicas de entrevista y encuesta. Como resultado, se detallaron las conductas criminales ejecutadas con herramientas informáticas según la legislación americana, se identificaron las deficiencias existentes y se propuso una solución consistente en tipificar ciertas conductas cibernéticas como delitos independientes en los cuerpos jurídico-penales de Sudamérica, evitando su sanción bajo figuras tradicionales que no reflejan proporcionalmente el daño causado.
Palabras Clave: Delito electrónico, internet, informático, ley, convenio.
Abstract: The analysis of cybercrime by jurists and experts in computer security has led to the classification of criminal behaviors in many legislations across the Americas. However, a comprehensive study of the reality of cybercrime in this region has not yet been conducted, making it difficult to identify and penalize certain cyber behaviors that should be treated as independent offenses. In response to this need, research was conducted to identify computer crimes classified in countries with significant advancements in the field, aiming to recognize deficiencies and gaps present in the legislations of the Americas. This research relied on academic publications and analysis by the authors, utilizing theoretical and empirical methods, as well as interview and survey techniques. As a result, criminal behaviors executed with computer tools were detailed according to American legislation, existing deficiencies were identified, and a solution was proposed consisting of classifying certain cyber behaviors as independent offenses in the legal-penal frameworks of South America, thereby avoiding their sanction under traditional figures that do not proportionally reflect the damage caused.
Keywords: Crime electronic, internet, computer, law, agreement

1. INTRODUCCIÓN

A lo largo de la historia, se señala el año 1969 como el punto de partida del internet. Desde su surgimiento, ha sido reconocido como una red descentralizada de comunicación, compuesta por una variedad de redes interconectadas que utilizan el protocolo TCP/IP. Este protocolo garantiza que estas redes heterogéneas formen una red global cohesiva. Inicialmente concebida para establecer múltiples canales de comunicación entre computadoras, el internet ha evolucionado hasta convertirse en una herramienta fundamental en la vida contemporánea, siendo descrito por algunos como una de las revoluciones tecnológicas más significativas (Muñoz, 2019).

Pons (2017) hace referencia al crecimiento exponencial de usuarios desde la década de 1990 hasta la actualidad ha transformado las sociedades, volviéndolas altamente dependientes de la tecnología informática para sus procesos económicos y sociales. Sin embargo, este avance también ha generado nuevas formas de delito, proporcionando a las criminales herramientas poderosas. Desde esta perspectiva, el ciberespacio se define como un dominio creado por el ser humano, separado de los tradicionales (tierra, aire, mar y espacio), pero interconectado con ellos y apoyado por infraestructuras físicas como las redes eléctricas.

Fernández y Martínez (2020) subrayan la relevancia de la ciberseguridad como un componente esencial en la protección de la sociedad actual. En su análisis, destacan que el ciberespacio brinda oportunidades, pero también conlleva riesgos, como las amenazas cibernéticas provenientes de diversos actores como Estados, organizaciones terroristas y grupos criminales. La ciberdelincuencia, se distingue por su naturaleza transfronteriza y la forma en que desafía las limitaciones tradicionales del Derecho Penal debido a la comunicación inmaterial a través de las TIC. Además, se hace referencia al Convenio de Ciberdelincuencia como un estándar internacional importante en la lucha contra este tipo de delitos en el entorno digital.

La aparición de términos como cibercrimen y ciberdelincuencia refleja la proliferación de actividades ilícitas en el ciberespacio, caracterizadas por su facilidad de ejecución, bajo costo en comparación con su impacto y la capacidad de llevarse a cabo de manera remota. Los ciberataques, impulsados por el anonimato y la accesibilidad técnica, resultan en vulnerabilidades y deficiencias en la protección, a menudo atrayendo la atención pública y siendo ampliamente difundidos por los medios digitales.

Según Choi y Toro-Álvarez (2017), a diferencia de los delitos no digitales, los ciberdelitos, especialmente en redes no indexadas, son extremadamente difíciles de detectar, pueden representar un mayor nivel de victimización secundaria, afectan a un mayor número de víctimas por cada acción cibercriminal, presentan desafíos en la prevención de la reincidencia en línea y proporcionan limitaciones en el enjuiciamiento. En cuanto a la dificultad de detección, afirmaron que los delitos cibernéticos requieren técnicas de investigación más elaboradas para identificarlos e individualizar a los delincuentes en línea, lo que crea una dificultad adicional para el sistema de justicia penal.

Holt (2012) afirma que esta dificultad puede estar relacionada con la naturaleza de la delincuencia en línea. En estos escenarios digitales, los delincuentes pueden usar técnicas de sigilo para disfrazar su identidad y ubicación, que se derivan de las funciones disponibles en ciertos navegadores de Internet y el entorno de comunicación de la red. Además, los ciberdelincuentes pueden utilizar las capacidades del crimen organizado o individual para evadir la detección y amplificar su capacidad delictiva. Entre estas capacidades se encuentran el uso de redes privadas virtuales (VPN) o la conexión a través de servidores proxy, lo que evita el seguimiento de la actividad cibercriminal en línea.

En la misma instancia Bolaños-Burgos y Gómez-Giacoman (2015) deduce la capacidad de

afectación que tiene el ciberdelito, a un gran número de víctimas con un solo acto, ilustra su impacto multiplicador. Por ejemplo, en ataques de denegación de servicio distribuido (DDoS), un solo delincuente puede involucrar a más de 2000 usuarios de Internet para llevar a cabo ataques a múltiples objetivos. Esta escalabilidad del daño supera con creces los límites de los delitos convencionales, permitiendo a los criminales alcanzar a miles de víctimas en cuestión de segundos mediante redes de dispositivos infectados. La prevención de la reincidencia en el ciberdelito presenta desafíos únicos debido a la naturaleza global de Internet y el anonimato que proporciona, junto con los avances tecnológicos rápidos y la dificultad para identificar y enjuiciar a los delincuentes en línea. La falta de programas efectivos de rehabilitación agrava esta situación, ya que los ciberdelincuentes pueden continuar operando en jurisdicciones con leyes menos efectivas o donde encuentren cierto grado de protección, aprovechando el anonimato en línea y la reducida capacidad de supervisión.

Los ciberdelincuentes, alimentados por el acceso a la tecnología y las oportunidades de autoformación en las redes sociales, perfeccionan sus habilidades técnicas para evadir las medidas de seguridad y persistir en sus actividades ilegales. En este contexto, Toro-Álvarez (2023) destaca la complejidad de las redes de ciberdelincuencia y la necesidad de una mayor coordinación internacional para hacer frente a esta amenaza. Se requieren respuestas multidisciplinarias que incluyan capacitación especializada, asignación adecuada de recursos para la investigación y manejo de evidencia digital, así como programas de rehabilitación adaptados a las complejidades del ciberdelito.

El delito informático, como cualquier otro delito, requiere una comprensión precisa de su definición jurídica. Según la definición clásica propuesta por Cuello (1964), un delito es una acción humana antijurídica, típica, culpable y punible. Esto implica que las infracciones informáticas son actos llevados a cabo por seres humanos que violan la ley y, al estar tipificados como tales, conllevan una sanción por parte del Estado.

Siguiendo esta línea, Salazar (2021) en su estudio “Ciberdelitos-Perfil-Criminológico” nos da a conocer que el delito informático puede entenderse como un acto humano culpable que se realiza utilizando herramientas informáticas y que causa daño a bienes jurídicamente protegidos, todo ello tipificado y sancionado por la normativa legal. Sin embargo, no todas las conductas cibernéticas merecen ser consideradas como delitos, ya que algunas pueden ser de menor gravedad y tratarse como contravenciones menores en el ámbito jurídico penal. Por lo tanto, es crucial diferenciar entre delitos informáticos e infracciones informáticas según su gravedad y repercusión.

A nivel internacional, se han establecido importantes medidas para combatir el ciberdelito, como la Convención de Cibercriminalidad organizada por el Consejo de Europa en 2001. Este instrumento amplió el alcance de las conductas consideradas delictivas y fue ratificado inicialmente por treinta países. Si los países no adoptan una postura seria frente al crecimiento de la criminalidad informática y no implementan medidas efectivas para combatir estas conductas delictivas, corren el riesgo de enfrentarse a una proliferación descontrolada de este fenómeno.

Para Tolinga (2021) en su estudio literario “Un análisis a la investigación de Ciberdelitos” atribuye que es fundamental que Ecuador esté a la vanguardia junto con otros países y tome decisiones proactivas, así como medidas concretas, para prepararse adecuadamente tanto para el presente como para el futuro. De esta manera, evitará quedar rezagado y enfrentar situaciones que podrían tener un impacto significativo en la sociedad ecuatoriana en la era de la información. Esto implica desarrollar estrategias integrales que aborden no solo la seguridad cibernética, sino también la legislación actualizada, la capacitación de profesionales en el campo de la ciberseguridad y la concienciación pública sobre los riesgos y las mejores prácticas en línea. Es esencial establecer colaboraciones tanto a nivel nacional como internacional para enfrentar de manera efectiva las amenazas cibernéticas y garantizar la protección de los ciudadanos y la infraestructura digital.

Cabe mencionar que, si bien la mayoría de las legislaciones en América tienen disposiciones legales que definen y penalizan las conductas delictivas en el ámbito cibernético, existe la necesidad de reconocer que algunas infracciones informáticas requieren una consideración más amplia y autónoma. Estas acciones no deberían ser simplemente vinculadas a figuras delictivas convencionales, especialmente cuando su impacto es significativamente mayor al perpetrarse a través de redes sociales o correos electrónicos.

El objetivo principal de este estudio es realizar un análisis de la tipificación de los ciberdelitos en la legislación ecuatoriana, así como también examinar las disposiciones legales en otras legislaciones de Sudamérica. Para lograr este propósito, se llevará a cabo un estudio jurídico, jurisprudencial y crítico que permitirá identificar las leyes pertinentes en el ámbito penal, tanto a nivel nacional como internacional. Se busca comprender cómo se interpretan y aplican estas normativas en la práctica judicial, centrándose especialmente en las penas y sanciones asociadas a los delitos cibernéticos. Este enfoque multidisciplinario proporcionará una visión completa de la situación legal y judicial en relación con los ciberdelitos en Ecuador y en la región sudamericana en general.

2. METODOLOGÍA

El enfoque de la presente investigación fue cualitativo con un diseño narrativo. Se realiza una revisión bibliográfica de leyes, libros y artículos encontrados en diferentes bases de datos científicas. El tipo de investigación propuesto abarca tres enfoques complementarios: jurídico, jurisprudencial y crítico. En primer lugar, se realizará una revisión de la legislación pertinente tanto en Ecuador como en otros países sudamericanos, con el objetivo de comprender cómo se definen y tipifican los ciberdelitos en cada contexto legal. Se realizó un análisis de los enfoques legales entre países a través del derecho comparado, destacando similitudes, diferencias y posibles áreas de mejora.

3. DESARROLLO

3.1. Ecuador

En 1999, el Ecuador vio surgir la relevancia del tema del comercio electrónico, los mensajes de datos y las firmas electrónicas a través del proyecto de Ley correspondiente. Este evento desencadenó una serie de actividades como cursos, seminarios y encuentros para discutir y profundizar en la materia.

Posteriormente, en 2002, se aprobó la versión final de la Ley de Comercio Electrónico, Mensajes de Datos y Firmas Electrónicas, lo que conllevó reformas al Código Penal para abordar lo que se conoce como delitos informáticos. Esta legislación abarca la regulación de diversos aspectos, como los mensajes de datos, la firma electrónica, los servicios de certificación, la contratación electrónica y telemática, así como la prestación de servicios electrónicos, incluyendo el comercio en línea y la protección de los usuarios de estos sistemas. En el año 2014, se introdujo un nuevo marco normativo penal en el país bajo el nombre de Código Orgánico Integral Penal (COIP), que reemplazó la legislación previa, antes contenida en la Ley de Comercio Electrónico. El COIP aborda aspectos fundamentales como los tipos penales, el procedimiento penal y el sistema penitenciario, y posteriormente se complementó con la Ley Orgánica Reformatoria del Código Orgánico Integral Penal, enfocada en combatir la corrupción.

El Código Orgánico Integral Penal (2014), como marco legal penal del país contempla una amplia gama de tipos delictivos relacionados con el ámbito digital y tecnológico. Entre ellos se incluyen delitos como la pornografía infantil, el acoso sexual por medios electrónicos, la estafa, el aprovechamiento ilícito de servicios públicos, la apropiación fraudulenta por medios electrónicos, la manipulación de información de terminales móviles, la supresión o alteración de identidad, la revelación ilegal de información en bases de datos, la interceptación ilegal de datos, el fraude informático, los daños informáticos y los delitos contra la información pública reservada, entre otros. Estos delitos abarcan penas que van desde meses de prisión hasta años, dependiendo de la gravedad y el alcance de la actividad delictiva. Además, se establecen sanciones específicas para delitos relacionados con el terrorismo, con penas significativamente más altas, reflejando la seriedad con la que se aborda este tipo de actividad ilícita.

3.2. Argentina

El análisis realizado por Schurjin (2022) sobre de la legislación argentina en materia de delitos informáticos, junto con las propuestas de actualización a través del proyecto de nuevo Código Penal, destaca especialmente las disposiciones relacionadas con los delitos informáticos contra la integridad sexual. El artículo 128 del Código Penal fue modificado en varias ocasiones, siendo la última en 2018 mediante la ley 27.436. Estas modificaciones han generado una redacción que aborda la producción, financiación, oferta, comercialización, publicación, facilitación, divulgación y distribución de imágenes de abuso sexual infantil, así como la tenencia simple y con fines de comercialización de dichas imágenes.

La versión actual del artículo establece penas que van desde 3 a 6 años de prisión para aquellos que produzcan o distribuyan imágenes de menores dedicados a actividades sexuales explícitas, o de sus partes genitales con fines predominantemente sexuales. También se contempla prisión de 4 meses a 1 año para la tenencia de estas representaciones, y de 6 meses a 2 años si la tenencia tiene fines de distribución o comercialización. Estas penas se incrementan en un tercio si la víctima es menor de 13 años.

El objetivo principal de estas disposiciones es proteger el derecho de los menores a no ser utilizados en producciones o publicaciones que puedan afectar su desarrollo psicológico y sexual. La legislación busca adaptarse a los avances tecnológicos, abordando de manera específica los delitos informáticos relacionados

con la integridad sexual y proporcionando herramientas legales para combatirlos de manera efectiva en la sociedad actual.

3.3. Brasil

Brasil cuenta con una legislación robusta que tipifica varios ciberdelitos, incluida la piratería, que se considera un delito penal según la Ley No. 737/2012. Esta legislación modificó la Disposición 154-A del Código Penal brasileño para establecer que la invasión de dispositivos informáticos de terceros, con o sin conexión a una red informática, constituye un delito cuando se realiza mediante una violación indebida de los mecanismos de seguridad con el propósito de obtener, adulterar o destruir datos. Las sanciones incluyen hasta un año de prisión y multa, o dos años de prisión y una multa si se acceden a contenidos de comunicaciones electrónicas privadas, secretos comerciales o industriales, o información confidencial. Además, existen disposiciones importantes relacionadas con los derechos civiles en la Ley de Internet de Brasil (Marco Civil da Internet) y su Decreto reglamentario No. 771/2015, así como normativas relacionadas con la protección de datos personales y la ciberseguridad, como la Resolución N ° 4.658 / 2018 del Banco Central de Brasil.

El país también ha avanzado en la protección de datos personales con la firma de la primera Ley de Protección de Datos de Brasil en 2018, que entró en vigencia en 2020. Aunque se espera la creación de una Autoridad de Protección de Datos para regular y hacer cumplir esta ley, su implementación se ha retrasado debido a vetos presidenciales y a la necesidad de una legislación adicional para formalizar su establecimiento. Sin embargo, se espera que esta Autoridad desempeñe un papel crucial en la supervisión del cumplimiento de la ley, la imposición de sanciones en caso de incumplimiento y la protección de los datos personales de los ciudadanos brasileños en el contexto digital.

3.4. Venezuela

Se puede revelar que, en cuanto a delitos informáticos, la legislación venezolana es de las más completas del continente americano. Los cibercrímenes tipificados son: Acceso indebido; sabotaje o daño a sistemas; acceso indebido o sabotaje a sistemas protegidos; posesión de equipos o prestación de servicios de sabotaje; espionaje informático; falsificación de documentos; hurto informático; fraude informático; obtención indebida de bienes o servicios; manejo fraudulento de tarjetas inteligentes o instrumentos análogos; apropiación de tarjetas inteligentes o instrumentos análogos; provisión indebida de bienes o servicios, posesión de equipo para falsificaciones; violación de la privacidad de la data o información de carácter personal; violación de la privacidad de las comunicaciones; revelación indebida de data o información de carácter personal; difusión o exhibición de material pornográfico; exhibición pornográfica de niños o adolescentes; apropiación de propiedad intelectual y oferta engañosa (Ley Especial contra los Delitos Informáticos , 2011, pág. 320).

3.5. Chile

Chile, aunque oficialmente invitado por el Consejo de Europa desde 2009, aún no ha completado el proceso de adhesión al Convenio de Budapest, según los artículos 27 y 38 del mismo. La aplicación del

derecho penal en Chile se basa en el principio de territorialidad, establecido en el artículo 5, y en los límites de extraterritorialidad definidos en el artículo 6 del Código Penal.

En este contexto, los delitos informáticos sancionados en el país están regulados por la Ley 19.223 sobre Delitos Informáticos, que aborda una amplia gama de acciones ilícitas, incluyendo la destrucción o inhabilitación de sistemas de procesamiento de información, el acceso no autorizado a información, la alteración o destrucción maliciosa de datos, la revelación maliciosa de información y los actos sexuales con menores, entre otros.

Chile cuenta con instituciones especializadas para investigar y combatir estos delitos. El Ministerio Público es responsable de investigar los delitos, incluidos los cibernéticos, y de ejercer la acción penal pública. La Policía de Investigaciones de Chile opera la Brigada Metropolitana de Investigación de Delitos Cibernéticos desde el año 2000, encargada de detectar e investigar conductas ilegales en Internet y proporcionar evidencia a los tribunales.

Además, el país cuenta con el Centro de Respuesta a Incidentes de Computación y Seguridad (CSIRT-CL), respaldado por el Ministerio del Interior y Seguridad Pública, cuya misión abarca desde brindar asistencia en ciberseguridad hasta promover la protección de infraestructuras críticas y fortalecer el marco legal relacionado con el delito cibernético.

3.6. Bolivia

Se penaliza la violación de la correspondencia electrónica privada, así como la falsificación y suplantación de identidad en línea. También se castiga la manipulación informática, incluida la alteración, acceso y uso indebido de datos informáticos, así como la falsificación de documentos privados en entornos digitales. Es importante señalar que, previo a la promulgación de esta ley, la falsedad y falsificación estaban limitadas únicamente a documentos físicos o impresos. Además, se abordan los delitos contra la propiedad intelectual de obras con soporte electrónico, en consonancia con la Ley 004 de Lucha Contra el Cibercrimen en Bolivia. Se impone sanciones a aquellos que lleven a cabo sabotaje informático, afectando el funcionamiento normal de sistemas de información o telecomunicaciones.

3.7. Colombia

El marco legal referente a delitos informáticos en Colombia, particularmente regulado por la Ley No. 1273 de 2009, abarca una amplia gama de conductas delictivas relacionadas con el uso indebido de sistemas informáticos y redes de telecomunicaciones. Este estatuto tipifica acciones como el acceso abusivo a un sistema informático, la interferencia ilícita en sistemas o redes de telecomunicaciones, la interceptación de datos informáticos, el daño informático, y el uso de software malicioso, entre otros. Es importante destacar que este artículo específicamente contempla el delito de "phishing", que consiste en la suplantación de sitios web legítimos para obtener de manera fraudulenta datos personales de los usuarios, lo cual representa una amenaza significativa para la seguridad de la información y la privacidad en línea.

Además, la ley aborda el hurto por medios informáticos y conductas similares, así como la transferencia no consentida de activos digitales. Estas disposiciones legales reflejan la importancia de

proteger tanto los sistemas de información como los datos personales de los individuos en el entorno digital. La promulgación de esta ley responde a la necesidad de actualizar el marco legal para abordar los nuevos desafíos y riesgos asociados con el uso cada vez más extendido de la tecnología en la sociedad contemporánea. Asimismo, refleja el compromiso del gobierno colombiano de combatir la ciberdelincuencia y salvaguardar la seguridad cibernética en el país, mediante la adopción de medidas legales que fortalezcan la prevención, detección y sanción de los delitos informáticos.

3.8. Perú

En los delitos contra datos y sistemas informáticos se contempla: el acceso ilícito, atentado contra la integridad de datos informáticos, y el atentado contra la integridad de sistemas informático. En los delitos informáticos contra la indemnidad y libertades sexuales se contempla: proposiciones a niños, niñas y adolescentes con fines sexuales por medios tecnológicos. En los delitos contra la intimidad y el secreto de las comunicaciones se contempla: tráfico ilegal de datos, interceptación de datos informáticos. En los delitos informáticos contra el patrimonio se contempla: fraudes informáticos. En los delitos informáticos contra la fe pública: suplantación de identidad (Ley No 30096, 2014).

3.9. Paraguay

La legislación paraguaya, en específico la Ley No. 5801 de Delitos informáticos, promulgada en 2017, contempla una serie de delitos informáticos que abarcan desde la pornografía infantil hasta la violación del secreto de la comunicación y la interferencia en sistemas informáticos. Entre estos delitos, se encuentra el grave problema de la pornografía infantil, que es sancionado de manera severa en virtud de esta ley, reflejando el compromiso del país en la protección de los derechos de los menores y en la lucha contra la explotación sexual de niños y adolescentes en el ámbito digital.

Además, la normativa aborda la violación del secreto de la comunicación y la intercepción ilícita de datos, lo que constituye una amenaza para la privacidad y la confidencialidad de la información de los ciudadanos. Estos actos delictivos, junto con la interferencia en sistemas informáticos y el fraude informático, son considerados como una violación a la seguridad y la integridad de los sistemas de información, lo que puede tener graves consecuencias tanto a nivel individual como a nivel empresarial o gubernamental. Por lo tanto, la ley tiene como objetivo prevenir y sancionar estas prácticas para garantizar un entorno digital seguro y protegido para todos los usuarios en Paraguay.

3.10. Uruguay

Uno de los países cuya legislación penal se encuentra más rezagada en materia de delitos informáticos es la uruguaya. Aunque en la actualidad cuenta con la ley No 19172 de Delitos Informáticos y con los artículos 72 y 332 de la Constitución que abordan parcialmente esta temática, el Parlamento uruguayo está debatiendo una reforma del Código del Proceso Penal para abordar de manera más completa y actualizada este ámbito.

La discusión parlamentaria se ha intensificado debido al creciente número de delitos cometidos a través de medios informáticos. La reforma propuesta contempla la inclusión de un capítulo específico sobre

delitos informáticos, dentro del cual se abordarán diversas conductas ilícitas. Entre ellas se encuentran el acceso ilícito a sistemas informáticos, la intercepción ilícita de información, los ataques a la integridad de los datos y del sistema, el uso indebido de dispositivos, software o claves de acceso, así como la falsificación y el fraude informático, regulados por la Ley No 18.331 de 2008. Esta iniciativa legislativa busca adecuar el marco legal uruguayo a los desafíos y realidades de la era digital, garantizando una protección efectiva contra los delitos informáticos y promoviendo la seguridad y confianza en el uso de las tecnologías de la información y comunicación en el país.

El análisis de la presente investigación revela una variedad de penas y sanciones establecidas por los países sudamericanos para abordar los delitos informáticos. En la tabla 1, se detallan las penas y sanciones impuestas en cada país para los ciberdelitos, así como también el cuerpo legal que lo sustenta.

Tabla 1

Penas y sanciones para los ciberdelitos en Sudamérica

País	Penas y Sanciones	Cuerpo Legal
Ecuador	Prisión: 1-3 años para delitos menores, 13-16 años para delitos graves. Multas proporcionales al daño.	Código Orgánico Integral Penal (COIP)
Argentina	Prisión: 1-5 años para delitos menores, 5-15 años para delitos graves. Multas proporcionales al daño.	Código Penal Argentino
Brasil	Prisión: 3 meses - 2 años para delitos menores, 2-10 años para delitos graves. Multas proporcionales al daño.	Ley Nº 12.737 (Ley Carolina Dieckmann), Código Penal Brasileño
Bolivia	Prisión: 1-3 años para delitos menores, 5-15 años para delitos graves. Multas proporcionales al daño.	Ley 004 de Lucha Contra el Cibercrimen en Bolivia
Chile	Prisión: 1-5 años para delitos menores, 5-20 años para delitos graves. Multas proporcionales al daño.	Ley 19.223 sobre Delitos Informáticos en Chile
Colombia	Prisión: Variable según delito. Multas económicas.	Ley 1273 - Ley de Delitos Informáticos
Paraguay	Prisión: 1-5 años para delitos menores, 5-15 años para delitos graves. Multas proporcionales al daño.	Ley N° 5801 de Delitos Informáticos en Paraguay
Perú	Penas de prisión de hasta 8 años y multas. Pueden variar dependiendo de la gravedad del delito.	Ley 30096 - Ley de Delitos Informáticos
Uruguay	Prisión: 1-4 años para delitos menores, 5-15 años para delitos graves. Multas proporcionales al daño.	Código Penal de Uruguay
Venezuela	Prisión: 1-6 años para delitos menores, 6-20 años para delitos graves. Multas proporcionales al daño.	Ley Orgánica Contra la Delincuencia Organizada y Financiamiento al Terrorismo (LOCTI) en Venezuela

4. DISCUSIÓN

Después de una revisión desde la perspectiva del derecho comparado sobre la legislación relacionada con los delitos informáticos o ciberdelitos, se destaca una marcada disparidad en los criterios legales adoptados por diferentes países, lo que dificulta la instauración de un estándar internacional. La investigación de Escobedo (2013) deja en claro las diferencias legislativas entre naciones sudamericanas como Colombia y otras partes del mundo. Cada país ha configurado su propio sistema legal, influenciado por diversas corrientes históricas, que van desde las europeas y las inglesas hasta las francesas, españolas y americanas. Esta diversidad de influencias ha resultado en enfoques dispares para abordar los delitos cibernéticos. Por ejemplo, mientras que en Colombia se observan notables diferencias en comparación con otros países, como España, donde se encuentran similitudes, especialmente en lo que respecta a la tipificación de la transferencia no consentida de activos, en otras jurisdicciones esta acción se considera simplemente como estafa, apropiación ilícita, hurto u otras acepciones similares, lo que evidencia la necesidad de una mayor armonización legal a nivel internacional.

Al revisar de manera concisa la legislación sobre delitos informáticos en Sudamérica y Europa, se resalta la importancia de diferenciar y sancionar de forma independiente las conductas cibernéticas, desvinculándolas de figuras penales tradicionales. Lara et al. (204) fundamentan esta distinción en el marco legal referente a la complejidad y especificidad de los delitos cometidos en el ámbito digital. Asimismo, se hace hincapié en la necesidad de que los Estados adopten recomendaciones concretas para prevenir la comisión de estos delitos. Entre estas recomendaciones se incluyen medidas para fortalecer la ciberseguridad, promover la educación digital y concienciar sobre los riesgos asociados con el uso de la tecnología, así como el fomento de la cooperación internacional para abordar de manera efectiva los ciberdelitos en un contexto globalizado. Este análisis subraya la importancia de una acción coordinada a nivel global para abordar los desafíos en materia de ciberseguridad y legislativos que enfrenta la comunidad internacional.

La falta de uniformidad en la tipificación de los ciberdelitos en Sudamérica representa una de las principales limitaciones que surgen de nuestro análisis. Esta disparidad se refleja en la variedad de legislaciones y enfoques adoptados por cada país para abordar este problema, lo que, a su vez, dificulta la cooperación internacional y la aplicación coherente de medidas preventivas y sanciones. Al comparar las distintas legislaciones desde una perspectiva comparativa, se observa una diversidad notable de criterios no unificados ni tipificados, lo que complica la creación de un estándar internacional. Por ejemplo, al contrastar la normativa colombiana con la de otros países, se encuentran diferencias significativas, influenciadas por el contexto histórico y las corrientes legales de Europa, Estados Unidos y otras regiones.

Para abordar esta complejidad, resulta crucial fomentar el diálogo y la colaboración entre los países sudamericanos con el fin de desarrollar normativas comunes que faciliten la cooperación internacional y la lucha efectiva contra los ciberdelitos. Esto implicaría no solo una revisión exhaustiva de las leyes existentes, sino también la implementación de mecanismos de coordinación y armonización legales que consideren las

particularidades de cada país sin comprometer la coherencia y la eficacia en la persecución de los delitos cibernéticos. López (2013) afirma que una colaboración eficaz entre organismos internacionales y la adopción de estándares y mejores prácticas reconocidos a nivel global podrían contribuir significativamente a este esfuerzo. En última instancia, la unificación de criterios legales en la región no solo fortalecería la capacidad de respuesta ante los ciberdelitos, sino que también reforzaría el compromiso de Sudamérica con la protección de la ciberseguridad y el cumplimiento de las normas internacionales.

Se sostiene firmemente que para abordar los delitos informáticos en Sudamérica y en todo el mundo, resulta fundamental establecer un marco legal armonizado que identifique y tipifique adecuadamente estas conductas cibernéticas. Además de fortalecer la ciberseguridad y promover la educación digital, es crucial que los países sudamericanos colaboren en el desarrollo de políticas y estrategias conjuntas para enfrentar eficazmente los desafíos del ciberespacio. Esto implica la formación de equipos especializados en la investigación y persecución de delitos informáticos, así como la implementación de medidas que fomenten la cooperación internacional y el intercambio de información entre las autoridades pertinentes de diferentes países. Asimismo, es necesario impulsar la concienciación pública sobre los riesgos asociados con el uso de la tecnología y promover las buenas prácticas en línea para reducir la vulnerabilidad de los usuarios frente a posibles ataques cibernéticos. En definitiva, únicamente mediante una colaboración coordinada y anticipada tanto a nivel regional como internacional será posible enfrentar de forma eficaz los crímenes informáticos y asegurar la protección de la ciberseguridad tanto en Sudamérica como en el ámbito global.

5. CONCLUSIONES

Los resultados de esta investigación revelan la diversidad de penas y sanciones adoptadas por los países sudamericanos para abordar los delitos informáticos, que van desde penas de prisión de corta duración hasta períodos de décadas, junto con multas proporcionales al daño causado. Sin embargo, destaca la falta de uniformidad en la tipificación de los ciberdelitos en la región, lo que dificulta la creación de un estándar internacional y la colaboración transfronteriza en la lucha contra estos crímenes.

La complejidad de la armonización legal en Sudamérica se enfatiza en la discusión, evidenciando las diferentes influencias jurídicas en la configuración de los marcos legales de cada país, lo que resulta en diferencias significativas en la definición y tratamiento de los delitos informáticos. Esta falta de cohesión legal plantea desafíos para la aplicación uniforme de la ley y destaca la necesidad de impulsar el diálogo y la cooperación entre los países de la región para fortalecer la ciberseguridad y garantizar la protección contra los riesgos cibernéticos.

FINANCIACIÓN

La investigación fue financiada completamente por los autores.

CONFLICTO DE INTERESES

Los Autores declaran que no existe ningún conflicto de intereses con su investigación.

CONTRIBUCIÓN DE AUTORÍA

Participar activamente en:	*Autor 1.*	*Autor 2*	*Autor 3*	*Autor 4*
Conceptualización	X			
Análisis formal		X		
Adquisición de fondos	X	X	X	X
Investigación	X		X	X
Metodología	X	X		
Administración del proyecto	X			
Recursos	X	X	X	X
Redacción –borrador original		X	X	
Redacción –revisión y edición	X	X	X	X
La discusión de los resultados	X			
Revisión y aprobación de la versión final del trabajo.	X	X	X	X

REFERENCIAS

Bolaños-Burgos, F., & Gómez-Giacoman, C. (2015). Estudio cualitativo de la relación de las leyes y la pericia informática en el Ecuador. *ReCIBE. Revista electrónica de Computación, Informática, Biomédica y Electrónica*, (3). https://www.redalyc.org/pdf/5122/512251503001.pdf

Choi, K., & Toro-Álvarez, MM (2017). *Cibercriminología: Guía para la Investigación del Cibercrimen y Mejores Prácticas en Seguridad Digital.* Bogotá: Fondo Editorial Universidad Antonio Nariño. https://vc.bridgew.edu/fac_books/171/

Código Orgánico Integral Penal [COIP]. 03 de febrero de 2014. (Ecuador) https://www.oas.org/juridico/PDFs/mesicic5_ecu_ane_con_judi_c%C3%B3d_org_int_pen.pdf

Cuello, E. (1964). *Derecho penal. Parte General.* Barcelona: Bosch.

Fernández, D., & Martínez, G. (2020). *Ciberdelitos: (ed.).* Barcelona, Ediciones Experiencia. https://elibro.net/es/ereader/uniandesecuador/167811?page=7

Holt, T. J. (2012). Exploring the intersections of technology, crime, and terror. *Terrorism and Political Violence, 24*(2), 337-354. https://doi.org/10.1080/09546553.2011.648350

Lara, J. C., Martínez i, M., & Viollier, P. (2014). Hacia una regulación de los delitos informáticos basada en la evidencia. *Revista Chilena de Derecho y Tecnología, 3*(1). https://doi.org/10.5354/0719-2584.2014.32222

López, R. (2013). *Delitos informáticos, ciberterrorismo, terrorismo y delincuencia organizada*. https://haddensecurity. wordpress.com/2013/06/17/delitos-informaticos-iberterrorismo-terrorismoy-delincuencia-organizada/amp/ 05-12-2018.

Escobedo, A. (2013), *El concepto impunidad, su abordaje en los instrumentos del Derecho Internacional de los Derechos Humanos, Derecho Internacional Humanitario y Derecho Penal Internacional*. [Tesis de Maestría, Universidad Carlos III de Madrid] https://core.ac.uk/download/pdf/29405623.pdf

Muñoz, J. J. (2019). *Derecho de daños tecnológicos, ciberseguridad e insurtech*. Midac, SL. https://books.google.es/books?id=ydOfDwAAQBAJ&lr

Pons, V. (2017). Internet, la nueva era del delito: ciberdelito, ciberterrorismo, legislación y ciberseguridad/ Internet, the new age of crime: cibercrime, ciberterrorism, legislation and cibersecurity. *URVIO - Revista Latinoamericana de Estudios de Seguridad*, (20), 80. https://doi.org/10.17141/urvio.20.2017.2563

República de Argentina. (2008). Ley 26.388 de Delitos Informáticos en Argentina. Recuperado el 17 de Abril de 2015, de: http://www.taringa.net/post/info/2087099/Ley-26-388---Delitos-Informaticosen-Arg.html

Código Orgánico Integral Penal de la Nación Argentina. 29 de octubre de 1921. (Argentina). https://servicios.infoleg.gob.ar/infolegInternet/anexos/15000-19999/16546/texact.htm

República de Bolivia (2010). Ley 004 de Lucha Contra el Cibercrimen. https://www.planificacion.gob.bo/uploads/normativa/ley_004_lucha_contra_corrupcion_enriquecimiento.pdf República de Chile. (1993). Ley 19223. Recuperado el 13 de Abril de 2015, de: http://www.leychile.cl/Navegar?idNorma=30590

República de Brasil (2012). Ley de delitos informáticos 12737/12. Recuperado el 21 de Marzo de 2015, de http://riquertdelincuenciainformatica.blogspot.com/2013/01/brasil-ley-dedelitos-informaticos.html

República de Colombia. (2009). Ley 1273. Recuperado el 11 de Mayo de 2015, de: http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

República de Chile. (2022). Ley 19223. Recuperado el 11 de Junio de 2022, de: https://www.bcn.cl/leychile/navegar?idNorma=30590

República de Paraguay. (2017). Ley 5801 de Delitos Informáticos en Paraguay. Recuperado el 10 de Mayo de 2017, de: https://silpy.congreso.gov.py/web/ley/137473

República del Perú. (2013). Ley 30096 de Delitos Informáticos en Paraguay. Recuperado el 27 de Septiembre de 2017, de: https://www2.congreso.gob.pe/sicr/cendocbib/con5_uibd.nsf/C5F98BB564E5CCCF05258316006064AB/$F

ILE/6_Ley_30096.pdf

República de Uruguay. (2014). Ley 19172. Ley de Delitos Informáticos. Recuperado el 7 de Enero de 2014, de: https://www.impo.com.uy/bases/leyes/19172-2013#:~:text=Proh%C3%ADbese%20toda%20forma%20de%20publicidad,v%C3%ADa%20p%C3%BAblica%2C%20folletos%2C%20estandartes%2C

República de Venezuela. (2011). *Ley Especial Contra los Delitos Informáticos*. http://www.oas.org/juridico/spanish/mesicic3_ven_anexo18.pdf

Salazar, D. (2021). El rol de la Administración de Justicia y la cooperación internacional en la lucha contra la ciberdelincuencia. *Perfil criminológico*, *30*, 8-15. https://www.fiscalia.gob.ec/pdf/politica-criminal/Ciberdelitos-Perfil-Criminologico.pdf

Schurjin, D. (2022). Delitos informáticos en argentina: normativa actual y posibilidades de cambio según el proyecto de nuevo código penal. *REVISTA Pensamiento Penal*, *412*. https://www.pensamientopenal.com.ar/system/files/doctrina89883.pdf

Tolinga (2021). El rol de la administración de Justicia y la cooperación internacional en la lucha contra la ciberdelincuencia. *Revista Científica de Ciencias Jurídicas, Criminología y Seguridad FISCALÍA GENERAL DEL ESTADO*. https://www.fiscalia.gob.ec/pdf/politica-criminal/Ciberdelitos-Perfil-Criminologico.pdf

Toro-Álvarez, M. M. (2023). El control del cibercrimen. Análisis exploratorio de sentencias y medidas de supervisión. *Revista Logos Ciencia & Tecnología, 15*(2), 162–173. https://doi.org/10.22335/rlct.v15i2.1768