Ciencia Latina Revista Científica Multidisciplinar, Ciudad de México, México.
ISSN 2707-2207 / ISSN 2707-2215 (en línea), noviembre-diciembre 2024,
Volumen 8, Número 6.

https://doi.org/10.37811/cl_rcm.v8i6

CRIMINOLOGÍA RELACIONADA CON LOS DELITOS CIBERNÉTICOS Y LA FALTA DE PUNIBILIDAD DE CONDUCTAS

CRIMINOLOGY RELATED TO CYBERCRIME AND THE LACK OF PUNISHABILITY OF CONDUCT

Pedro Fabian Troya Aldaz
Universidad Nacional de Mar del Plata - Ecuador

Marina Anabel Vargas Almachi
Universidad Nacional de Mar del Plata - Ecuador

Carola Jacqueline Barrera Espín
Universidad Nacional de Mar del Plata - Ecuador

Alex Rigoberto Barrera Espín
Universidad Nacional de Mar del Plata - Ecuador

DOI: https://doi.org/10.37811/cl_rcm.v8i6.14605

Criminología relacionada con los delitos cibernéticos y la falta de punibilidad de conductas

Pedro Fabian Troya Aldaz[1]
pedrotroya@hotmail.com
https://orcid.org/0009-0005-1911-1768
Universidad Nacional de Mar del Plata
Ecuador

Marina Anabel Vargas Almachi
marinaanabelvargas@gmail.com
https://orcid.org/0009-0004-8039-8422
Universidad Nacional de Mar del Plata
Ecuador

Carola Jacqueline Barrera Espín
carolabarrera2@yahoo.com
https://orcid.org/0009-0007-2141-4578
Universidad Nacional de Mar del Plata
Ecuador

Alex Rigoberto Barrera Espín
alexbarreraespin@gmail.com
https://orcid.org/0009-0003-2872-1205
Universidad Nacional de Mar del Plata
Ecuador

RESUMEN

La investigación explora la criminología de los delitos cibernéticos y la falta de punibilidad de ciertas conductas, analizando la respuesta jurídica frente a estas prácticas en un entorno digital en constante evolución. Se destaca cómo ciertas conductas quedan sin penalización debido a vacíos legales, dificultades en la detección y limitaciones en la jurisdicción y la legislación que no se adapta con la rapidez necesaria a las nuevas modalidades de delitos en línea. El principal problema de investigación se centra en responder el cuestionamiento acerca de la eficacia de la legislación para combatir el cibercrimen y cuáles son los aspectos que podrían mejorar para evitar la impunidad en la persecución y sanción de estas conductas, dado que los ciberdelitos son un nuevo paradigma que cambia por completo aspectos sustantivos, procesales e investigativos en el derecho penal. El análisis identifica las áreas donde el marco legal debe evolucionar para abordar de manera más eficaz los desafíos únicos de los delitos cibernéticos, contribuyendo así a la discusión sobre la adaptación de la legislación para mejorar la punibilidad y la prevención en el ciberespacio.

Palabras clave: ciberdelitos, criminología informática, ciberpunibilidad, delitos informáticos

[1] Autor Principal
Correspondencia: pedrotroya@hotmail.com

Criminology related to cybercrime and the lack of punishability of conduct

ABSTRACT

The research explores the criminology of cybercrime and the lack of punishability of certain conducts, analyzing the legal response to these practices in a constantly evolving digital environment. It highlights how certain conducts go unpenalized due to legal loopholes, difficulties in detection and limitations in jurisdiction and legislation that does not adapt quickly enough to new forms of online crime. The main research problem focuses on answering the question about the effectiveness of legislation to combat cybercrime and what aspects could be improved to avoid impunity in the prosecution and punishment of these conducts, given that cybercrime is a new paradigm that completely changes substantive, procedural and investigative aspects in criminal law. The analysis identifies the areas where the legal framework must evolve to more effectively address the unique challenges of cybercrime, thus contributing to the discussion on adapting legislation to improve punishability and prevention in cyberspace.

***Keywords*:** cybercrime, computer criminology, cyberpunishability, computer crimes

Artículo recibido 08 septiembre 2024

Aceptado para publicación: 10 octubre 2024

INTRODUCCIÓN

Este trabajo pretende explicar la aparición de nuevos delitos como consecuencia del uso de internet, y la necesidad del Derecho de actualizarse con los cambios que trae consigo la evolución tecnológica. En este debate se abordarán los delitos digitales en el contexto de la influencia de las tecnologías de la información en el Derecho Penal y la necesidad de adaptar el derecho a la nueva realidad tecnológica de la sociedad actual.

En este contexto, la promulgación de nuevas leyes sobre ciberdelincuencia así como las reformas a las leyes penales estatales ha sido la primera respuesta para combatir estos delitos. Sin embargo, además de la simple tipificación de nuevos delitos surgidos de la influencia de los avances tecnológicos en la sociedad actual, otras cuestiones, directamente afectadas por las particularidades propias de los ciberdelitos, merecen una discusión especial, como la producción de la prueba digital y los aspectos procesales.

La sociedad contemporánea, interconectada y global está experimentando cada vez más transformaciones tecnológicas importantes. Como resultado de este crecimiento desenfrenado de las tecnologías de la información, han surgido varias herramientas para optimizar el tiempo, desarrollar las ideas creativas y mejorar la conectividad. El más dinámico e importante de ellos, Internet, una red informática global, es capaz de conectar a usuarios de todo el mundo, una innovación que ha facilitado la conexión.

Las ventajas y beneficios que ofrece internet dieron como resultado la formación de la llamada sociedad de la información, caracterizada por la creciente importancia de la información y la vertiginosa dependencia de los recursos tecnológicos en las actividades cotidianas. Sin embargo, Internet, que surgió inicialmente como una nueva tecnología de comunicación y debía utilizarse en beneficio de la sociedad, se ha convertido en un instrumento para practicar conductas ilegales y extremadamente peligrosas, como resultado de la fácil adaptación de las personas a las innovaciones tecnológicas.

La magnificencia de la tecnología, la velocidad de acceso y la difusión de la información han añadido algunas particularidades en el tratamiento de los ciberdelitos. Este tipo de delitos se caracterizan por la rapidez con que se cometen y la novedad de su presentación al mundo jurídico, que considerados en

conjunto, requieren de conocimientos específicos para poder arribar a indicios de autoría y materialidad de la infracción.

Por lo tanto, la discusión en esta temática sobre los delitos cibernéticos resulta de gran utilidad, considerando que, con la evolución tecnológica, Internet ha demostrado ser el principal medio de comunicación y tráfico de información, transformando la vida cotidiana de la sociedad actual. Sin embargo, por ello destaca el principal problema de investigación: ¿Es eficaz la legislación para combatir el cibercrimen?

La rapidez y novedad con que se perpetúan estos delitos, así como los bienes jurídicos afectados por estos delitos son peculiaridades que dificultan la investigación penal y la producción de pruebas. La dificultad para identificar la autoría y la necesidad de producción temprana de evidencia requiere y de peritos especializados, pero sobre todo de un marco jurídico adecuado que responda a estos nuevos desafíos.

La temática fue elegida por su contemporaneidad y, más que eso, por la importancia de que se presente un escenario peligroso de violación de derechos subjetivos y objetivos en un entorno en el que parece reinar la impunidad. Esto denota no sólo la relevancia jurídica del tema, sino también su relevancia político-social, ya que, cada día miles de personas en todo el mundo son víctimas de ciberdelitos de todo tipo, superando incluso el número de delitos tradicionales.

METODOLOGÍA

En este estudio cualitativo de carácter exploratorio, se emplea un diseño fenomenológico para investigar la criminología de los delitos cibernéticos y la falta de punibilidad de ciertas conductas. La revisión documental es la técnica principal de recolección de datos, con la finalidad de analizar textos, estudios previos y normativas que permiten comprender las percepciones y realidades sobre la punibilidad en el ámbito de los delitos cibernéticos, abordando las perspectivas de diversas fuentes para profundizar en la comprensión de las causas y consecuencias de la falta de sanciones en este ámbito.

Las consideraciones éticas del estudio se centran en el proceso de recolección de datos y la fiabilidad de las fuentes de los documentos, asegurando una interpretación objetiva del fenómeno de estudio. Los criterios de inclusión y exclusión se basan en la relevancia y actualidad de los documentos, incluyendo los estudios que aborden el contexto de los delitos cibernéticos y su punibilidad. Las limitaciones

incluyen las variaciones en las normativas entre jurisdicciones. Para garantizar el rigor metodológico, se aplicarán estrategias de validación de fuentes, para lograr coherencia y profundidad en los hallazgos del estudio.

RESULTADOS Y DISCUSIÓN

Ciberespacio

Cuando se habla de delimitación espacial, se puede interpretar como barreras físicas que imponen limitaciones al comportamiento y actividades de los seres humanos, ya sean limitaciones de origen natural o limitaciones que los propios humanos construyen para mejorar o incluso dificultar su forma de vida. A lo largo de la historia de la humanidad, tales limitaciones fueron muchas veces las motivaciones para la conquista de territorios, y la protección de estos territorios influyó directamente en nuestra evolución como sociedad. El concepto de Estado permea precisamente el territorio físico sobre el cual la población establece, posee y ejerce soberanía sobre este territorio (Fernández & Martínez, 2018).

Sin embargo, según Ferro (2020), los espacios virtuales, formados por innovaciones tecnológicas y mejoras en las redes de comunicación globales, aportan nuevas perspectivas para entender las relaciones interpersonales e incluso internacionales debido a la ausencia de barreras físicas. Según Mitnick (2022), la visión tradicional de los límites se basa en las características de los límites políticos, naturales y artificiales, que generalmente se refieren a los espacios físicos o naturales en los que los humanos han actuado a lo largo de su historia, con base en factores políticos, culturales y seguridad. Así, por ejemplo, la delineación de fronteras, como los altos muros de pueblos y ciudades en la época feudal, indicaba la necesidad de que los humanos obtuvieran seguridad y control sobre lugares específicos. En aquella época, además de los muros exteriores, existía el aislamiento asociado a los castillos de los señores feudales, que estaban protegidos por gruesos muros.

A su vez, los entornos digitales, virtuales e intangibles que se utilizan debido al uso de tecnologías electrónicas se caracterizan por fronteras que se alejan de esta visión convencional. Sus límites son materialmente invisibles, dentro de los cuales se produce intensamente el flujo y la interacción de información y datos (Ortega J. , 2021)

Concepto de mundo virtual

El mundo virtual ha pasado a conocerse como ciberespacio y puede definirse como el dominio de las redes informáticas (y los usuarios detrás de ellas) en el que se almacena, comparte y comunica información en línea. Esta naturaleza transfronteriza conduce a nuevas perspectivas sobre las nociones tradicionales de poder, territorio y soberanía. Según la conceptualización de Weber, un Estado es una comunidad humana que pretende monopolizar con éxito el uso legal de la fuerza dentro de un territorio definido. De esta forma, la delimitación de fronteras es coherente con las competencias que determinados países ejercen sobre los territorios (Ortega A. , 2018)

Sin embargo, el ciberespacio es un entorno con fronteras invisibles, cuya demarcación puede verse como un desafío para los gobiernos. En este aspecto, el ciberespacio se caracteriza por influir en el comportamiento humano de múltiples maneras, estimulando cambios en la cultura y el comportamiento social al permitir flujos de información a alta velocidad, ser de naturaleza transnacional y no tener una autoridad regulatoria central (Bustamante, 2023).

Por lo tanto, se supone que, así como los dispositivos tecnológicos cambian la forma en que se vive en sociedad, también afectan las interacciones entre los actores en las relaciones internacionales. En otras palabras, el ciberespacio no puede considerarse completamente virtual e inmaterial, ya que su existencia está ligada al arraigo de servidores ubicados en el territorio físico, de modo que el control de estos servidores por parte de un determinado Estado se considera una cuestión de soberanía nacional.

Virtualización del espacio comunitario

La legitimación del ejercicio del poder por parte del Estado se da a través de la dominación territorial y el reconocimiento de su soberanía estatal. Como resultado, el ciberespacio ha sido visto por la política internacional como la quinta esfera de poder, además de otras esferas tradicionales: tierra, agua, aire y espacio. Sin embargo, no existe una gobernanza del ciberespacio y por lo tanto es responsabilidad del gobierno promulgar leyes nacionales sobre seguridad cibernética, comportándose como ven el ciberespacio, ya que no existen regulaciones que puedan guiar y/o limitar el comportamiento estatal en este espacio. De esta manera, el ciberespacio tiene la capacidad de desafiar la soberanía estatal, ya que puede poner en duda la capacidad de los estados para regular el flujo de información dentro de sus fronteras. Estos flujos de información y datos virtuales cruzan fronteras terrestres en milisegundos, lo

que dificulta mucho filtrar su contenido, lo que puede verse como un aspecto que puede alterar los sistemas políticos (Casas, 2017).

Por tanto, según Barrio (2017), lograr el control estatal del dominio cibernético sobre los dominios tradicionales es poco probable porque el ciberespacio se configura como un dominio de difusión de poder donde, además de controlar el flujo de información, es difícil, imponer barreras de entrada en el mundo en línea, lo que permite la participación activa de individuos, Estados y actores no estatales. El uso excesivo de internet por parte de la humanidad es un reflejo de esto, demostrando la dependencia digital que se ha acumulado en los últimos años.

La forma en que las personas producen, consumen, venden, se comunican, interactúan y se comportan política y profesionalmente en su vida privada está influenciada por estas tecnologías e infraestructuras. A medida que las personas participan más activamente para obtener el poder de proporcionar información, es probable que los gobiernos modifiquen su uso de la tecnología de la información para mantener el control del dominio cibernético.

Con base en esto, Barrio (2017), afirma que los gobiernos de varios países se han preocupado por la difusión y control de la información. Además, los nuevos tipos de ataques y agresiones que se pueden realizar entre actores debido al mundo cibernético muestran que, a pesar de las ventajas, la dependencia digital también trae vulnerabilidades. Actualmente, el funcionamiento de varios sectores considerados esenciales para la sociedad moderna está directamente relacionado con el sector de la Cibernética, y, por tanto, el entorno digital se ha convertido en el principal medio de relaciones financieras, sociales, académicas y funciones de los sistemas de comunicación, transporte, energía, etc.

Por lo tanto, la cibernética es responsable del funcionamiento de la infraestructura de estos sectores vitales, mismos que puede definirse como recursos vitales o centros de gravedad, cuya perturbación puede tener un impacto significativo en la seguridad nacional y el funcionamiento normal de la capacidad del país (Arreola, 2019). De esta manera, las políticas de ciberseguridad proliferan en todo el mundo y ganan notoriedad porque su aplicabilidad es cada vez más importante para mantener la armonía social.

Ciberpunibilidad

Los ciberdelitos consisten en la comisión de actividades ilícitas a través de una red informática o de internet y se clasifican según la forma en que se cometen (Aboso, 2020). Ante la ausencia de una legislación específica que aborde el tema, corresponde al sistema penal actual juzgar a quienes cometen delitos cibernéticos. Según Conal (2022), los principales delitos cibernéticos incluyen: ataques a los sistemas informáticos, piratería, pornografía infantil, calumnias, injurias, fraude, entre otros. En base a esto, más adelante se explicarán algunas nociones sobre el ciberdelito y su clasificación en delitos propios o indebidos, así como los tipos de ciberdelitos cometidos con mayor frecuencia.

Comprensión general del delito cibernético

A principios del milenio, el mundo digital, aunque extremadamente fascinante, todavía era enigmático y oscuro para el ser humano común. Con la popularización y el uso generalizado de Internet en las más variadas actividades, también resurgió una genuina preocupación por la seguridad de la información que se compartía en línea, no sólo para los gobiernos, sino para todos los que hacían uso de ella. Aunque el concepto es antiguo, el término ciberdelito sólo surgió a finales de los años 90, en una reunión del G-8 que tenía como objetivo discutir la lucha contra las prácticas ilícitas en Internet de forma punitiva y preventiva. Desde entonces, el término se utiliza para designar delitos penales cometidos en línea (Ferrer, 2023).

Sin embargo, el progresivo cambio tecnológico dificulta la lucha contra estos delitos, que están en constante alineación con las nuevas tecnologías. Así, con el uso desenfrenado e indiscriminado de internet, algunos individuos con conocimientos de informática comenzaron a dominar y utilizar esos conocimientos para robar información cifrada, como se había hecho hace mucho tiempo, para beneficio económico o incluso por mera diversión. Estos individuos se ganaron el nombre de hackers, una designación moderna para individuos que siempre han existido. El término importado del idioma inglés se utiliza para designar a programadores muy hábiles, alguien que obtiene en secreto información sobre el sistema informático de otra persona para poder mirarla, utilizarla o intercambiarla, por los más variados motivos (Punín, 2021).

De esta manera, con el desarrollo y popularización de internet, descifrar códigos e invadir sistemas dejó de ser un instrumento de guerra y pasó a ser una oportunidad de lucro ilícito o un mero pasatiempo,

convirtiendo el ciberdelito en el mal social que es hoy. Los estafadores, vieron en las transacciones comerciales a través de Internet una oportunidad para llevar a cabo sus estafas. Atraídos por la facilidad de comprar y recibir productos sin salir de casa o realizar transacciones con sus cuentas bancarias a través de una pantalla de computadora, las personas abrazaron este nuevo mercado, sin mayor preocupación por comprobar la autenticidad de los sitios en los que ingresaban sus datos, lo que les hacía presa fácil para estos delincuentes, que operan en el mundo criminal de Internet. En línea se practican todo tipo de conductas delictivas, delitos sexuales, trata, piratería, sabotaje y terrorismo (Gámez, 2024).

La digitalización de los métodos de trabajo ha provocado perturbaciones en muchos países, provocadas por una nueva ola de delitos cibernéticos, incluyendo numerosos secuestros de información de empresas en todo el mundo. Si bien las formas de cometer delitos en Internet están evolucionando, existe una larga historia de conductas informáticas dañinas. Sin embargo, la legislación en gran parte del mundo, lleva poco tiempo abordando esta cuestión de los delitos virtuales y poco a poco ha ido alcanzando a los infractores de la norma en el nivel virtual y aplicando sanciones (Giant, 2017).

La normativa ciberdigital se compone el conjunto de normas cibernéticas, que establece principios, garantías, derechos y deberes para el uso de Internet y también determina las directrices para la actuación de las entidades en relación con la materia. Además, establece sanciones por el incumplimiento de algunas de sus normas, es decir ciberinfracciones. Además, se debe componer por las leyes que tipifiquen y castiguen específicamente los tipos más graves de infracciones cometidas en línea. Sin embargo, la forma de legislar del poder judicial, en gran parte del mundo, muchas veces es insuficiente, poco eficiente y carente de celeridad, lo que contrasta con la velocidad con la que se crean nuevas conductas penales o se modifican las modalidades de delitos tradicionales (García, 2018).

Análisis de los tipos más comunes de delitos informáticos

Desde el momento en que la criminología se dio cuenta de que internet se había convertido en un nuevo foco de delincuencia, fue necesario crear teorías para definir los delitos virtuales, así como comprender por qué ocurren. Los ciberdelitos virtuales, además de las características de los delitos tradicionales, se identifican como cometidos mediante el uso de dispositivos tecnológicos. Algunos académicos utilizan otras nomenclaturas para abordarlos, como delitos virtuales, cibercrímenes o delitos informáticos. A

pesar de no existir consenso entre los estudiosos que abordan el tema y la diversidad de nomenclaturas sobre el tema, todas abarcando las diversas conductas ilícitas llevadas a cabo por algún tipo de dispositivo tecnológico, por lo que está claro que la conducta se lleva a cabo en un entorno virtual (Romeo, 2014).

Sztandarowski (2021) corrobora este concepto, cuando concluye que los delitos virtuales son actos típicos y antijurídicos cometidos a través o contra las tecnologías de la información, es decir, un acto típico y antijurídico, cometido a través de la informática en general, o contra un sistema, dispositivo informático o redes informáticas. Es importante recordar que la función del Derecho Penal consiste en detener las conductas tipificadas, imponer sanciones y proteger los bienes jurídicos. Para ello se genera una estructura normativa, creando una lógica propia. En base a esto, se propone la idea de una clasificación más precisa de los delitos informáticos, dividiendo el delito en delitos informáticos propios e impropios como se expresa a continuación.

Delitos informáticos propios

Los delitos cibernéticos propiamente dichos, o también conocidos como puros, son aquellos en los que el agente necesita absolutamente del ordenador para realizar ataques de forma remota o directa utilizando sistemas informáticos sobre todos los bienes jurídicos ya protegidos. En esta situación no sólo está involucrada la invasión y captura masiva de datos guardados, sino también la intención de alterar, insertar, manipular o destruir datos existentes en el ordenador (Martínez, 2022).

En esta línea, Poveda (2015) afirma que son aquellos en los que el bien jurídico tutelado por la ley penal es la inviolabilidad de la información o datos automatizada. Aún en este contexto. Los delitos informáticos puros o propios son aquellos que se cometen mediante computadoras y también se realizan o consumen electrónicamente. En ellos, la tecnología de la información (seguridad del sistema, propiedad de la información e integridad de los datos, máquinas y periféricos) es el objeto jurídico protegido. En otras palabras, los delitos informáticos son aquellas conductas ilícitas y culposas que tienen como objetivo un sistema informático o sus datos, vulnerando su confiabilidad, integridad y/o disponibilidad.

Se destaca también la presencia de dos figuras en esta misma situación: los hackers y los crackers. Según Posada (2017), uno de los significados del término hacker es, una persona que utiliza sus conocimientos

técnicos para obtener acceso a sistemas privados. Al analizar el significado de esta palabra, se puede concluir que es aquella persona que tiene conocimiento único sobre el tema y que no necesariamente lo utiliza con el propósito de actuar ilícitamente pues de este discernimiento se concluye que el dominio en dicho tema puede ser visto positiva y negativamente. Los crackers son personas que actúan centrándose en la ventaja ilícita. Invaden y destruyen sitios web, rompen contraseñas, desarrollan software capaz de destruir varias máquinas al mismo tiempo.

Delitos informáticos impropios

Los ciberdelitos impuros o indebidos son aquellos que se cometen utilizando un ordenador. A diferencia de los ciberdelitos puros, esta forma de delito utiliza el ordenador como mero instrumento para llevarlo a cabo. Sin embargo, los delitos que se cometen con esa ayuda ya están tipificados por la normativa penal, demostrando que el uso del ordenador no es un factor primario sino una de las diferentes formas de materializar conductas delictivas que ya están protegidas (Martínez & Fernández, 2020).

De esta manera, Mirashi (2023) afirma que los ciberdelitos impuros o inapropiados son aquellos en los que el agente utiliza la computadora como medio para producir un resultado naturalista, que ofende el mundo físico o el espacio real, amenazando o dañando otros bienes, tecnologías de la información no computacionales u otros tipos. En el caso de internet, la posibilidad del anonimato fomenta el incumplimiento de las normas, ya que genera mayor certeza de impunidad. Por tanto, los delitos impropios son conductas habituales –típicas, antijurídicas y culposas– que se perpetran utilizando como herramienta mecanismos informáticos, pero que podrían haberse realizado por otros medios.

Eficacia de la legislación para combatir el delito cibernético

Los avances tecnológicos y los nuevos descubrimientos científicos han propiciado el surgimiento de una nueva realidad para la humanidad. El ciberespacio, un nuevo entorno social en el que la práctica de conductas y hechos jurídicos existe independientemente del espacio y la presencia física, es el motor que permite el surgimiento de esta nueva realidad. El desarrollo de la tecnología, además de permitir el manejo y procesamiento automatizado de la información y las telecomunicaciones en diferentes ámbitos de la vida, también ha hecho que la práctica de los delitos informáticos sea más diversa y peligrosa. En palabras de Toro (2023), la evolución tecnológica de la sociedad presupone la evolución de conductas ilícitas, tanto a nivel de medios como de objetos.

El cibercrimen se caracteriza cada vez más por la variedad y peligrosidad que presenta, generando mayores dificultades para investigar y probar estos delitos, así como para elaborar peritajes y establecer autorías, entre otras cuestiones. Existe aún hoy en el mundo, dificultades por procesar las escenas del crimen digital, realizar procesos de verificación informática de la autenticidad de las pruebas digitales, así como del juez para valorarla adecuadamente.

Cuando un usuario navega por Internet, se le asigna un número de IP - el Protocolo de Internet es un número que permite identificar al usuario en la red, o investigar cualquier delito que haya ocurrido, el problema es que este número solo se asigna al usuario en el momento de la conexión, pasado el tiempo, al apagar el módem, la dirección IP será asignada a otro usuario si no ha seleccionado una IP fija, siendo estos datos imprescindibles, considerando que sin ellos es imposible romper la confidencialidad de los datos y obtener una identidad o al menos una dirección real de donde se cometió el delito (Medina, 2018).

El uso cada vez mayor de computadoras e Internet para cometer delitos ha llevado a la necesidad de investigar los delitos cometidos en redes informáticas globales. Así surgió la informática forense, cuyo objetivo es investigar y recolectar evidencia de actos ilícitos cometidos a través de computadoras. Toda investigación comienza con las pruebas y la información recopiladas, y el entorno virtual es indistinguible del entorno físico. En el caso del ciberdelito, las pruebas se pueden obtener desde cualquier dispositivo electrónico (celular, disco duro) (Kiser, 2021).

En otras palabras, la evidencia digital puede definirse como toda la información obtenida en un formato comprensible para los humanos a partir de compilaciones o repositorios electrónicos, con o sin intervención humana (Martínez, 2022). En las investigaciones de delitos digitales, debido a la volatilidad y falsificación de los datos, las pruebas electrónicas deben someterse a un riguroso examen técnico antes de ser aceptadas en el proceso para garantizar la validez e integridad de los resultados. Este es el objetivo de la informática forense: demostrar lo más claramente posible lo ocurrido.

La informática forense es una ciencia encargada de dilucidar hechos, recolectar, verificar y evaluar evidencia digital a través de métodos científicos, para que los infractores sean castigados. El objetivo de la informática forense es extraer la mayor cantidad de información posible al analizar rastros relacionados con un delito, lo que lleva a conclusiones (Punín, 2021). En otras palabras, la informática

forense es una especialidad que se caracteriza por el examen científico y sistemático de las computadoras, a través de la recolección de evidencia digital, buscando sacar conclusiones sobre los casos de investigación. Los eventos descubiertos se reconstruyen, lo que permite determinar si la computadora analizada se utilizó para realizar actos ilegales o no autorizados.

Debido a que se desarrollan y perfeccionan en un entorno virtual caracterizado por la ausencia física del sujeto activo, los delitos virtuales a menudo se consideran delitos bastante complejos, ya que el delincuente existe enteramente en un ciberespacio. A esta complejidad se suma la facilidad con la que las pruebas (fotos, vídeos, archivos digitales, datos) proporcionadas para tales delitos pueden desaparecer. En otras palabras, qué fácil es modificar, perder o incluso eliminar dichas pruebas.

Los delitos digitales son difíciles de probar. Por un lado, está la comodidad de cometer delitos utilizando ordenadores; por otro, comprobar los vestigios requiere habilidades técnicas específicas, que no están disponibles en todas las escenas del crimen. La fragilidad del carácter modificado de los documentos digitales exige el nombramiento de expertos técnicamente cualificados para confirmar la autenticidad de los documentos (Mirashi, 2023).

Aunque la informática forense es muy precisa, la recopilación de pruebas se vuelve frágil. Si se hace incorrectamente, en violación de las disposiciones del derecho sustantivo o de los principios constitucionales, puede hacer que la prueba sea ilegal o inválida. La producción de pruebas ilícitas puede ser extremadamente perjudicial para el proceso, ya que dichas pruebas contaminan todas las pruebas producidas. Así, toda prueba ilícita debe ser retirada del proceso, entendiéndose por prueba ilícita la obtenida en violación de la ley, de las normas constitucionales o legales.

Debido al rigor que requiere este tipo de pericias, el mayor problema jurídico en la obtención de pruebas en delitos virtuales es la insuficiente preparación de la policía de investigaciones y de los peritos forenses. Pocos profesionales están preparados para este tipo de investigaciones y, como tales, deben estar altamente calificados para manejar la evidencia en investigaciones de delitos digitales y cumplir con los requisitos técnicos de recolección y custodia para evitar cuestionamientos de identidad y legalidad de la obtención de pruebas. Las investigaciones penales y la orientación procesal requieren de procedimientos técnicos para legitimar las pruebas generadas en delitos virtuales. Profesionales especializados en hardware, software, tráfico y seguridad de redes se someterán a peritajes para revelar

la verdad. La eficacia de las investigaciones criminales dependerá del desempeño de estos expertos en el análisis del entorno criminal y la verificación de la autenticidad (Bustamante, 2023).

Al analizar el entorno en el que se produjo el delito, los profesionales podrán comprobar si existen rastros de actividad delictiva. Ante la necesidad de especialización de los profesionales encargados de investigar los delitos digitales, es necesaria la creación de un departamento especializado en tecnologías de la información y medios de comunicación, lo que podría ser una de las formas de solucionar algunos de los problemas relacionados con los delitos cibernéticos. Debido a la rapidez y novedad con que ocurren los delitos contra bienes jurídicos especiales (información), se genera conocimiento específico para obtener evidencia de la autoría y significado de los tipos penales (Ferro, 2020).

Los departamentos de policía deben tener unidades destinadas a la investigación de delitos cibernéticos, mediante la capacitación de profesionales encargados de investigar dichos delitos y prevenir las actividades ilegales que ocurren todos los días en las redes informáticas globales. En una era de la vida cotidiana que incluye delitos, es sumamente importante el papel de los especialistas en informática, responsables de desentrañar y resolver delitos que requieren conocimientos específicos.

Orden jurídico nacional sobre el tema y la insuficiencia de normas específicas

Respecto al ordenamiento jurídico y las leyes específicas para tratar de frenar el crecimiento de esta modalidad criminal, en los últimos años el tema ha sido debatido varias veces, sin embargo, a pesar de varias leyes para tratar de resolver los problemas que ocurren relacionados con los delitos cibernéticos, todavía quedan varios vacíos por llenar.

Los delitos cometidos en el ciberespacio afectan a todos, ya sean empresas, personas y Estados. Se puede observar que, en algunos casos, la legislación vigente del Estado abarca algunas situaciones que ocurren en el entorno virtual, y entonces se aplica la analogía. Sin embargo, existe un crecimiento desmedido de las actividades criminales, lo que hace cada vez más necesaria una legislación más específica. Los avances tecnológicos crean la necesidad de implementar cambios todo el tiempo en relación a estas normas (Aboso, 2020)

Aunque la legislación no puede seguir el ritmo de los cambios que se producen, es necesario crear un punto de equilibrio en la puntividad penal y la indeterminación, con la finalidad de que las descripción de una conducta pueda sancionar de manera efectiva varias infracciones informáticas, de modo que se

pueda simplificar y acelerar el procesamiento de estas conductas, averiguar qué sucedió realmente y facilitar la investigación probatoria para sancionar a los responsables (Gámez, 2024). En el entorno cibernético, identificar quién realmente cometió el delito es la mayor dificultad durante las investigaciones, debido a la falta de un agente físico. El principal problema relacionado con los delitos virtuales se debe al anonimato, ya que en este entorno te permite crear o transformar tu identidad.

Proceso y sentencia

En cuanto a la parte procesal y sentencia de los delitos cibernéticos, existe una gran complejidad en la resolución de las demandas, pues son muchos los aspectos que deben tomarse en consideración a la hora de verificar qué competencia se debe aplicar, como la dirección electrónica, el lugar donde la conducta se realizó o tuvo efectos, el domicilio de la víctima, el domicilio del imputado. Ante esto, la legislación que regulan la competencia para perseguir y juzgar los delitos cometidos en el ciberespacio debe establecer que el delito se considera cometido en el lugar donde ocurrió la acción u omisión, en todo o en parte, así como donde ocurrió o debió ocurrir el resultado. Así, el ordenamiento jurídico se adapta a la teoría de la ubicuidad, independientemente de que hayan ocurrido o no en territorio nacional, esto sin perjuicio de las convenciones, tratados y normas de derecho internacional, a los que se haya suscrito el Estado.

Posibles soluciones y optimización

Los ciberdelitos ocurren muy rápidamente, tan rápido como la transmisión de datos. Para mejorar este escenario se necesita mayor celeridad en la emisión y cumplimiento de los mandatos, celeridad por parte de los expertos; unión entre fuerzas de seguridad pública y los actores privados, así como mejorar la legislación. Otro método que se puede utilizar es el uso de programas que puedan mejorar los mecanismos de lucha contra el cibercrimen, como la Inteligencia Artificial IA y el *Machine Learning*, algunos de estos mecanismos ya se utilizan en el entorno bancario para simplificar las tareas cotidianas (Bustamante, 2023).

Sin embargo, no basta simplemente con programar estas nuevas tecnologías, se deben elegir servicios de calidad, con una seguridad muy fuerte, efectiva y bien alineada con las necesidades de la entidad que se utilizará, es decir, se requiere trabajar en la prevención del delito. Con estos mecanismos se pude obtener muchos beneficios que pueden ir desde optimizar la identificación de amenazas hasta una mayor

agilidad en la investigación de alertas y la corrección de amenazas, dirigiendo los esfuerzos de los equipos de prevención y facilitando la correlación de datos, además de aplicar las sanciones correspondientes.

CONCLUSIONES

Según la investigación, está claro que la dificultad de legislar en un espacio virtual se verifica fácilmente. En consecuencia, resulta difícil sancionar el delito cibernético, lo que resulta una tarea agotadora y difícil, dadas las complejas limitaciones de su territorio, la propensión al anonimato, la falta de conocimiento y formación de las autoridades investigadoras, el gran número de personas capaces de utilizar la tecnología para estos usos, lo que facilita enormemente la comisión de delitos virtuales, además de dificultar el contacto con los responsables y sancionarlos.

Luego de realizar investigaciones sobre el tema, se concluyó que es necesario el ordenamiento jurídico estatal pueda tipificar de manera inmediata los delitos cometidos a través de Internet, ya que para combatir los delitos en entornos virtuales sólo se aplica el derecho penal, y casi siempre los agentes que cometen dichos delitos quedan impunes. Por lo tanto, visto lo anterior, queda claro que estos delitos virtuales deben ser regulados para que los delitos en el entorno virtual no queden impunes y causen daño a la sociedad. Hay que recordar que el derecho debe acompañar los cambios y transformaciones de la sociedad, adaptarse a la sociedad de la información y al mundo virtual, velar por la seguridad y garantizar la protección jurídica de los derechos humanos fundamentales. Además, se debe resaltar que, con el apoyo de las computadoras, el cibercrimen no sólo conduce al surgimiento de nuevos actos ilícitos, sino que también permite la violación de intereses legítimos que antes no se veían afectados por delitos ya regulados.

Las especificidades en la incidencia de los delitos cibernéticos, como el dinamismo con el que se cometen, están estrechamente relacionados con la investigación de las pruebas. Así, ante la falta de tecnología y de una fuerza laboral humana preparada, surge la importancia de la especialización de los profesionales que se dedican a estas investigaciones. Además, es importante mejorar el procesamiento de la evidencia y escenas del crimen, dada la enorme volatilidad de estos elementos en el espacio cibernético.

REFERENCIAS BIBLIOGRÁFICAS

Aboso, G. (2020). *Ciberdelitos. Análisis doctrinario y jurisprudencial.* Madrid: El Dial.

Arreola, A. (2019). *Ciberseguridad ¿Por qué es importante para todos?* Ciudad de México: Siglo XXI Editores México.

Barrio, M. (2017). *Ciberdelitos: amenazas criminales del ciberespacio. Adaptado reforma Código Penal 2015.* Madrid: Reus.

Bustamante, M. (2023). *Cibercriminalidad e investigación penal tecnológica.* Buenos Aires: Palestra Editores.

Casas, E. (2017). *En las sombras de Internet: el cibermiedo y la persecución de los delitos tecnológicos.* Madrid: La esfera de los libros, S.L.

Conal, I. (2022). *Ciberseguridad y Derecho penal.* Madrid: Civitas.

Fernández, D., & Martínez, G. (2018). *Ciberseguridad, ciberespacio y ciberdelincuencia.* Madrid: Thomson Reuters Aranzadi.

Ferrer, E. (2023). *Estudios de cibercrimen.* Santiago: Ediciones Olejnik.

Ferro, J. (2020). *Seguridad informática: aspectos generales y especiales. Introducción a la ciberdelincuencia.* Madrid: Ferro Veiga Ediciones.

Gámez Bustamante, V. (2024). *Victimología cibernética.* San Pablo: Editora Dialética.

García, S. (2018). *Ciberdelincuencia y crimen digital global.* León: Universidad de León.

Giant, N. (2017). *Ciberseguridad para la i-generación.* Madrid: Narcea Ediciones.

Kiser, Q. (2021). *Redes de ordenadores y ciberseguridad: Una guía sobre los sistemas de comunicación, las conexiones a Internet, la seguridad de las redes, protección contra el hackeo y las amenazas de ciberseguridad.* Nueva York: Independently Published.

Martínez, G. (2022). *Ciberdelitos. Instrucción y prueba.* Barcelona: Ediciones Experiencia.

Martínez, G., & Fernández, D. (2020). *Ciberdelitos.* Madrid: Ediciones Experiencia.

Medina, M. (2018). *El Ciberconflicto: nuevos desafíos para el derecho internacional humanitario.* Bogotá: Universidad Externado de Colombia.

Mirashi, E. (2023). *Tratamiento procesal del cibercrimen y diligencias de investigación tecnológica. Casuística y problemática.* Madrid: Arazandi.

Mitnick, S. (2022). *Una guía de seguridad cibernética. Seguridad en Internet y protección para niños, adolescentes, padres y profesionales.* Londres: Babelcube Incorporated.

Ortega, A. (2018). *Convivencia y ciberconvivencia. Un modelo educativo para la prevención del acoso y el ciberacoso escolar.* Madrid: Antonio Machado Libros.

Ortega, J. (2021). *Ciberseguridad. Manual práctico.* Madrid: Ediciones Paraninfo, S.A.

Posada, R. (2017). *Los cibercrimenes: un nuevo paradigma de criminalidad. Un estudio del Título vii bis del Código Penal colombiano.* Bogotá: Universidad de los Andes.

Poveda, M. (2015). *Delitos en la red: cibercrimen, ciberdelitos, ciberseguridad, ciberespionaje y ciberterrorismo.* Madrid: Fragua.

Punín, P. (2021). Breve aproximación a la ciberdelincuencia desde una perspectiva criminológica. *Revista Ruptura de la Asociación Escuela de Derecho PUCE, 1*(40), 191-230.

Romeo, C. (2014). *De los delitos informáticos al cibercrimen.* Salamanca: Ediciones Universidad de Salamanca.

Sztandarowski, L. (2021). *La verdadera cibercriminalidad. Manual jurídico del cibercrímen, ensayo de cibercriminología.* Barcelona: Cyberdéfenseur.

Toro, M. (2023). El control del cibercrimen. Análisis exploratorio de sentencias y medidas de supervisión. *Revista Logos Ciencia & Tecnología, 15*(2), 162-173.