REVISTA OFICIAL DEL PODER JUDICIAL
Vol. 17, n.º 23, enero-junio, 2025, 205-248
ISSN: 2663-9130 (En línea)
DOI: https://doi.org/10.35292/ropj.v17i23.906

Cibercriminalidad: retos y desafíos para la administración de justicia peruana

Cybercrime: challenges and difficulties for the administration of justice in Peru

Crime cibernético: desafios para a administração da justiça peruana

FÉLIX ANDRÉS ALCALÁ MOLINA
Universidad Nacional Mayor de San Marcos
(Lima, Perú)
Contacto: felix.alcala@unmsm.edu.pe
https://orcid.org/0000-0001-9549-9462

RESUMEN

Los avances significativos de la informática, las telecomunicaciones y el internet han impulsado el progreso social, económico, político y han dado lugar a un cambio de paradigma: del delito común al ciberdelito, la delincuencia informática se ha expandido globalmente, lo que ha generado nuevas formas de conductas ilícitas y actividades delictivas en línea. Este fenómeno se ha expandido a nivel mundial causando acciones punibles en el ciberespacio, las cuales se cometen a través de redes sociales, medios informáticos, entornos digitales, dispositivos móviles y/o tecnológicos; ello ha llevado a los legisladores a reestructurar y adoptar herramientas normativas para prevenir este delito. El ciberespacio carece de fronteras y regulaciones legales, lo que otorga ventaja al ciberdelincuente

debido a la alta complejidad, el anonimato, la falta de prueba y la legislación procesal en materia de prueba electrónica. En la actualidad, la labor del representante del Ministerio Público se ve enfrentada a múltiples desafíos y retos en el sistema de justicia, lo que dificulta la investigación, la persecución penal y la formulación de la acusación en el sistema de justicia. Asimismo, los órganos jurisdiccionales cumplen un rol fundamental: los Juzgados de Investigación Preparatoria desempeñan un papel clave en el control de la legalidad, los Juzgados Penales se encargan de conducir el juicio oral; finalmente, las Salas Superiores evalúan posibles vicios procesales y deciden sobre la modificación, la revocación o la confirmación de las sentencias de primera instancia. Los delitos informáticos representan un reto creciente debido a diversos factores, como la constante evolución de la tecnología, el uso de tácticas avanzadas, incluyendo el uso de la inteligencia artificial y *deepfakes*; la ciberdelincuencia posee una gran capacidad para aprovechar la transformación digital con el fin de realizar ciberataques contra redes y sistemas informáticos. El presente estudio tiene como objetivo analizar los retos y los desafíos para la administración de justicia peruana en materia de esta clase de delitos.

Palabras clave: actividades criminales por computadora; ciberdelincuentes; ciberespacio; delito informático; tecnologías de la información y la comunicación.

ABSTRACT

Significant advances in computing, telecommunications, and the internet have driven social, economic, and political progress, leading to a paradigm shift: from common crime to cybercrime. Cybercriminal activity has expanded globally, giving rise to new forms of illicit conduct and criminal activity online. This phenomenon has spread worldwide, resulting in punishable actions in cyberspace, committed through social networks, digital media, online environments, and mobile or technological devices. Consequently, legislators have had to restructure and adopt regulatory tools to prevent such crimes. Cyberspace lacks

borders and legal regulations, which gives cybercriminals an advantage due to high complexity, anonymity, lack of evidence, and procedural legislation regarding electronic evidence. Currently, the role of the Public Prosecutor faces numerous challenges in the justice system, making investigation, criminal prosecution, and the formulation of accusations more difficult. Likewise, judicial bodies play a fundamental role: the Preliminary Investigation Courts are key in controlling legality; Criminal Courts conduct oral trials; and the Superior Courts assess procedural flaws and decide whether to modify, revoke, or uphold first-instance rulings. Cybercrime represents a growing challenge due to various factors, such as the constant evolution of technology and the use of advanced tactics, including artificial intelligence and deepfakes. Cybercriminals possess great capacity to exploit digital transformation to launch cyberattacks against networks and information systems. This study aims to analyze the challenges and difficulties faced by the Peruvian justice system in addressing this type of crime.

Key words: computer-based criminal activities; cybercriminals; cyberspace; cybercrime; information and communication technologies.

RESUMO

Avanços significativos em tecnologia da informação, telecomunicações e Internet impulsionaram o progresso social, econômico e político e levaram a uma mudança de paradigma: do crime comum ao cibercrime, a criminalidade informática se expandiu globalmente, gerando novas formas de conduta ilegal e atividades criminosas on-line. Esse fenômeno se espalhou pelo mundo, causando ações puníveis no ciberespaço, que são cometidas por meio de redes sociais, meios informáticos, ambientes digitais, dispositivos móveis e/ou tecnológicos; isso levou os legisladores a se reestruturarem e adotarem ferramentas regulatórias para evitar esse crime. O ciberespaço carece de fronteiras e regulamentações legais, dando aos cibercriminosos uma vantagem devido à alta complexidade, anonimato, falta de provas e legislação processual sobre evidências eletrônicas. Atualmente, o trabalho do representante do Ministério

Público enfrenta múltiplos desafios no sistema judicial, dificultando a investigação, o julgamento e a formulação de acusações no sistema judicial. Além disso, os tribunais desempenham um papel fundamental: as Varas de Instrução Criminal desempenham um papel fundamental no controle da legalidade, as Varas Criminais são responsáveis pela condução do processo oral; finalmente, as Câmaras Superiores avaliam possíveis defeitos processuais e decidem sobre a modificação, revogação ou confirmação de sentenças de primeira instância. Os crimes informáticos representam um desafio crescente devido a vários fatores, como a constante evolução da tecnologia, o uso de táticas avançadas, incluindo o uso de inteligência artificial e *deepfakes*; o cibercrime tem uma grande capacidade de aproveitar a transformação digital para realizar ataques cibernéticos contra redes e sistemas informáticos. O objetivo deste estudo é analisar os desafios para a administração da justiça peruana na área desse tipo de crimes.

Palavras-chave: atividades criminosas por computador; cibercriminosos; ciberespaço; crime informático; tecnologias da informação e comunicação.

Recibido: 31/12/2023 **Revisado:** 22/8/2024
Aceptado: 12/6/2025 **Publicado en línea:** 15/7/2025

1. INTRODUCCIÓN

La evolución del conocimiento humano y el avance de las tendencias en tecnología implicó un cambio en la vida social, cultural y económica del hombre. Ello aunado al origen del internet y las telecomunicaciones involucró nuevos paradigmas a nivel internacional y nacional que revolucionaron el modo y la forma de vida en sociedad. Esto dio origen a ilícitos que se cometen a través de medios tecnológicos, y como consecuencia de las diferentes modalidades de delitos informáticos que afectan a los derechos fundamentales de la sociedad, el Poder Legislativo

tuvo que adecuar las instituciones jurídicas del derecho peruano con la finalidad de describir y regular las conductas ilícitas materializadas a través de leyes que permitan subsumirlas en un tipo penal y a futuro ser sancionadas. En efecto, estos nuevos paradigmas abordan el estudio de nuevos tipos penales que son fenómenos generados por la informática, capaces de ocasionar problemas debido a la complejidad del delito, la falta de tipificación en diferentes países, la transnacionalidad del delito, la falta de consenso entre países, el anonimato, la falta de pruebas, la falta de conocimiento por los operadores de justicia, entre otros que representan ciertas dificultades al derecho penal peruano y la administración de justicia.

Somos testigos de que a lo largo de la historia del Perú han existido reformas en la legislación penal peruana, y está vigente el Código Penal de 1991; sin embargo, el impacto de las tecnologías de la información y la comunicación (en adelante TIC) cambió la concepción tradicional del delito común al delito informático, y dio lugar a nuevas figuras ilícitas inexistentes para la sociedad, los operadores de justicia, los legisladores y para dicho código. Bajo este precepto nos encontramos ante una nueva realidad, donde no existe un mundo real, sino uno digital, que mantiene sus propias reglas, donde no existe legalidad, tampoco principios jurídicos del derecho. Frente a esta situación nuestro ordenamiento jurídico se adecuó a las necesidades y a la realidad social y a lo largo de estos años ha incorporado modificaciones al Código Penal peruano de 1991, con la publicación de la Ley n.º 27309, que añadió delitos informáticos al Código Penal; se advierte que dicha norma incorporó dos tipos penales en su artículo 207-A: intrusismo; en el artículo 207-B: sabotaje; y en el artículo 207-C las agravantes.

La Ley n.º 27309 surge como respuesta a los desafíos suscitados en la época y a la creciente necesidad de adaptar el ordenamiento jurídico a la era digital, su finalidad era incluir de manera específica los delitos informáticos en el Código Penal, lo que en su momento representó un avance significativo para la sociedad. Posteriormente, mediante la Ley n.º 30076, que incorpora en el art. 207-D el tráfico ilegal de datos, se situó en un marco normativo orientado a adaptar el ordenamiento

jurídico a la era digital; en este contexto de manejo y comercialización de la información, dicho artículo tenía como objetivo proteger la esfera privada y los derechos fundamentales de la persona, e instauró sanciones para quienes realicen actividades ilícitas con las bases de datos que contengan información.

Los cambios en la globalización han facilitado la comisión de acciones ilícitas por el hombre al establecer nuevas modalidades de delitos informáticos y subtipos, creando un nuevo tipo penal. Acorde a las necesidades de regular delitos contra datos y sistemas informáticos, delitos contra la indemnidad y la libertad sexual de menores, delitos contra la intimidad y el secreto de las comunicaciones, delitos contra el patrimonio, delitos contra la fe pública, el Estado peruano tuvo que innovar introduciendo y estableciendo nuevas figuras específicas mediante la Ley n.º 30096, que deroga los artículos de la Ley n.º 30076, en respuesta a la necesidad de actualizar el marco legal ante la evolución de la tecnología y el creciente aumento de la ciberdelincuencia en el Perú. La normativa anterior presentaba ciertas deficiencias, vacíos legales, así como limitaciones para tipificar y sancionar conductas ilícitas, lo que motivó la incorporación de un marco normativo conforme a la realidad, es decir, buscar la claridad y la precisión en la tipificación de delitos informáticos.

A fin de fortalecer el marco normativo frente a los desafíos que impone la era digital y la diversificación de las conductas delictivas, se hace imprescindible contar con una norma que contemple nuevos escenarios, diferentes modalidades y tipologías delictivas. En ese contexto, la Ley n.º 30096 se formuló en circunstancias en las que el uso de las TIC aún se encontraba en una fase incipiente; en la actualidad, resulta insuficiente para abordar la complejidad y la dinamización de los delitos cibernéticos. Con el avance de la tecnología y la transformación de las conductas delictivas era necesario adoptar mecanismos más precisos, así, se deroga la anterior ley a favor de la Ley n.º 30171.

La creciente digitalización, el avance acelerado y el apogeo de las nuevas tendencias en tecnología impone retos y desafíos a la administración de justicia, además, la diversidad de modalidades y tipologías

de ciberdelitos ha generado un aumento en la comisión de conductas delictivas a través de medios informáticos. En respuesta a esta realidad, la Ley n.º 30171 se implementó para actualizar el marco normativo con la finalidad de combatir los ciberdelitos, al no solo sancionar las conductas ilícitas, sino también establecer mecanismos de investigación y cooperación internacional. Adicionalmente, con el paso de los años han surgido nuevos fenómenos delictivos en el ciberespacio, como el ciberterrorismo, el ciberataque y el ciberespionaje.

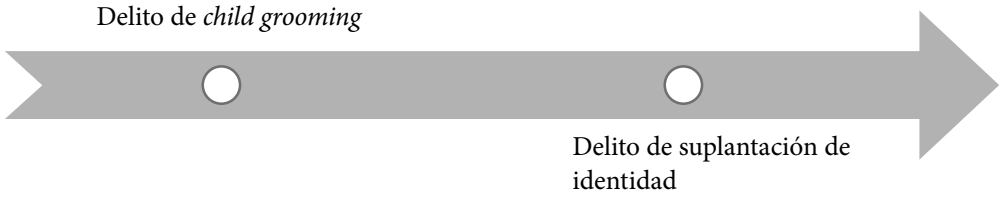
En un contexto de creciente preocupación por los casos de *grooming* en el Perú, los legisladores han reformado el Código Penal y el Código de Ejecución Penal con el objetivo de fortalecer la prevención y la sanción de los delitos contra la libertad y la indemnidad sexual. Ciertos alcances se regulaban en la Ley n.º 30838, que buscaba proteger a niños(as) y adolescentes frente a los delitos que vulneran su libertad e indemnidad sexual, con especial énfasis en aquellos relacionados con el *child grooming*. En particular, el artículo 5 de la norma establece medidas específicas para afrontar las nuevas modalidades y tipologías de agresión sexual en el entorno digital; la norma persigue sancionar de manera rigurosa a los agresores que hacen uso del internet u otros medios análogos y establecen contacto con menores de catorce y dieciocho años de edad, con el fin de solicitar u obtener material pornográfico o la realización de actos sexuales. Desde esta perspectiva la norma se configura como un mecanismo de prevención y protección de la libertad y la indemnidad sexual en el entorno digital.

De acuerdo con el Decreto Legislativo n.º 1591, el Congreso de la República del Perú ha delegado al Poder Ejecutivo la facultad de legislar aspectos específicos de la Ley n.º 30076, a fin de responder a la creciente ola de delincuencia informática y proteger a los menores frente a conductas delictivas que son cometidas en entornos digitales. Este marco legislativo se focaliza en los siguientes aspectos:

1.1. Modificación de disposiciones legales

Figura 1

Precisión en la modificación de la Ley n.º 30096



Fuente: adaptado del Decreto Legislativo n.º 1591, del Congreso de la República del Perú.

1.1.1. Delito de *child grooming*

El Decreto Legislativo n.º 1591, art. 5, introduce modificaciones en la tipificación y la sanción de conductas delictivas dirigidas a menores, establece penas diferenciadas según la edad de la víctima y refleja la necesidad de brindar protección a niños(as) y adolescentes frente al entorno digital.

Para Giménez García (2006), el entorno digital se destaca como eje central de las plataformas digitales, herramientas y espacios virtuales, al permitir a la generación actual procesar información, comunicarse, almacenar datos y gestionar contenido a través de dispositivos electrónicos e internet.

En el ámbito de la investigación del *child grooming*, el entorno digital presenta desafíos en la obtención y la preservación de prueba, tales como la volatilidad de la información y la transnacionalidad del delito (Temperini, 2018). Cabe señalar que la lucha para combatir los delitos contra la libertad y la indemnidad sexual requiere una articulación entre diversas instituciones, Ministerio Público, Poder Judicial, Ministerio de la Mujer y Poblaciones Vulnerables, División de Investigación de Delitos de Alta Tecnología (en adelante Divindat), es por ello que la ausencia de protocolos de actuación conjunta y la falta de capacitación en delitos de *grooming* constituyen obstáculos.

1.1.2. Delito de suplantación de identidad

La inteligencia artificial (en adelante IA) ha traído consigo grandes avances, pero a la vez desafíos, especialmente en delitos de suplantación de identidad. Para Moreno *et al*. (2022) este es uno de los principales problemas a nivel mundial y resulta aún más preocupante en un mundo cada vez más conectado.

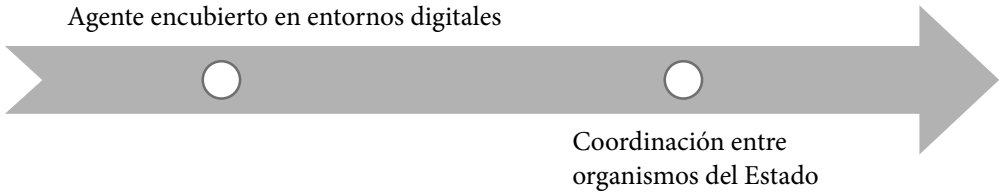
Con el avance de la IA esta práctica se ha perfeccionado mediante el uso de herramientas tecnológicas avanzadas, como los *deepfakes*, que permiten la creación de videos y audios capaces de replicar la apariencia y la voz de una persona; *chatbots*, diseñados para simular conversaciones de una persona; y el *phishing*, que emplea mensajes generados por la IA con la finalidad de suplantar la identidad de terceros.

Bajo estas circunstancias, el delito en mención se encuentra tipificado mediante el Decreto Legislativo n.º 1591, art. 9, que establece penas agravadas para quien suplante la identidad de un menor de dieciocho años de edad. Esta modificación responde a la vulnerabilidad en el entorno digital, donde la suplantación de identidad genera daños de índole moral y psicológica. El crecimiento exponencial de las TIC ha facilitado la difusión mundial de este tipo de delito en sus diferentes modalidades, lo cual ha tenido impacto en la seguridad de los ciudadanos. No cabe duda de que la tipificación penal establece sanciones en función del perjuicio causado a menores de dieciocho años, no obstante, resulta insuficiente al no detallar de forma específica las modalidades sofisticadas de esta nueva clase de delitos, tales como *deepfakes*, *chatbots* y *phishing* avanzado. La evolución tecnológica demanda que las leyes se adapten a la evolución del entorno digital con la finalidad de reconocer y tipificar de modo claro las conductas ilícitas, es importante la incorporación de mecanismos de la prueba electrónica que respondan a la complejidad del delito, así como el desarrollo de criterios doctrinales y técnicos que orienten la interpretación de la norma.

1.2. Actos de investigación y mecanismos de coordinación interinstitucional

Figura 2

Reformas digitales: la nueva función del agente encubierto



Fuente: adaptado del Decreto Legislativo n.º 1591, del Congreso de la República del Perú.

1.2.1. Agente encubierto en entornos digitales

En la actualidad la era digital y la incorporación masiva de las TIC ha transformado el modo en que nos comunicamos, realizamos actividades cotidianas, efectuamos transacciones bancarias y compartimos información a través de diferentes plataformas tecnológicas, este progreso tecnológico ha propiciado el surgimiento de los delitos informáticos o ciberdelitos, derivados de la automatización y la digitalización de procesos que facilitan la interconexión global; sin embargo, este avance ha originado la aparición de nuevos métodos delictivos, lo que obliga a los legisladores a actualizar y perfeccionar las normas, y a los fiscales a revisar y adaptar sus estrategias de investigación y su persecución penal, y al Poder Judicial a administrar justicia. Uno de los grandes retos para el ordenamiento jurídico reside en adaptarse a la realidad digital, así, mediante el Decreto Legislativo n.º 1591 se establece una respuesta integral y eficiente del Estado peruano orientada a fortalecer la persecución penal a través de la tipificación de los delitos informáticos, la precisión de la realización de los actos de investigación y la coordinación entre instancias competentes en materia penal y el uso de agentes encubiertos.

Entre las principales innovaciones más destacadas en las legislaciones internacionales en la lucha contra los ciberdelitos se encuentra el uso de agentes encubiertos como método de investigación. Para Villar

Fuentes (2022), en los tiempos actuales, la incorporación de la tecnología en los procesos judiciales es una realidad ineludible, esta integración no solo responde a la necesidad de modernizar el sistema de justicia, sino que plantea el desafío de garantizar que se respeten las garantías y los derechos fundamentales de los ciudadanos. El fenómeno del ciberdelito se caracteriza por su rápida evolución, lo que permite mantenerse un paso por delante de las herramientas y los métodos de investigación, esto evidencia que mientras los delincuentes se benefician de la rapidez de los medios digitales, el sistema de justicia tiene que actualizar, perfeccionar, sus instrumentos técnicos y metodológicos; en efecto, se trata de materias versátiles con evoluciones complejas, que hacen imposible adaptarse.

Mediante el Decreto Legislativo n.º 1591 se han incorporado las modificaciones de la Ley n.º 30096 y el Decreto Legislativo n.º 957 en lo relativo a la figura del agente encubierto, la redacción otorga al representante del Ministerio Público la facultad de autorizar la actuación de agentes encubiertos en entornos digitales. Esta modificación de la norma resulta esencial para adaptarse a las nuevas modalidades delictivas, sin duda alguna, se plantea el desafío de garantizar respeto al debido proceso, a los principios constitucionales y a los derechos fundamentales y humanos, así como la necesidad de contar con un control judicial estricto. En esencia, la norma jurídica adapta herramientas tradicionales de investigación al integrar la tecnología que responde a la dinámica del ciberdelito; no obstante, la correcta aplicación dependerá de protocolos de actuación entre el Ministerio Público, el Poder Judicial y la División de Investigación de Delitos de Alta Tecnología, mecanismos de supervisión del cumplimiento del debido proceso por parte del Poder Judicial.

En los últimos años, el incremento de delitos en el Perú mediante el uso de las TIC, junto con la diversificación de las modalidades delictivas, demanda que el Estado peruano refuerce la persecución penal. Tal como se establece en el Decreto Legislativo n.º 1614, el Congreso de la República del Perú ha encomendado al Poder Ejecutivo la labor de legislar en materia de seguridad ciudadana, con la finalidad de enfrentar el fenómeno de la ciberdelincuencia y proteger los derechos fundamentales de los menores de edad frente a conductas ilícitas perpetradas por los ciberdelincuentes; bajo este contexto, este marco legislativo se focaliza en:

1.3. Decreto Legislativo n.º 1614

Figura 3

Acceso ilícito y fraude informático: la nueva era del delito

Fuente: adaptado del Decreto Legislativo n.º 1614, del Congreso de la República del Perú.

1.3.1. Acceso ilícito

Con el avance de la tecnología, el desarrollo de las innovaciones en tecnología y la creciente interconexión mundial, el acceso ilícito a sistemas informáticos se ha convertido en un problema de alcance internacional. Como uno de los desafíos para la ciberseguridad, comúnmente este delito atenta contra la privacidad de la información de empresas públicas, privadas, ministerios, instituciones del Estado y ciudadanos, engloba una amplia gama de tipologías y actividades ilícitas, desde acceder en todo o parte deliberada e ilegítimamente, sin tener autorización, ello implica la manipulación de datos personales en aplicaciones del Estado, aplicaciones web, bases de datos y plataformas digitales del Estado. Este fenómeno ha ido evolucionando a lo largo de los años, impulsado por la globalización del internet y el incremento de dispositivos interconectados, de acuerdo con la Organización de Cooperación y Desarrollo Económico (1986), que emitió un informe denominado «Delitos informáticos: análisis de la política jurídica», el cual abordó el impacto del avance de la tecnología en el ámbito del derecho penal y la necesidad de adaptar el marco jurídico a la nueva era del ciberdelito.

El pasar de los años y la necesidad de tipificar adecuadamente las conductas ilícitas dentro de los delitos previstos en la legislación vigente en la década de los ochenta exigía la reevaluación de los conceptos jurídicos existentes y la creación de nuevos tipos penales, con la finalidad

de lograr una respuesta inmediata frente a la nueva era del ciberdelito. En este contexto, el informe de la OCDE de 1986 presenta un hito importante, pues enfatiza la importancia de establecer de forma clara, específica, las definiciones de los delitos informáticos, disposiciones que faciliten la obtención y el tratamiento de la evidencia digital, mecanismos de cooperación internacional.

El acceso ilícito es la intromisión no autorizada, total o parcial, en un sistema informático, sin el consentimiento del propietario o administrador, mediante la vulneración de medidas de seguridad establecidas para impedirlo (OCDE, 1986). Sin embargo, para la configuración del tipo penal es fundamental evaluar la conducta del ciberdelincuente al ingresar a un sistema informático, sin autorización del propietario o administrador, vulnerando las barreras de seguridad informática establecidas para proteger la confidencialidad, la integridad y la disponibilidad de información, dicha conducta infringe la normatividad penal vigente, ya que constituye un delito, al ingresar de forma deliberada e ilegítimamente a todo o parte de un sistema informático, debido a que corrompe la protección legal vigente (Morón, 2007).

El Ministerio Público (2024), en el *Boletín n.º 12*, indica que de enero a noviembre de 2024 se registraron 42 161 delitos informáticos, lo que representa un incremento del 42.53 % en comparación con el período 2023 en que fueron 29 580 delitos. Entre estos delitos se encuentran los cometidos contra el patrimonio, contra la fe pública, contra datos y sistemas informáticos, disposiciones comunes, contra la indemnidad y la libertad sexual, contra la intimidad y el secreto de las comunicaciones, así como otros no especificados.

La transformación digital ha impactado en todos los ámbitos de la sociedad, ya que ha mejorado la eficiencia y la conectividad; sin embargo, ha propiciado la aparición de una nueva modalidad delictiva: el *hacking*, conocido como acceso ilícito a sistemas informáticos. En el año 2024, la incidencia de delitos informáticos ha adquirido una relevancia creciente en el Perú; tal como se mencionó en el párrafo anterior, este aumento se evidencia especialmente en los delitos de acceso ilícito a sistemas informáticos en un 3.06 %. Para Villavicencio (2014, p. 49), la redacción del tipo penal penaliza la violación de la confidencialidad que

se comete al ingresar al sistema sin autorización, eludiendo las medidas de seguridad. De acuerdo con Gutiérrez (1996), el delito de *hacking* consiste en el acceso no autorizado a sistemas informáticos, redes o bases de datos, con la finalidad de obtener, modificar o usar información sin el consentimiento del propietario titular.

El Decreto Legislativo n.º 1614, art. 2, responde a la creciente amenaza de delitos cometidos mediante el uso de tecnología, que constituyen uno de los desafíos más complejos para el derecho penal en el Perú. Hablar de *hacking* implica comprender la naturaleza transnacional del delito, lo cual demanda una respuesta jurídica adaptada al dinamismo del entorno digital, dicho decreto legislativo buscar actualizar, mejorar la redacción del tipo penal y perfeccionar el marco sancionador frente a las conductas que vulneran la seguridad y la integridad del sistema informático.

A pesar de los avances significativos logrados con el Decreto Legislativo n.º 1614, uno de los principales desafíos que enfrenta la administración de justicia es el vertiginoso avance de las TIC, pues mientras que la tecnología avanza a un ritmo acelerado, el marco normativo y los procesos judiciales lo hacen con mayor lentitud. Ello genera un desbalance que, en muchas ocasiones, es aprovechado por los ciberdelincuentes, quienes hacen uso de diferentes herramientas tecnológicas para vulnerar la seguridad y las barreras de protección de los sistemas informáticos.

El ciberespacio se caracteriza por el anonimato y el esparcimiento geográfico (Morillas, 2017), es importante destacar que los métodos, las técnicas y las estrategias empleadas por los ciberdelincuentes dificultan la identificación del origen del ataque. Ante este desafío, resulta fundamental fortalecer la pericia técnica, la cooperación internacional y el desarrollo de protocolos eficaces de investigación.

La admisión y la valoración de pruebas digitales presenta otro reto en el proceso penal peruano, en la actualidad existen dificultades, tales como la preservación de la cadena de custodia digital y la necesidad de contar con un marco legal en la prueba electrónica. A pesar de los avances en materia de delitos informáticos, existen lagunas y ambigüedades en la tipificación de conductas emergentes, debido a nuevas modalidades y tipologías del delito.

1.3.2. Fraude informático

El surgimiento del internet ha dado origen a nuevas modalidades ilícitas, entre las que destaca el fraude informático. Según Gutiérrez (1991), esta nueva modalidad se lleva a cabo a través de medios electrónicos e informáticos y causa un perjuicio patrimonial a un tercero mediante la manipulación sobre los sistemas informáticos, al alterar datos y programas con la finalidad de obtener un beneficio ilícito.

El fraude informático se distingue por su impacto tanto en la economía como en la ciberseguridad, ya que implica diversas acciones ilícitas como el diseño, la introducción, la alteración, el borrado, la supresión, la clonación de datos informáticos, así como la suplantación de interfaces (Decreto Legislativo n.º 1614, art. 8).

Según Hernández (2009), durante los años sesenta, el avance progresivo de los ordenadores en el ámbito gubernamental y empresarial revolucionó por completo la forma en la que se cometían delitos. Durante esta época, la ciberdelincuencia se centraba en actividades vinculadas a la economía, dado que las nuevas tecnologías proporcionaban herramientas inéditas para ejecutar fraudes informáticos, manipular datos, sabotear sistemas informáticos, espionaje empresarial, entre otros. Estas diferentes formas delictivas permitían a los ciberdelincuentes aprovechar las vulnerabilidades de los sistemas informáticos con la finalidad de obtener beneficios económicos ilícitos.

En relación con lo anterior, estas prácticas delictivas no solo demuestran cómo la criminalidad se adapta a las innovaciones tecnológicas, sino que revelan un cambio en la psiquis de los delincuentes, quienes hacen uso de la tecnología para mejorar y expandir sus actividades ilegales. Este fenómeno ha impulsado a los legisladores a desarrollar marcos legales que permitan combatir eficazmente este tipo de delito.

El Ministerio Público (2024), en el *Boletín n.º 12*, indica que de enero a diciembre de 2024 el fraude informático representó un 68.09 %, y durante enero de 2025 representó un 68.14 %. El Decreto Legislativo n.º 1614 emerge como una respuesta legislativa debido a la frecuencia de este delito y establece mecanismos y criterios para su tipificación y su sanción. De acuerdo con Mayer y Oliver (2020), para la configuración

del tipo penal se requiere el uso de sistemas y herramientas digitales que manipulen, alteren o falsifiquen información con el fin de engañar a individuos o instituciones y obtener beneficios ilícitos o causar perjuicios. Sin duda alguna, se trata de obtener ventajas de las vulnerabilidades en los entornos tecnológicos con la finalidad de cometer ilícitos fraudulentos, lo que implica el conocimiento técnico y la intención del ciberdelincuente de defraudar.

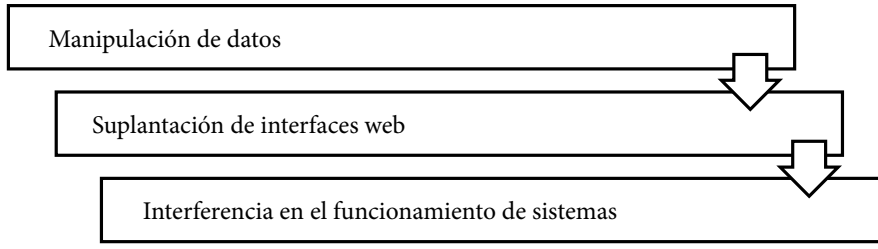
El fraude informático es una de las tipologías de delitos informáticos que consiste en manipular, alterar sistemas, datos, documentos y programas con el objetivo de conseguir beneficios ilícitos o causar un perjuicio a un tercero. Esta figura delictiva se caracteriza por el uso de la tecnología para introducir datos falsos y distorsionar la información, lo que permite al ciberdelincuente lograr ventajas económicas (González, 1999).

1.3.2.1. Tipologías

El Decreto Legislativo n.º 1614, art. 8, hace mención de tres tipologías del delito de fraude informático, tales como:

Figura 4

Tipologías del delito de fraude informático



Fuente: adaptado del Decreto Legislativo n.º 1614, del Congreso de la República del Perú.

En esencia, el delito de fraude informático en el Perú presenta una complejidad creciente debido a la rápida evolución de la tecnología y las diferentes formas de delinquir del ciberdelincuente. Esta tipología se clasifica en tres categorías principales:

a) Manipulación de datos

De acuerdo con Faraldo-Cabana (2007), es una acción deliberada e ilegítimamente destinada a alterar, modificar, distorsionar datos en sistemas o procesos digitales, cuyo propósito es inducir a error y obtener beneficios económicos ilícitos (Decreto Legislativo n.º 1614, art. 8). Este fenómeno se caracteriza por el diseño, la introducción, la alteración, el borrado, la supresión, la clonación de datos informáticos a fin de obtener beneficios ilícitos, y afecta tanto a individuos como a instituciones, empresas y a terceras personas. No cabe duda de que la transformación digital ha impulsado a los legisladores peruanos a modificar la tipificación penal para adaptarla a esta nueva realidad, los delitos informáticos cometidos en el ciberespacio presentan diversas características, sin embargo, es fundamental establecer una delimitación clara respecto a las particularidades del fraude informático. Para Fernández Delpech (2014), esta modalidad delictiva se caracteriza por ser compleja, transnacional y por el dinamismo en las estrategias usadas por los ciberdelincuentes.

b) Suplantación de interfaces web

La creciente evolución de los lenguajes de *frontend*, como *HyperText Markup Language* (en adelante HTML), *Cascading Style Sheets* (en adelante CSS); así como los lenguajes de *backend*, como *Hypertext Preprocessor* (en adelante PHP) y de los lenguajes de base de datos, como *Structured Query Language* (en adelante SQL), han impulsado avances significativos en el desarrollo web y lo han convertido en un pilar fundamental de la sociedad del siglo XXI. No obstante, este crecimiento conlleva nuevos desafíos, especialmente en materia de seguridad informática, un tema de gran preocupación a nivel internacional. Entre los riesgos más notorios se encuentra la suplantación de interfaces web, una técnica utilizada por ciberdelincuentes para crear réplicas de sitios web legítimos, con la finalidad de engañar a los usuarios y obtener beneficios ilícitos, como el robo de información de datos, tarjetas de crédito; estas prácticas amenazan la integridad, la seguridad y la confianza de los usuarios en el entorno digital.

La suplantación de interfaces web es una técnica de ingeniería social, que según Díaz (2021) se trata de un conjunto de técnicas sofisticadas y de estrategias utilizadas para manipular psicológicamente a las personas, con el objetivo de obtener información confidencial, datos personales, información financiera, datos de cuenta bancarias. Para Faraldo-Cabana (2007) es el uso de métodos diseñados para inducir al error mediante la creación y la reproducción de réplicas que imitan la apariencia de un entorno web, con el fin de engañar a los usuarios que interactúan con una plataforma legítima.

En este contexto, la naturaleza y la velocidad en la que se comete el delito plantean desafíos significativos para su investigación y su persecución, de igual modo para la identificación del ciberdelincuente y la sanción de los responsables por parte del Poder Judicial.

c) Interferencia en el funcionamiento de sistemas informáticos

El avance de la tecnología en la era digital ha revolucionado distintos ámbitos de la sociedad y ha facilitado la automatización de sistemas informáticos en múltiples sectores; esta transformación ha optimizado procesos, al incrementar la eficiencia operativa y elevar la productividad. Como la precisión en la gestión de la información, la automatización se extiende a la industria, el comercio, las finanzas, la educación y la salud, y redefine la forma en que interactuamos con la tecnología; sin embargo, este desarrollo plantea importantes desafíos jurídicos en la protección de los sistemas informáticos, ciberseguridad en dichos sistemas. Este aspecto se ha convertido en una prioridad a nivel internacional, debido a que los gobiernos, las empresas y las instituciones se enfrentan a diferentes formas de amenazas cada vez más sofisticadas. Entre los riesgos más notorios se encuentra la interferencia en el funcionamiento de sistemas informáticos, regulada en el Decreto Legislativo n.º 1614, art. 8.

La interferencia en el funcionamiento de sistemas informáticos comprende toda acción deliberada, ilegítima, maliciosa, destinada a alterar, bloquear o deteriorar el normal funcionamiento de sistemas informáticos. Este tipo de conductas se materializa a través de ataques de negación de servicios (en adelante DDoS). Arizaga *et al.* (2022) refieren que un ataque DDoS es una modalidad de ciberataque que consiste

en la saturación de un sistema, servicio o red, cuyo fin es bloquear el acceso a los usuarios. Mientras que para Rivera *et al*. (2020) esta clase de ataque ocurre cuando diferentes dispositivos envían al mismo tiempo demasiadas solicitudes a un sitio web con el único fin de saturar sus recursos y hacer que deje de funcionar correctamente.

Un ciberataque de DDoS abarca acciones cometidas de manera deliberada, ilícita, con intención maliciosa, con el fin de interrumpir el funcionamiento de un sistema, base de datos. Con el pasar de los años, el derecho penal se ha visto forzado a evolucionar para adaptarse a los vertiginosos cambios tecnológicos; en la actualidad diversos países han reformado sus legislaciones, sus estatutos legales, estas reformas no solo responden al avance tecnológico, sino al surgimiento de los ciberdelitos.

2. EL CIBERESPACIO

En la historia de la humanidad hemos transcurrido por diferentes etapas especiales cuyas características han marcado un hito importante en la sociedad. Actualmente estamos viviendo en la era de la información, la incorporación de las TIC y el uso del internet ha generado un cambio internacional en el gobierno de cada país, se ha incorporado su uso a las gestiones públicas. Según Espinoza Sánchez (2019), la irrupción de las TIC en la sociedad ha inducido a la intercomunicación entre personas y entre países, lo cual ha facilitado la transmisión de su cultura, su economía, su política y su forma de vida. Además, la tecnología ha contribuido a la modernización, la transformación de sistemas en la industria y en las instituciones del Estado. Estos cambios han alterado la forma de convivencia en sociedad; sin embargo, el internet ha ocasionado ciertos perjuicios e incertidumbres a la sociedad, donde el ciberespacio se ha convertido en un escenario delictivo para una nueva forma de criminalidad.

La era digital está caracterizada por la globalización de los mercados, la interconexión en la economía internacional entre diferentes países del mundo y los movimientos migratorios, frente a estas transformaciones sociales se producen cambios en el sistema penal que dan lugar a la adaptación del Código Penal, actualmente el internet ha revolucionado el mundo de las comunicaciones y del conocimiento (Giménez, 2006).

La globalización y el internet no solo han mejorado las relaciones económicas entre países, sino también en el ámbito político, social y personal. Con el pasar de los años la evolución tecnológica ha optimizado el ciberespacio, que es el escenario perfecto para cometer delitos informáticos, pues la universalización de la informática en los países ha permitido mejorar los procesos de tiempo y espacio, creando ciertas vulnerabilidades que los delincuentes informáticos han aprovechado para cometer hechos ilícitos, ello ha implicado la evolución del delito tradicional al delito informático. Para Sain (2018), el uso de dispositivos automatizados y la tecnología ha generado nuevas formas ilícitas y se han adoptado nuevas figuras, nuevas tipologías del delito tradicional al delito informático.

Es evidente que el delito informático marcó una diferencia en la sociedad, con el transcurso de los años han surgido diferentes ilícitos que no están regulados en los ordenamientos jurídicos, figuras inexistentes y que hoy en día se han tenido que regular en el Código Penal. Debido al fenómeno criminal de la ciberdelincuencia se han desarrollado instrumentos internacionales, diferentes ordenamientos jurídicos han adaptado sus legislaciones al Convenio de Budapest, puesto que dicho instrumento internacional busca combatir y erradicar toda forma de ciberdelincuencia. En el Perú, a causa de la pandemia por COVID-19 los delincuentes informáticos han hecho uso de la tecnología para facilitar la comisión de actos ilícitos y eludir las investigaciones del Ministerio Público. Para Chirino Sánchez (2021) existen fenómenos constituidos por acciones ilícitas de alcance mundial que ponen en peligro a la sociedad, se trata de la criminalidad con características peculiares y específicas. Debe considerarse que con el pasar de los años las nuevas tendencias en tecnología han abarcado otro nivel originando la evolución de la criminalidad en cibercriminalidad, por lo cual los escenarios en que se desenvuelve requieren un análisis del legislador en sus modalidades para su futura tipificación por los operadores de justicia. Dentro de este orden de ideas estamos ante un conjunto de nuevos actos ilícitos que ponen en peligro a la sociedad a nivel nacional e internacional.

Debe tenerse en cuenta que esta nueva realidad ha determinado una nueva forma de ver el delito a través de medios tecnológicos, en

sus distintas tipologías y modalidades. Sin duda alguna, no solo se trata de suplantar la identidad de la víctima en las redes sociales o realizar transacciones bancarias, propagar virus informáticos, estafas, extorsión, hackeo, acoso sexual, que han sido positivizados en la Ley n.º 30171 en concordancia con el Convenio de Budapest. En efecto, están categorizados en delitos contra datos y sistemas informáticos, delitos contra la indemnidad y libertad sexual de menores, delitos contra la intimidad y el secreto de las comunicaciones, delitos contra el patrimonio, delitos contra la fe pública.

Cabe resaltar que la proliferación del acceso a internet ha transformado el modelo de la organización criminal y banda criminal mutando a un nuevo escenario digital. Para la Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC, 2022), en efecto, las TIC han transformado las características, las clasificaciones, las modalidades, el modo de obrar, las tipologías, así como la naturaleza de la delincuencia común y han dado vida a la delincuencia organizada; en concreto, esta transformación ha permitido la participación de personas dentro de la organización criminal cuyos aspectos delictivos han ampliado gradualmente su intervención, su propia estructura, su organización y la colaboración de sus autores y sus coautores. Estos grupos suelen tener una función dentro de la organización, dentro de ellos los más destacados son los codificadores y los piratas informáticos. Así, el Instituto Nacional de Estadística e Informática (INEI, 2023), en el *Informe Técnico n.º 03*, indica que durante el primer trimestre del año 2023 la sociedad peruana ha experimentado una nueva forma de ilícitos penales por medios tecnológicos. A nivel nacional se han registrado un total de 413 denuncias; en el primer trimestre del año 2022, 403 denuncias; y en el primer trimestre del año 2021, 313 denuncias. Conforme se ha podido observar en las estadísticas del INEI, comprobamos que el índice de delincuencia ha aumentado notoriamente a nivel nacional.

Es evidente que el alcance transfronterizo del internet se ha expandido en todo el Perú, no importa la ubicación geográfica, el territorio, la nacionalidad, el idioma, las personas pueden formar parte de organizaciones criminales desde cualquier lugar del mundo. Ello genera cuestionamientos en los juzgados que son competentes para resolver la presente

causa. Para la UNODC (2022, p. 3), en definitiva, las TIC desempeñan un papel importante en la expansión de las telecomunicaciones, las redes, y son fundamentales para la sociedad; de modo similar surge la expansión de mercados y negocios ilícitos en el ciberespacio debido a que proporcionan un espacio virtual para llevar a cabo actividades ilícitas, debido al anonimato, las lagunas de los ordenamientos jurídicos son problemas frecuentes que suelen ocurrir a menudo.

La era digital se caracteriza por poseer un componente tecnológico, lo que ha llevado en la actualidad a la automatización de sistemas informáticos. Este desarrollo se encuentra presente en el gobierno estatal, el sistema de salud, el sistema tributario, el sistema financiero, el sistema inmobiliario, los sistemas aduaneros, entre otros. Dentro de este desarrollo se ha producido un nuevo fenómeno delictivo para la sociedad, denominado delitos informáticos, razón por la cual, desde la comisión de un hecho ilícito, es el Ministerio Público el que conduce inicialmente la investigación, cuyos resultados determinarán si promueven o no la acción penal, conforme a la Constitución Política del Perú, art. 159, inciso 4.

Mediante la Resolución de la Fiscalía de la Nación n.º 1503-2020-MP-FN se apertura la Unidad Fiscal Especializada en Ciberdelincuencia del Ministerio Público, con competencia nacional, y de acuerdo con esta última institución, durante el año 2021 se interpusieron 12 637 denuncias y en el año 2022 16 788 denuncias en las Fiscalías Provinciales, Penales, Especializadas y Mixtas a nivel nacional en delitos informáticos (Ministerio Público, 2022).

Las TIC han marcado un antes y un después en la sociedad; con el auge de las tecnologías el delincuente común se ha adaptado a los cambios que han surgido y se ha amoldado a este nuevo escenario, aprovechando las ventajas de este nuevo escenario debido las deficiencias en la legislación que acarrean como consecuencia un espacio de impunidad, donde expertos en informática, *hackers*, toman el control y abren paso a nuevas formas de delincuencia más avanzada (Salom, 2011).

3. INTERNET, LA NUEVA ERA DEL DELITO

Para que la conducta sea considerada como un hecho punible es necesario que cumpla las características de la teoría del delito, el objeto de la

imputación penal permite acusar las conductas delictivas. Por lo tanto, es un instrumento cuyos criterios y argumentaciones son utilizados en la decisión y la solución de casos penales; en efecto, el delito es una conducta típica, antijurídica y culpable (Villavicencio, 2006).

Para investigar la comisión de un delito hay que seguir una serie de métodos y técnicas para determinar si se promueve o no la acción penal, así como la fórmula legal de la teoría del delito. Cuando hacemos referencia al principio de tipicidad, opinamos que toda acción humana voluntaria o involuntaria lleva a cometer un acto y dicho acto se subsume a los presupuestos establecidos en la norma legal. Al respecto, de acuerdo con Villavicencio (2006), la tipicidad es la comprobación de la conducta realizada y si encaja en el tipo coinciden, este proceso se denomina juicio de tipicidad, cuyo objetivo es determinar si un hecho se adecúa en el tipo penal; asimismo, se toma como pilar fundamental el bien jurídico protegido con la finalidad de determinar si el hecho puede ser o no atribuido al sujeto activo.

Con la expansión del internet a nivel mundial y el desarrollo de las TIC se han multiplicado los beneficios y los perjuicios que suelen existir en el ciberespacio, por esta razón se puede decir que el derecho se ha amoldado a la realidad actual creando una forma de regular las conductas del ser humano, que se manifiesta a través del derecho penal como acciones antijurídicas. De acuerdo con la teoría del delito es necesario instaurar qué conductas del ser humano son consideradas como delito, es transcendental enfatizar que no toda acción humana es considerada antijurídica, por esta razón, la acción humana para que sea estimada como delito tiene que ser típica, antijurídica y culpable. Dichas acciones son plasmadas en un cuerpo legal con su respectiva tipificación, con la finalidad de que las personas que incumplan sean sancionadas. Tómese en cuenta que el Código Penal peruano regula en su título preliminar el principio de legalidad, que es la base del derecho penal y donde se refleja la tipicidad. Según Posada Maya (2017), el cibercrimen ostenta características especiales, por lo que la teoría del caso en esta nueva forma de criminalidad debe ser replanteada, pues los delitos que suelen ocurrir son a través de realidades virtuales. De acuerdo con el estudio de Leyva

Serrano (2019), tipificar los delitos informáticos es una tarea compleja debido a su amplitud, sus modalidades, sus tipologías, así como señalar el bien jurídico afectado.

Desde el momento en que una persona comete un delito infringe el ordenamiento jurídico, sin embargo, desde que se incurre en un delito informático cambia el panorama a causa de que los delincuentes hacen uso de la tecnología y de dispositivos tecnológicos con la finalidad de cometer diferentes modalidades de delitos informáticos, ciberataques. La comisión de este tipo de ilícitos se originó desde antes de que estuviesen regulados en el ordenamiento jurídico, por lo que a futuro se ajustaron normas para su debida tipificación. Tipificar los delitos informáticos se hace necesario debido a que si ciertas conductas ilícitas no se encuentran reguladas en el ordenamiento jurídico, sería imposible establecer la tipicidad, la antijuricidad y la culpabilidad, y a futuro las sanciones a los delincuentes informáticos. Asimismo, se debe privilegiar el principio de legalidad, que es reconocido a nivel internacional y nacional en la legislación peruana como un pilar fundamental para el derecho penal.

En efecto, la necesidad de tipificar el tipo penal, recabar la prueba informática, la cadena de custodia y el respeto de los principios constitucionales resulta ser importante en todo proceso judicial. Uno de los primeros casos en Europa sobre espionaje informático fue en Barcelona, en 1997, y es conocido como el caso de Hispahack, llevado por el Juzgado de lo Penal n.º 02 de Barcelona, en el Procedimiento Abreviado n.º 130/99-E de la Ley Orgánica 7/1988. En principio, en este proceso los hechos enjuiciados al acusado no eran delitos tipificados en la época, tampoco existían pruebas fehacientes que permitieran la corroboración del hecho ilícito; no obstante, todo requerimiento acusatorio debe cumplir ciertas formalidades en los requisitos de procedibilidad, conductas punibles y la calificación jurídica, entre otros.

En el Perú, la acusación fiscal está expresamente regulada en el art. 349 del Código Procesal Penal (2004), donde se señalan expresamente los requisitos que deberá contener la acusación. Para Arbulú (2015, p. 227) es la potestad del representante del Ministerio Público, cuya finalidad es solicitar el procesamiento de una persona, donde se debe desarrollar la individualización del acusado, el hecho imputado, la

tipificación, los medios de prueba, la pena y la reparación civil. El Acuerdo Plenario n.º 6-2009/CJ-116 ha establecido que la acusación es un acto de postulación del Ministerio Público donde fundamenta y deduce la pretensión penal, dicha petición debe estar debidamente motivada al órgano jurisdiccional.

El Código Procesal Penal (2004) regula en su título preliminar el principio acusatorio y ha establecido que el Ministerio Público es el titular de la acción penal, a quien también se le encomienda la carga de la prueba y asume la función de conducir la investigación desde el momento en que ha tomado conocimiento de la noticia criminal. Por su parte, la Policía Nacional del Perú previene, investiga y combate la delincuencia y contribuye en la investigación del delito.

El problema surge al tratar de aplicar los mismos métodos, los criterios y las técnicas a la delincuencia informática debido a la alta complejidad del delito que es materia de investigación. Según Acurio del Pino (2016), investigar el delito es una etapa compleja, de eso no hay duda, las dificultades surgen al tratar de aplicar las técnicas de investigación, el método científico a la delincuencia transnacional y al crimen organizado y enfrentar este nuevo paradigma es una de las labores a las que se avoca el representante del Ministerio Público. Durante los últimos años este fenómeno ha tenido un avance significativo debido a la globalización y esta clase de delitos son denominados como delitos informáticos.

Cabe considerar que las TIC han propiciado el acontecimiento de nuevas conductas ilícitas, la dificultad de poder encuadrar estos supuestos en los tipos penales ha motivado la actualización de las normas penales en sus diferentes codificaciones y legislaciones con la finalidad de evitar la impunidad. Desde la comisión de un hecho punible a través de medios tecnológicos han existido diferentes problemas al tipificar cualquier tipo de delitos informáticos, cuyas características son el anonimato, la falta de cadena de custodia, dificultades en la investigación y en su comprobación. Ello trae como consecuencia pérdidas económicas y el archivo de la investigación en contra de los presuntos responsables.

4. ASPECTO GENERAL DEL DELITO INFORMÁTICO

4.1. Antecedentes normativos internacionales

En 1977 el senador Abraham Ribicoff presentó ante el Nonagésimo Quinto Congreso la primera propuesta legislativa sobre delitos y fraudes informáticos denominada Federal Computer Systems Protection Act of 1978 (S-1766), a causa de delitos que afectaban a sistemas informáticos de organismos públicos, servicios públicos en pérdidas considerables en dinero, pérdidas en *software* y datos. Dentro de los delitos que figuraban en dicho proyecto de ley se encuentran: introducción fraudulenta en sistemas, uso no autorizado de instalaciones informáticas, destrucción o alteración de datos, robo de bienes (dinero en efectivo, datos informáticos), dicho proyecto de ley no fue aprobado por el Comité Judicial del Senado.

El Convenio n.º 108 del Consejo de Europa, del 28 de enero de 1981, fue uno de los primeros instrumentos internacionales adoptado en el ámbito de la protección de datos.

Con la finalidad de combatir la delincuencia informática transnacional en sus diferentes modalidades, tipologías y el peligro que ocasiona en el ciberespacio de tal forma que acarrea como consecuencia pérdidas económicas, en 1983 un grupo de expertos de la Organización para la Cooperación y el Desarrollo Económico (en adelante OCDE), a causa de la delincuencia informática y sus consecuencias en la sociedad internacional, inició un estudio cuyo fin era aplicar en el derecho internacional las leyes penales, el cambio en la estructura de los códigos penales para incorporar delitos informáticos (Sieber, 1987).

El Consejo de Europa (en adelante CdE) en la Recomendación n.º R (85) 10, adoptada el 28 de junio de 1985, reconoce la importancia de la asistencia mutua internacional en la lucha contra la delincuencia internacional.

En 1986 la OCDE publicó un informe denominado «Delitos de informática: análisis de la normativa jurídica», cuyo contenido hace referencia a la reforma legislativa, así como recomendaciones por las que deben optar los países miembros sobre las prohibiciones y las sanciones a través de sus leyes penales (Acurio del Pino, 2016).

El CdE en la Recomendación n.º R (87) 15, adoptada el 17 de septiembre de 1987, reconoce las amenazas a la intimidad de las personas por el uso de tratamientos automatizados de datos, así como la importancia en la prevención y la represión de las transgresiones penales.

El CdE en la Recomendación n.º R (89) 9, adoptada el 13 de septiembre de 1989, reconoce el carácter transfronterizo de la delincuencia informática y la importancia de una respuesta adecuada y rápida a este nuevo fenómeno, así como la necesidad de una legislación adecuada al mejorar la cooperación jurídica internacional, y concluye las pautas que deben tener en cuenta los legisladores a la hora de modificar su legislación o elaborar normas legislativas. Cabe considerar que dentro de la recomendación emitida se remarca la necesidad de actualizar la legislación en materia de delitos informáticos conforme al desarrollo tecnológico para erradicar todo tipo de actos ilícitos a través de medios tecnológicos.

La necesidad de contar con una legislación específica en delitos informáticos fue parte de la discusión y el análisis en el Décimo Tercer Congreso Internacional por la Academia de Derecho Comparado de Montreal, Canadá, en 1990.

No obstante, en La Habana (Cuba) se realizó el Octavo Congreso de las Naciones Unidas sobre Prevención del Delito y Tratamiento del Delincuente (1990), el cual reconoce que la delincuencia internacional iba en aumento y dentro de sus recomendaciones indica la investigación a la estructura de la delincuencia organizada, y sucesivamente la cooperación internacional contra el terrorismo.

El CdE en la Recomendación n.º R (95) 13, adoptada el 11 de septiembre de 1995, reconoce la importancia de adaptar los instrumentos legales en la legislación procesal penal sobre investigaciones en sistemas de información electrónica.

En el 2001 el CdE y los demás Estados reconocieron el interés de la cooperación entre los países en materia de ciberdelincuencia y decidieron, asimismo, aplicar una política penal con el objetivo de proteger a la sociedad en general a través de una legislación adecuada mediante el Convenio sobre la Ciberdelincuencia.

4.2. Noción

Hoy en día la sociedad está cada vez más conectada a través de internet, razón por la cual la delincuencia informática ha aprovechado esta transformación y plantea una amenaza a los gobiernos, las empresas nacionales e internacionales, y a la sociedad a nivel mundial. Para la delincuencia informática no existen fronteras, jurisdicción, y se complica al momento de recabar la prueba electrónica, lo que resulta ser un problema a la hora de realizar una investigación y recabar elementos de convicción. Desde que se empezaron a investigar los primeros delitos por computadora existieron diferentes autores que se centraban en un punto de partida: la reforma de la legislación, debido a la ineficacia de la legislación de la época, los vacíos legales, la prueba por delitos informáticos. Bequai (1978), con el estudio *Computer crime* (Crimen informático), indica que el crimen informático y la ineficacia en la aplicación de la ley era un problema en 1978, pues existían robos de grandes cantidades de dinero a través de computadoras, aunque la cifra real podía variar debido a la tasa de descubrimiento del delito; los delincuentes informáticos evaden la justicia a causa de los vacíos legales, la lentitud de la investigación, las leyes relacionadas con delitos informáticos son insuficientes. El sistema de justicia de la época no estaba preparado para contrarrestar el problema y se hizo necesario adaptar la prueba informática y la legislación a fin de ocuparse del crimen informático. Si estos problemas no se abordan a futuro, las consecuencias podrían ser fatales para la sociedad.

El abuso de las nuevas tecnologías a nivel mundial ha originado en el legislador criterios para tipificar las conductas generadas por los delincuentes informáticos. Cabe destacar que en los años sesenta las primeras conductas infringían los derechos de la personalidad, situación que condujo a los legisladores a la protección de datos personales; mientras que en los años setenta eran los delitos económicos con contenido informático (Mazuelos, 2007).

4.3. Definición doctrinal

Para seguir el presente trabajo es importante abarcar un punto de partida conceptual sobre la terminología de delito informático, nos preguntamos

¿es lo mismo delito informático, delito cibernético, cibercrimen, crimen por computadoras? Es evidente que citaremos a diferentes autores que han tratado de abarcar su terminología, para Hernández Díaz (2009) a lo largo de los últimos años el concepto de delito informático va unido a la evolución de las TIC y las conductas delictivas; las primeras conductas ilícitas se centraban en el ámbito empresarial, que consistía en lesionar el patrimonio, por este motivo las definiciones iniciales se limitaban a dicho ámbito.

Parker (1976) en su estudio precisó que el abuso informático es cualquier incidente que involucra a la tecnología informática, donde existen dos sujetos: la víctima (quien sufre el agravio o el daño) y el autor (quien comete el delito y obtiene un beneficio). Por otra parte, Camacho Losa (1987) considera que el delito informático es toda acción dolosa cuya finalidad es provocar un perjuicio a personas o entidades, sin la necesidad de que conlleve un beneficio para el autor, y para su comisión interviene el uso de dispositivos utilizados en actividades informáticas.

Mientras que para Téllez Valdés (2009) abarcar la definición sobre delitos informáticos no es una tarea sencilla, ya que la denominación de delito está consignada de manera expresa en textos jurídicos penales, es decir, hablamos de acciones típicas o atípicas, puesto que en algunos países no han sido objeto de tipificación; por esta razón, el delito informático se clasifica en forma típica (conductas típicas, antijurídicas y culpables) y atípica (actitudes ilícitas).

Otro sector de la doctrina, como Jijena Leiva (1994), estima que es toda acción que es típica, antijurídica y culpable, para cuya consumación es necesario el uso de la tecnología computacional. Por otra parte, según Davara Rodríguez (2015) es toda acción que cumple con los requisitos del delito y que se ejecuta mediante el uso de dispositivos informáticos. Para finalizar, en opinión de Fernández Calvo (1996), el delito informático es una acción que delimita el concepto de delito y se lleva a cabo haciendo uso de un elemento informático o telemático en agravio de la sociedad.

A pesar del transcurso de los años ya existían diversas actividades delictivas que empleaban elementos de la informática (computadoras, red informática, dispositivos de red) al usar diferentes técnicas con el

fin de obtener dinero ilícito, robar información personal, suplantar la identidad de personas, entre otras. Sarzana (1979), en su artículo «Criminalita e tecnología» (Crimen y tecnología), indica que el crimen por computadora es cualquier forma de comportamiento criminógeno en donde la computadora es el eje principal como material u objeto de una acción criminógena.

El avance tecnológico y el uso del internet han originado el acceso a la información en tiempo real y una interconexión a nivel mundial; sin embargo, dentro del ciberespacio existen riesgos que han generado una nueva forma de delinquir y según la literatura norteamericana este nuevo fenómeno se conoce como crimen por computadora y está vinculado a delitos informáticos. Se puede inferir que Mazuelos (2007) hace énfasis en que la computadora es pasible de dos objetos, por un lado, existen usuarios que la utilizan con fines criminales. Por otro lado, las computadoras son pasibles de ataques informáticos, y se debe resaltar que la denominación de delito informático es poco mencionada en las legislaciones penales; sin embargo, bajo este precepto se describen nuevas formas de ilícitos.

El delito informático es aquel que se relaciona con la comisión del delito a través del uso de la computadora y el internet, no obstante, esta forma de criminalidad no se realiza únicamente a través de medios tecnológicos, pues estos son solo instrumentos para cometer el delito (Villavicencio, 2014). De acuerdo con Mühlen (1973, citado por Mazuelos, 2007), el delito informático comprende todo tipo de comportamiento ilícito en donde la computadora es un instrumento y objeto del hecho ilícito.

Dentro de este orden de ideas, la denominación de delitos informáticos es utilizada en algunos sectores de la doctrina, y en las diferentes legislaciones internacionales puede variar. No obstante, dado el desarrollo de esta nueva forma ilícita va adquiriendo nuevas denominaciones, tales como delito cibernético, cibercrimen, crimen por computadoras, delincuencia informática, criminalidad mediante computadoras, abuso informático, criminalidad informática. Por nuestra parte, en el Estado peruano, mediante la Ley n.º 30096 adquiere la denominación de delitos informáticos, no contiene una definición específica, y a nivel internacional tampoco se ha determinado una. En nuestra

opinión, se considera como delito informático toda acción humana, típica, antijurídica y culpable, que involucra el uso indebido de la tecnología. Asimismo, dichas acciones están debidamente reguladas en la legislación y sancionadas con una pena privativa de la libertad, causan un perjuicio económico a una persona natural o jurídica en forma directa o indirecta, son realizadas a través de las TIC y/o entornos digitales, y perpetradas por individuos u organizaciones criminales con la finalidad de obtener beneficios de carácter patrimonial ilícito (lucro financiero).

4.4. Características

Los delitos informáticos cometidos en el ciberespacio ostentan diversas características, por lo que se hace necesario delimitar estas para saber diferenciarlos de otros tipos de delitos. Fernández Delpech (2014) detalla una serie de circunstancias que hacen que la persecución de esta clase de ilícitos sea complicada por parte del representante del Ministerio Público:

a) La falta de tipificación específica sobre el delito.
b) La transnacionalidad de las conductas.
c) La falta de consenso internacional

Palazzi (2016) detalla como características:

a) La magnitud de daños a nivel global e internacional.
b) La complejidad y la dificultad en las investigaciones.
c) La facilidad de cometer el delito.
d) La dificultad en la cooperación internacional.

Téllez Valdés (2009), por otro lado, señala las siguientes características:

a) Conductas criminales de cuello blanco.
b) Acciones que ocasionan pérdidas económicas.
c) Delitos que se cometen a distancia debido a la separación temporal y espacial.
d) La falta de regulación en su legislación.
e) Dificultad para su comprobación y para recabar elementos de prueba.

Mientras que Temperini (2018) detalla como características:

a) Delitos de cuello blanco.
b) Son delitos transnacionales.
c) Son delitos instantáneos.
d) Son delitos masivos.
e) Son delitos anónimos.
f) Son pluriofensivos.
g) Complejidad en la investigación.

Morillas Fernández (2017) indica como características:

a) Son delitos transnacionales.
b) Son delitos donde no existe el contacto físico.
c) Son delitos con tipología transfronteriza.
d) Son delitos cometidos por redes de telecomunicaciones internacionales.
e) Son delitos con acceso al medio tecnológico para alterar datos, sistemas.
f) Facilidad de encubrir el hecho ilícito al borrar las huellas del delito.
g) El anonimato y no dejar huella del hecho al momento de cometer el delito.
h) La dificultad en la investigación.

Los hallazgos de este estudio revelan una serie de características que son inherentes a los delitos informáticos: uno de los primeros problemas a nivel internacional es la falta de tipificación en diferentes países, tal es el caso del Perú, donde no existe una ley para formular una política pública para la sensibilización, la prevención y la protección de niños(as) y adolescentes frente a diferentes delitos que se realizan mediante el internet, las redes sociales, los medios informáticos, los entornos digitales y los dispositivos móviles, como el *morphing*, el *ciberbullying* y los *deepfakes*. Esto, a futuro, puede generar que las acciones delictivas en el ámbito digital no estén debidamente tipificadas, como el caso del ciberterrorismo.

La amplia gama y la evolución constante de la delincuencia informática ha permitido el uso de *software* especializado para eliminar datos, registros e información almacenada en la nube o en dispositivos electrónicos; otro de los métodos más usados es el enmascaramiento de direcciones IP (protocolo de internet), que ha permitido ocultar la dirección del protocolo de internet, lo que dificulta rastrear la ubicación, así como eliminar evidencias digitales que pueden ser de gran uso para identificar al autor del delito, debido a la insuficiencia de la ley sobre prueba electrónica, que complica la labor de investigación por el representante del Ministerio Público. Por lo tanto, son delitos complejos al no poder corroborar el hecho ilícito con la evidencia digital.

La transnacionalidad en delitos informáticos y la capacidad de la tecnología en traspasar fronteras nacionales e internacionales genera que dichos delitos puedan ser cometidos desde un país contra diferentes objetivos. Un claro ejemplo es el *grooming*, en el cual el perpetrador puede estar ubicado en un país diferente de aquel en el que va a realizar acciones ilícitas con fines sexuales por medios tecnológicos, que afectan la indemnidad sexual y la libertad sexual del menor que se encuentra en otro país. No cabe duda de que los ciberdelincuentes pueden operar desde diferentes lugares del mundo con la finalidad de ocasionar un perjuicio económico a empresas, entidades del Estado y diferentes naciones. Debemos señalar que la transnacionalidad crea desafíos a la administración de justicia debido a la jurisdicción, a la cooperación internacional y a la dificultad de la extradición.

Como cuarta característica se encuentra el impacto a nivel global, que afecta a los gobiernos estatales de cada país, a empresas y a la sociedad en general, este incluye pérdidas económicas, violación de la privacidad de datos, riesgo en la estabilidad financiera, ataques informáticos, ciberterrorismo.

Debido a su amplia gama de tipologías, esta herramienta tecnológica permite el anonimato de los perpetradores para ocultar su identidad mientras realizan operaciones mediante el internet, las redes sociales, los medios informáticos, los entornos digitales y los dispositivos móviles. Ello dificulta la identificación y la futura persecución del

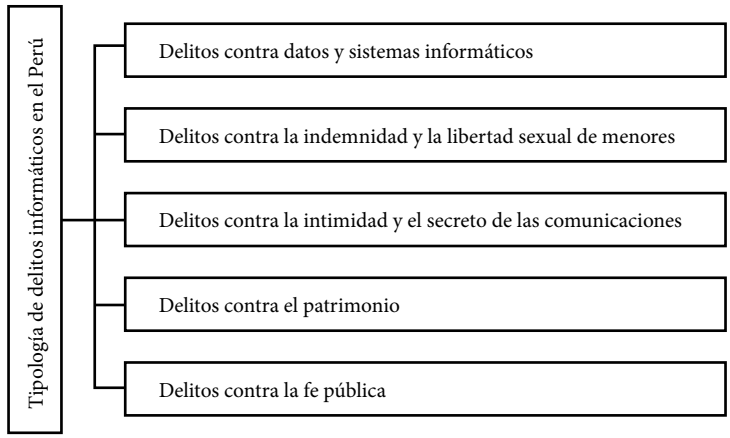
delito por el representante del Ministerio Público, lo que plantea desafíos a la administración de justicia.

4.5. Tipología

El Estado peruano no ha sido ajeno al desarrollo normativo, jurisprudencial, convenios, instrumentos, tratados internacionales en materia de delitos informáticos para encarar los desafíos que existen con las TIC. Para determinar la tipología es importante agregar que mediante el Decreto Supremo n.º 010-2019-RE, del 10 de marzo de 2019, el Gobierno peruano ratificó el Convenio sobre la Ciberdelincuencia a través de la publicación del *Diario Oficial El Peruano*, del 22 de septiembre de 2019, y tiene como vigencia el 1 de diciembre de dicho año; y de acuerdo con la Ley n.º 30096, que fue modificada por la Ley n.º 30171, no cabe duda de que el desarrollo normativo estuvo inspirado en el Convenio sobre la Ciberdelincuencia. En tal sentido, existen las siguientes tipologías:

Figura 5

Ley contra la ciberdelincuencia: prevención y sanción de delitos informáticos



Fuente: adaptado del Decreto Legislativo n.º 30096, del Congreso de la República del Perú.

De acuerdo con el Ministerio Público (2024), en el período de enero a diciembre de 2023 se registraron un total de 29 580 denuncias por delitos informáticos, dentro de este orden de ideas tenemos 724 denuncias por delito contra datos y sistemas informáticos, 88 denuncias por el delito

contra la indemnidad y la libertad sexual, 317 denuncias por el delito contra la intimidad y el secreto de las comunicaciones, 317 denuncias por el delito contra el patrimonio, 5246 denuncias de delitos contra la fe pública. Asimismo, se incluyen 663 disposiciones comunes, 700 denuncias sin especificar el delito subgenérico. No obstante, en el período de enero a diciembre de 2024 se registraron un total de 42 161 denuncias por delitos informáticos, dentro de las que se tienen 1289 denuncias por el delito contra datos y sistemas informáticos, 126 denuncias por el delito contra la indemnidad y la libertad sexual, 101 denuncias por el delito contra la intimidad y el secreto de las comunicaciones, 28 711 denuncias por el delito contra el patrimonio, 10 353 denuncias de delitos contra la fe pública; asimismo, se incluyen 666 disposiciones comunes y 915 denuncias sin especificar el delito subgenérico.

5. CONCLUSIONES

- La transformación digital ha permitido la proliferación de conductas ilícitas que a menudo no están reguladas en el marco normativo tradicional. Los ciberdelincuentes aplican técnicas, estrategias, métodos para operar de manera transnacional, lo que complica la labor de investigación y persecución del delito por parte del Ministerio Público y su sanción por parte del Poder Judicial. El reto radica en las lagunas legales debido a la falta de regulación para nuevos tipos penales, tales como el *vishing*, el *spoofing*, el *phishing* automatizado, los *deepfakes*, el *malware* inteligente, el ataque de denegación de servicio, el fraude financiero automatizado, la suplantación de identidad automatizada. Ante esta realidad transnacional, el desafío consiste en fomentar la cooperación internacional e implementar la legislación en la prueba electrónica, los peritajes informáticos, contar con presupuesto para poner en funcionamiento un laboratorio sofisticado en tecnología en apoyo de la labor fiscal.
- La falta de tipificación en el marco normativo, la transnacionalidad del ciberdelito, la ausencia de consenso y la necesidad de adaptar los procedimientos de investigación representan algunos de los obstáculos significativos que requieren solución. El principal reto radica en

la dificultad de mantener actualizadas las normas penales y procesales frente a la naturaleza cambiante del ciberdelito, lo que exige una revisión y modernización del marco jurídico. El verdadero desafío no solo consiste en enfrentar la carencia de la legislación adecuada, sino también la urgente necesidad de adaptar los procedimientos, las técnicas de investigación especial.

- El sistema de justicia peruano afronta retos en cuanto a la capacitación de los operadores de justicia en materia de cibercrimen y está desprovisto de herramientas tecnológicas avanzadas. Como desafío es indispensable la capacitación al representante del Ministerio Público respecto a técnicas especiales de investigación sobre ciberdelincuencia.
- Es increíble que los ciberdelincuentes hagan uso de la tecnología para cumplir con su objetivo de cometer delitos y evadir las investigaciones por el representante del Ministerio Público. Este hecho ha creado la necesidad de implementar normas jurídicas para prevenir y sancionar conductas que son cometidas mediante el uso de las TIC. En efecto, en el Perú al igual que en otros países existe el uso del agente encubierto, que son estrategias para investigar y recopilar pruebas contra los presuntos ciberdelincuentes; esta figura se menciona en el Decreto Legislativo n.º 1591, que introduce la modificación de la figura del agente encubierto.
- Con el desarrollo de las TIC, las telecomunicaciones y la globalización a nivel mundial, la sociedad ha sido víctima de diferentes modalidades de delitos informáticos en las cuales están involucradas las redes sociales, los medios informáticos, los entornos digitales y los dispositivos móviles y/o tecnológicos. Tal situación ha generado la importancia del recojo de la evidencia digital mediante la cadena de custodia para su respectivo análisis informático forense.
- Resulta evidente que los delitos informáticos abarcan una amplia gama de tipologías y existen diversas formas de actividades ilícitas que pueden ser cometidas por individuos u organizaciones criminales con la finalidad de obtener un beneficio económico, uno de los principales delitos es el lavado de activos y el uso de la criptomoneda.

- Los delitos informáticos ostentan una serie de características que los hacen únicos; sin embargo, existe un desafío para el derecho penal peruano, el ciberterrorismo, que implica el uso de las TIC con la finalidad de causar un daño masivo a los gobiernos, las empresas, la sociedad en general. No obstante, los ciberataques tienen un objetivo en común: causar daño al sistema gubernamental ocasionando un impacto a la seguridad nacional y a la economía del país.
- A medida que las TIC, las telecomunicaciones, la globalización y la tecnología avanzan también surgen nuevas formas, modalidades, tipologías de delitos informáticos, así como métodos que los ciberdelincuentes utilizan para realizar ciberataques, o técnicas sofisticadas de ingeniería social. El ciberdelito trasciende fronteras internacionales con la finalidad de ocasionar un perjuicio a los gobiernos nacionales, a las empresas y a la sociedad en general. La interconexión del internet permite que los ciberdelincuentes realicen operaciones ilícitas desde cualquier parte del mundo, no existe lugar, tiempo y espacio.
- El Convenio sobre la Ciberdelincuencia indica que cada Estado parte deberá adoptar las medidas legislativas que les conciernan para establecer los procedimientos penales en la obtención de la prueba electrónica de cualquier delito. Se debe resaltar que en el Estado peruano al igual que en diferentes países que son parte de dicho convenio, la obtención de la prueba electrónica enfrenta desafíos dada su alta evolución tecnológica, así como la falta de una legislación específica en materia de prueba electrónica.
- Los ataques DDoS representan una grave amenaza para la integridad y la estabilidad de los sistemas informáticos y afectan tanto a entidades públicas como privadas. Es importante reconocer que la comisión de este delito no solo vulnera principios de seguridad informática, sino que afecta directamente la seguridad, la estabilidad y la confianza del usuario en el entorno digital.
- La manipulación de datos es un fenómeno complejo debido a que implica acciones deliberadas, ilegítimas, en la alteración de una base de datos. Esta práctica puede ocasionar consecuencias graves como la vulneración de los derechos fundamentales de la persona y daños a la integridad de la información; por ello resulta esencial construir y

fortalecer un marco jurídico de ciberseguridad, este marco legal debe incluir mecanismos de seguridad y protección de la privacidad.

- La suplantación de interfaces de páginas web es un delito complejo, sofisticado, transnacional, en constante evolución, que pone en riesgo la integridad de la información. Se logra evidenciar que mediante técnicas sofisticadas los ciberdelincuentes engañan a las víctimas con el fin de generar perjuicios económicos, en este contexto es importante fortalecer el marco penal peruano para abarcar nuevas formas de fraude informático.

REFERENCIAS

Acurio del Pino, S. (2016). *Delitos informáticos: generalidades.*

Arbulú, V. J. (2015). *Derecho procesal penal. Un enfoque doctrinario y jurisprudencial* (vols. 1-3). Gaceta Jurídica.

Arizaga, J., Chicala, J. y Alvarado, E. (2022). Detección de ataque de DDoS utilizando machine learning - algoritmo de Random Forest. *Serie Científica de la Universidad de las Ciencias Informáticas*, *15*(3), 45-53.

Bequai, A. (1978). *Computer crime*. Lexington Books.

Camacho, L. (1987). *El delito informático*. L. Camacho Losa.

Chirino, A. (2021). Una política criminal informática para América Latina. *Revista Digital de Ciencias Penales de Costa Rica*, *1*(32), 1-23.

Consejo de Europa. (1981). *Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal.*

Consejo de Europa. (1985). *Recomendaciones del Comité n.º R (85) 10: regula el uso de datos personales en el sector policial.*

Consejo de Europa. (1987). *Recomendaciones del Comité n.º R (85) 15: sobre la aplicación práctica del Convenio Europeo sobre Asistencia Judicial en Materia Penal en materia de cartas rogatorias para la interceptación de telecomunicaciones.*

Consejo de Europa. (1989). *Recomendación n.º R (89) 9.*

Consejo de Europa. (1995). *Recomendaciones del Comité n.º R (95) 13: sobre problemas de derecho procesal penal relacionados con la tecnología de la información*.

Davara, M. A. (2015). *Manual de derecho informático* (11.ª ed.). Aranzadi.

Díaz, J. P. (2021). Ingeniería social, un ejemplo práctico. *Revista Odigos*, *2*(3), 47-76. https://doi.org/10.35290/ro.v2n3.2021.493

Espinosa, J. F. (2019). Ciberdelincuencia. Aproximación criminológica de los delitos en la red. *La Razón Histórica: Revista Hispanoamericana de Historia de las Ideas Políticas y Sociales*, (44), 153-173.

Faraldo-Cabana, P. (2007). Los conceptos de manipulación informática y artificio semejante en el delito de estafa informática. *Eguzkilore*, (21), 33-57.

Fernández Calvo, R. (1996). El tratamiento del llamado delito informático en el proyecto de ley orgánica de código penal: reflexiones y propuestas de la CLI (Comisión de Libertades e Informática). *Informática y Derecho: Revista Iberoamericana de Derecho Informático*, (12-15), 1149-1162.

Fernández Delpech, H. (2014). *Manual de derecho informático*. Abeledo Perrot.

Giménez, J. (2006). Delito e informática: algunos aspectos de derecho penal material. *Eguzkilore*, (20), 197-215.

González, J. J. (1999). Protección penal de sistemas, elementos, datos, documentos y programas informáticos. *Revista Electrónica de Ciencia Penal y Criminología*, (1).

Gutiérrez, M. L. (1991). *Fraude informático y estafa (aptitud del tipo de estafa en el derecho español ante las defraudaciones por medios informáticos).* Ministerio de Justicia, Secretaría General Técnica, Centro de Publicaciones.

Gutiérrez, M. L. (1996). El intrusismo informático (hacking): ¿represión penal autónoma? *Informática y Derecho: Revista Iberoamericana de Derecho Informático*, (12-15), 1163-1184.

Hernández, L. (2009). El delito informático. *Eguzkilore: Cuaderno del Instituto Vasco de Criminología*, (23), 227-243.

Instituto Nacional de Estadística e Informática. (2023). *Estadísticas de la criminalidad, seguridad ciudadana y violencia. Una visión desde los registros administrativos abril-junio 2023.* Informe Técnico n.º 03. Setiembre 2023. https://m.inei.gob.pe/media/MenuRecursivo/boletines/boletin_estadisticas_criminilidad.pdf

Jijena, R. J. (1994). La criminalidad informática: situación de lege data y lege ferenda en Chile. *Informática y Derecho: Revista Iberoamericana de Derecho Informático*, (4), 507-513.

Leyva, C. (2019). Estudio de los delitos informáticos y la problemática de su tipificación en el marco de los convenios internacionales. *Lucerna Iuris et Investigatio*, (1), 29-47. https://doi.org/10.15381/lucerna.v0i1.18373

Mayer, L. y Oliver, G. (2020). El delito de fraude informático: concepto y delimitación. *Revista Chilena de Derecho y Tecnología*, *9*(1), 151-184.

Mazuelos, J. (2007). Modelos de imputación en el derecho penal informático. *Derecho Penal y Criminología*, *28*(85), 37-54.

Ministerio Público. (2022). *Boletín Estadístico del Ministerio Público diciembre 2022. Boletín n.º 12.*

Ministerio Público. (2024). *Boletín Estadístico del Ministerio Público. Diciembre 2024. Boletín n.º 12.*

Moreno, P. M., Paucar, C. E. y Cajas, C. M. (2022). Regulación global para evitar la suplantación de identidad digital. *Universidad y Sociedad*, *14*(6), 690-696.

Morillas, D. L. (2017). *Delitos informáticos* [Material de la maestría en Derecho Penal Económico Internacional]. Universidad de Granada.

Morón, E. (2007). Delitos contra la confidencialidad, integridad y disponibilidad de datos y sistemas informáticos. En González, J. J., Mata, N. J. de la, Morón, E., Mata y Martín, R. M., Moreno, J., Morales, F., Viota, M., Ortiz, J. M., Roig, L., Carreras, L., Narváez, A., Sanchís,

C. y Adán, C., *Delito e informática: algunos aspectos* (pp. 85-128). Universidad de Deusto.

Oficina de las Naciones Unidas contra la Droga y el Delito. (2022). *Compendio de ciberdelincuencia organizada.*

Organización de las Naciones Unidas. (1990). *Octavo Congreso de las Naciones Unidas sobre Prevención del Delito y Tratamiento del Delincuente. La cooperación internacional en materia de prevención del delito y justicia penal en el siglo XXI, La Habana, Cuba.*

Palazzi, P. A. (2016). *Los delitos informáticos en el Código Penal: análisis de la Ley 26388* (3.ª ed.). Abeledo Perrot.

Parker, D. B. (1976). *Crime by computer*. Charles Scribner's Sons.

Posada, R. (2017). El cibercrimen y sus efectos en la teoría de la tipicidad: de una realidad física a una realidad virtual. *Nuevo Foro Penal*, *13*(88), 72-112.

Rivera, E. F., Cárdenas, M. P. y Chiriboga, W. A. (2020). Evaluación de ataques DDoS y fuerza bruta utilizando entorno virtual Kali Linux como plataforma experimental [Edición especial]. *Dilemas Contemporáneos: Educación Política y Valores.* https://doi.org/10.46377/dilemas.v35i1.2248

Sain, G. (2018). La estrategia gubernamental frente al cibercrimen: la importancia de las políticas preventivas más allá de la solución penal. En R. A. Parada y J. D. Errecaborde (comps.), *Cibercrimen y delitos informáticos: los nuevos tipos penales en la era de internet* (pp. 7-32). Erreius.

Salom, J. (2011). El ciberespacio y el crimen organizado. *Cuadernos de Estrategia*, (149), 129-164.

Sarzana, C. (1979). Criminalità e tecnologia: il caso dei computer-crimes. *Rassegna Penitenziaria e Criminologica*, (1-2), 53-89.

Sieber, U. (1987). *The international handbook on computer crime: computer-related economic crime and the infringements of privacy*. Wiley.

Téllez, J. (2009). *Derecho informático* (4.ª ed.). McGraw-Hill.

Temperini, M. (2014). *Delitos informáticos en Latinoamérica: un estudio de derecho comparado.* XLIII Jornadas Argentinas de Informática e Investigación Operativa (43JAIIO)-XIV Simposio Argentino de Informática y Derecho (SID) (Buenos Aires, 2014).

Temperini, M. (2018). Delitos informáticos y cibercrimen: alcances, conceptos y características. En R. A. Parada y J. D. Errecaborde (comps.), *Cibercrimen y delitos informáticos: los nuevos tipos penales en la era de internet* (pp. 49-68). Erreius.

Villar, I. M. (2022). El agente encubierto informático: reto legislativo pendiente en un escenario digitalizado. *Revista de Estudios Jurídicos y Criminológicos*, (6), 197-228.

Villavicencio, F. (2006). *Derecho penal: parte general.* Grijley.

Villavicencio, F. (2014). Delitos informáticos. *Ius et Veritas*, *24*(49), 284-304.

Fuentes normativas y jurisprudenciales

Acuerdo Plenario n.º 6-2009/CJ-116. V Pleno Jurisdiccional de las Salas Penales Permanente y Transitorias. Corte Suprema de Justicia de la República (13 de noviembre de 2009).

Convenio sobre la Ciberdelincuencia (23 de noviembre de 2001).

Decreto Legislativo n.º 957. Decreto Legislativo que Promulga el Código Procesal Penal. *Diario Oficial El Peruano* (29 de julio de 2004).

Decreto Legislativo n.º 1591. *Diario Oficial El Peruano* (13 de diciembre de 2023).

Decreto Legislativo n.º 1614. Decreto Legislativo que modifica la Ley n.º 30096, Ley de Delitos Informáticos, para Prevenir y Hacer Frente a la Ciberdelincuencia. *Diario Oficial El Peruano* (21 de diciembre de 2023).

Dictamen a la proposición con punto de acuerdo que solicita información respecto a la adhesión al Convenio de Cibercriminalidad de Budapest (De Poder Legislativo Federal Comisión Permanente; LXII/3SPR-23-1756/56910). (2015).

Ley n.º 27309. Ley que Incorpora los Delitos Informáticos al Código Penal. *Diario Oficial El Peruano* (17 de julio de 2000).

Ley n.º 30076. Ley que modifica el Código Penal, Código Procesal Penal, Código de Ejecución Penal y el Código de los Niños y Adolescentes y crea registros y protocolos con la finalidad de combatir la inseguridad ciudadana. *Diario Oficial El Peruano* (19 de agosto de 2013).

Ley n.º 30096. Ley de Delitos Informáticos. *Diario Oficial El Peruano* (22 de octubre de 2013).

Ley n.º 30171. Ley que Modifica el Artículo 1 de la Ley 29631. *Diario Oficial El Peruano* (10 de marzo de 2014).

Ley n.º 30838. Ley que modifica el Código Penal y el Código de Ejecución Penal para fortalecer la prevención y sanción de los delitos contra la libertad e indemnidad sexuales. *Diario Oficial El Peruano* (4 de agosto de 2018).

Financiamiento
Autofinanciado.

Conflicto de intereses
El autor declara no tener conflicto de intereses.

Contribución de autoría
La etapa de investigación fue desarrollada en su totalidad por el autor y abarcó un proceso riguroso que incluyó la recolección y el análisis de información documental, la interpretación crítica de datos obtenidos y la redacción integral del trabajo.

Agradecimientos
Quiero expresar mi más profundo agradecimiento al equipo editorial de la *Revista Oficial del Poder Judicial*, por su dedicación, su compromiso con la excelencia y su pasión por la difusión del conocimiento, que han hecho posible que cada edición refleje la integridad, el profesionalismo y el rigor que caracterizan a la revista.

Biografía del autor
Félix Andrés Alcalá Molina es abogado, graduado de la Universidad Católica Los Ángeles de Chimbote, egresado de la maestría en Ciencias Penales de la Universidad Nacional Mayor de San Marcos. Con un marcado interés en el estudio de los delitos informáticos. Entre sus contribuciones académicas se encuentra el artículo de investigación titulado «Violencia en el contexto de las nuevas tecnologías de la información: el delito de acoso sexual».

Correspondencia
felix.alcala@unmsm.edu.pe