DELITOS INFORMÁTICOS

Contexto jurídico peruano

Edwin Flores Castillón
Aydee Emérita Quiñones Galindo
Javier Alfredo Condori Amanqui

EDITORIAL TERCER SOL MEXICO

DELITOS INFORMÁTICOS

Contexto jurídico peruano

Edwin Flores Castillón
Aydee Emérita Quiñones Galindo
Javier Alfredo Condori Amanqui

Edwin Flores Castillón

Correo: edwinflocas@gmail.com

ORCID: https://orcid.org/0000-0002-1924-1862

Afiliación: Universidad Andina Néstor Cáceres Velásquez.

Aydee Emérita Quiñones Galindo

Correo: aydegalindo@hotmail.com

ORCID: https://orcid.org/0000-0003-0021-5573

Afiliación: Ministerio Público del Perú.

Javier Alfredo Condori Amanqui

Correo: alfredoamanqui@gmail.com

ORCID: https://orcid.org/0009-0002-8127-7548

Afiliación: Universidad Nacional de Juliaca

Todas nuestras publicaciones son sometidas a revisión doble-ciego
de pares académicos (Peer Review Double Blinded).

ISBN 978-607-59951-3-7

2023
DOI: https://doi.org/10.5281/zenodo.10075830

www.editorialtercersol.com

Este libro es resultado de la investigación *"Tratamiento jurídico de los delitos informáticos en el derecho peruano"*, realizada en la Universidad Andina Néstor Cáceres Velásquez.

Diseño de carátula y composición: Editorial Tercer Sol.

Edición electrónica: Editorial Tercer Sol

Editado en México/ *Published in Mexico*

ÍNDICE

CAPÍTULO III

CAPÍTULO IV

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

PRÓLOGO

En la era digital en la que vivimos, el avance vertiginoso de la tecnología ha traído consigo una serie de desafíos legales, entre ellos, los delitos informáticos. Estos actos ilícitos perpetrados a través de medios electrónicos e informáticos han cobrado una relevancia cada vez mayor, y su combate se ha convertido en una prioridad en el ámbito jurídico peruano.

En este libro, se explora el tratamiento jurídico de los delitos informáticos en el derecho peruano, un tema de gran importancia en la sociedad actual. Pues, a medida que las tecnologías evolucionan y la interconexión digital se extiende, los delincuentes han encontrado nuevas formas de cometer sus fechorías, poniendo en riesgo la seguridad, la privacidad y la integridad de las personas y las organizaciones.

El derecho peruano ha respondido a esta problemática con un marco legal sólido y actualizado por medio de la Ley 30096 en 2013, que busca proteger a los ciudadanos y establecer mecanismos eficientes para la prevención, persecución y sanción de los delitos informáticos. A través de artículos y normativas específicas, se ha creado un marco legal que abarca una amplia gama de caracteres ilícitos en el ámbito digital.

En estas páginas, se examinan las distintas tipificaciones delictivas contempladas en el Código Penal peruano, relacionadas con los delitos informáticos. Desde el acceso no autorizado a sistemas informáticos, pasando por el fraude electrónico, la falsificación de

documentos digitales, el sabotaje informático, hasta el robo de información sensible, entre otros delitos, analizaremos cómo el derecho peruano ha adaptado sus disposiciones para hacer frente a estos desafíos tecnológicos.

Además, se abordan los aspectos procedimentales y penales relacionados con la investigación y persecución de los delitos informáticos. La colaboración entre las autoridades competentes, como la Policía Nacional del Perú y el Ministerio Público, es fundamental para asegurar la eficacia en la persecución de estos delitos y la recolección de pruebas digitales.

No obstante, también se presentan los desafíos que enfrenta el derecho peruano en esta área, como la actualización constante de la legislación frente a la rápida evolución de la tecnología y la necesidad de contar con expertos especializados en la investigación y el análisis forense digital.

De manera que este tema resulta ser apasionante por su constante evolución en el ámbito jurídico peruano: el tratamiento jurídico de los delitos informáticos. A través del análisis de las normas, jurisprudencia y las prácticas judiciales, esperamos brindar una visión clara y concisa sobre cómo el derecho peruano enfrenta estos nuevos desafíos y protege a la sociedad en la era digital, con la certeza de que la información aquí presentada será una herramienta valiosa para entender y abordar los retos y oportunidades que presenta este campo en constante cambio.

INTRODUCCIÓN

En la actualidad, el mundo se encuentra inmerso en una revolución tecnológica que ha transformado profundamente la manera de comunicarse, trabajar, realizar transacciones y compartir información. Sin embargo, junto con los beneficios que brinda la tecnología, también hemos sido testigos de la aparición y proliferación de los delitos informáticos, una nueva forma de criminalidad que ha surgido en el entorno digital.

En este libro se presenta el complejo y revolucionario tema del tratamiento jurídico de los delitos informáticos en el derecho peruano, con el objetivo de brindar una visión completa y actualizada sobre cómo el sistema legal peruano aborda esta problemática que amenaza la seguridad y la confianza en el entorno digital cada año con nuevos métodos de robo.

En las siguientes páginas, analizaremos los conceptos generales, las normas y leyes que han sido promulgadas en Perú para prevenir, investigar y sancionar los delitos informáticos. Exploraremos el Código Penal peruano y otras legislaciones pertinentes, así como la jurisprudencia relacionada, para comprender el alcance de las conductas ilícitas en el ámbito digital y las consecuencias legales que acarrean.

Asimismo, examinaremos las autoridades y organismos encargados de la persecución y prevención de los delitos informáticos en Perú, como la Policía Nacional, el Ministerio Público y el Poder Judicial. Comprenderemos su rol y su coordinación en la investigación, recolección de pruebas y juzgamiento de los casos relacionados con delitos informáticos.

No obstante, también se presentan los desafíos que enfrenta el sistema legal peruano en la lucha contra los delitos informáticos, apoyándonos en una investigación científica *Tratamiento jurídico de los delitos informáticos en el Derecho peruano* del estudioso Edwin Flores. Pues, la rápida evolución tecnológica y las tácticas cada vez más sofisticadas utilizadas por los cibercriminales plantean nuevos retos para las autoridades y los profesionales del derecho, quienes deben mantenerse actualizados y adaptarse constantemente a estos cambios para garantizar una justicia efectiva.

A lo largo de este libro se abordan aspectos prácticos, como la recolección y preservación de evidencia digital, la cooperación internacional en la lucha contra los delitos informáticos y las medidas de seguridad que las organizaciones y los individuos pueden adoptar para protegerse. También se presentan casos reales y ejemplos concretos que ilustran los diferentes tipos de delitos informáticos y la manera cómo han sido abordados en el sistema legal peruano.

Se espera que esta obra contribuya a la difusión del conocimiento sobre este tema crucial y promueva una mayor conciencia sobre la importancia de fortalecer el marco legal y las capacidades institucionales para hacer frente a los delitos informáticos en Perú.

CAPÍTULO I

LOS DELITOS INFORMÁTICOS

En la era digital en la que nos encontramos inmersos, la tecnología ha avanzado de manera vertiginosa, transformando nuestra forma de vida y la manera en que interactuamos con el mundo que nos rodea. Sin embargo, junto con los beneficios y las oportunidades que ofrece, también ha surgido una nueva forma de criminalidad: los delitos informáticos.

Estos nuevos delitos que se han ido haciendo más conocidos con el tiempo, también son llamados ciberdelitos. Son aquellos actos ilícitos que se cometen utilizando medios electrónicos, informáticos o telemáticos, los cuales pueden afectar tanto a personas individuales como a empresas, instituciones y hasta a gobiernos enteros. Desde el acceso no autorizado a sistemas informáticos y la manipulación de datos hasta el robo de identidad y el fraude en línea, los delincuentes informáticos han encontrado en la tecnología un medio propicio para llevar a cabo sus actividades delictivas, llevándolas a un nivel más avanzado y complejo.

En respuesta a esta creciente amenaza, la comunidad internacional ha reconocido la necesidad de adoptar medidas coordinadas y colaborativas para combatir los delitos informáticos a nivel global. Organismos internacionales, como las Naciones Unidas, la Interpol y otros, han promovido la cooperación entre los países para establecer marcos legales y normativos comunes que permitan la persecución y sanción de los delincuentes informáticos. Aunque no se puede cuadrar o clasificar a todos en una definición universal, Pérez y Mezzasalma (2009) mencionan que se trata de responder según la realidad del país porque los delitos informáticos no forman parte de la acción típica de delitos.

A nivel mundial, se han promulgado convenciones y tratados internacionales que buscan armonizar las legislaciones nacionales y promover la cooperación en la lucha contra los diversos delitos informáticos. Estos instrumentos legales buscan fortalecer las capacidades de los países para prevenir, detectar, investigar y enjuiciar los delitos informáticos, así como también fomentar el intercambio de información y la asistencia mutua entre las autoridades competentes.

Sin embargo, los gobiernos han reconocido que las disparidades entre los sistemas jurídicos y la falta de cooperación internacional obstaculizaban la investigación y enjuiciamiento de los delitos cibernéticos. Con base en esta premisa, algunos estudiosos han destacado que los países han debido implementar y adoptar diversas medidas para combatir los delitos informáticos en conjunto. Estas medidas incluyen la promulgación de legislación penal y normas contra el lavado de dinero, la regulación de los cibercafés, campañas de concienciación, el fortalecimiento de los mecanismos para presentar denuncias, la protección de grupos vulnerables, así como la creación de unidades especializadas y la implementación de plataformas interinstitucionales para los organismos encargados de hacer cumplir la ley (Vinelli, 2021).

Por ello, se ha reconocido la importancia de la concientización y la educación en materia de seguridad informática para empoderar a los individuos y a las organizaciones en la protección de sus activos digitales. La prevención y la adopción de buenas prácticas de seguridad cibernética son fundamentales para reducir la vulnerabilidad ante los delitos informáticos y mitigar sus efectos.

De modo que, siguiendo la postura de Vinelli (2021), la concepción restringida de un delito informático se debe limitar a la mera comisión de un delito a través de medios tecnológicos, ya sea *hardware* o *software*; pues, no se debe asumir que constituye automáticamente un delito informático. Se debe tener en cuenta que un delito pueda considerarse como tal, si cumple ciertas características específicas. De lo contrario, estaríamos categorizando erróneamente un delito. Por ejemplo, si una persona realiza declaraciones ofensivas en sus redes sociales, no se podría concluir automáticamente que se ha cometido un delito informático relacionado con el honor.

Aunque, la evolución constante de la tecnología y las nuevas modalidades delictivas presentan un desafío en la lucha contra los delitos informáticos a nivel mundial. Es necesario mantener una vigilancia constante y adaptar las leyes y los mecanismos de cooperación internacional para hacer frente a las nuevas amenazas que surgen en el entorno digital. Asimismo, Muñoz (2010) agrega que debido a este fenómeno se desarrollaron nuevas conductas con respecto al internet porque se volvió una fuente ilícita en todo el mundo, ya que, lo utilizan en parte para hacer daño.

Lo que hace inevitable que Reyna (2016) destaque cómo los riesgos emergentes de naturaleza global están estrechamente relacionados con los impactos de Internet en la estructura social contemporánea. Apoyándose en Zygmunt Bauman, un reconocido sociólogo, resalta el ciberespacio como el factor clave que da forma a una nueva élite

global. Esta élite ya no reside en el «mundo tradicional de la soberanía» con sus fronteras físicas y controles fronterizos que aseguraban la seguridad de los Estados-Nación, sino que opera en un "nuevo espacio global, transnacional y más allá de los límites estatales".

Con respecto al contexto peruano, el derecho que trata los delitos informáticos ha adquirido una importancia significativa que ha requerido de ciertas actualizaciones para la protección de la ciudadanía. Conscientes de los desafíos que plantea la delincuencia cibernética, las autoridades peruanas han promovido la promulgación de leyes y normativas específicas para abordar estos delitos y proteger a la sociedad de sus efectos perniciosos.

Por ello, Hernández (2009) manifiesta que la delincuencia informática forma parte de lo que se conoce como "derecho informático". Este campo abarca el conjunto de normas jurídicas que regulan el uso de los recursos y servicios informáticos en la sociedad. El objeto de estudio del derecho informático incluye diversos aspectos, como el marco legal del software, la regulación de las redes de transmisión de datos, los documentos electrónicos, los contratos electrónicos, el tratamiento jurídico de las bases de datos, la protección de la privacidad, los delitos informáticos y otras conductas surgidas del uso de computadoras y redes de transmisión de datos.

Así pues, el objetivo fundamental del tratamiento jurídico de los delitos informáticos en el derecho peruano es garantizar la seguridad, la integridad y la confianza en el entorno digital. A través de la legislación pertinente, se busca establecer un marco legal sólido que permita la persecución y sanción efectiva de los responsables de estos delitos, así como promover la prevención, la cooperación internacional y la concientización de la sociedad en general sobre los riesgos y las medidas de protección necesarias en el ámbito digital.

Por lo que, en el 2013 se publicó la Ley N° 30096 de la legislación peruana conocida como la "Ley de Delitos Informáticos" que se encarga de combatir los delitos cibernéticos y

proteger la seguridad de la información en el ámbito digital en Perú, los que cometen los delincuentes por la red y atenta la integridad de los datos que proporcionan los usuarios de redes y los mismos sistemas de información que almacenan los datos.

Esta ley establece disposiciones legales para prevenir, investigar y sancionar los delitos informáticos, así como para regular las acciones que afectan la confidencialidad, integridad y disponibilidad de los sistemas y datos informáticos. Algunos de los delitos contemplados en esta legislación son el acceso no autorizado a sistemas informáticos, la interceptación de comunicaciones, el sabotaje informático, el fraude informático, la pornografía infantil en línea, entre otros. Además, esta ley se subdivide en artículos y disposiciones complementarias que tratan de abarcar todos los aspectos posibles para que se puedan procesar debidamente en un determinado plazo de tiempo.

Debido a ello, es necesario destacar que el tratamiento de los delitos informáticos en el derecho peruano está en constante evolución, ya que la tecnología avanza rápidamente y los delincuentes informáticos buscan constantemente nuevas formas de cometer sus fechorías. Por lo tanto, es fundamental que la legislación se mantenga actualizada y se adapte a los cambios tecnológicos y a las nuevas modalidades delictivas que surjan en el entorno digital.

En resumen, el tratamiento jurídico de los delitos informáticos en el derecho peruano busca proteger a la sociedad de los peligros y perjuicios derivados de la actividad delictiva en el ámbito digital. A través de leyes y normativas específicas, se busca combatir la delincuencia cibernética, garantizar la persecución y sanción de los responsables, fomentándose la prevención y la conciencia de los riesgos en el entorno digital.

1.1. La nueva delincuencia: la criminalidad informática

Esta nueva modalidad delictiva apareció a la par de los avances tecnológicos, ya que, sus operaciones delictivas se empezaron a dar desde que los medios electrónicos y las redes de comunicación se hicieron parte de nuestra cotidianidad. Estos delitos pueden incluir una amplia gama de acciones maliciosas, como el robo de información confidencial, el fraude en línea, el acceso no autorizado a sistemas informáticos, el sabotaje informático, el *phishing*, el *malware*, el ciberacoso o *cyberbullying* y otros tipos de delitos cometidos a través de medios electrónicos.

Pero estas actividades se desarrollaron más con la creación de las computadoras que crearon a los denominados hackers, individuos que se especializan en el manejo de la informática. Bramont-Arias (1997) menciona que el continuo desarrollo tecnológico que tienen las diversas naciones se potencia cada vez más por las redes internacionales de comunicación que comparten datos e información en abundancia, esto crea la posibilidad de riesgos y problemas que pueden aprovechar personas inescrupulosas.

Por lo que, la criminalidad informática, también conocida como ciberdelincuencia o delitos informáticos, abarca una amplia gama de delitos, como el acceso no autorizado a sistemas informáticos, el robo de información confidencial, el fraude en línea, la suplantación de identidad, el ciberacoso, el sabotaje informático, la distribución de contenido ilegal, entre otros; que se dan normalmente bajo el manejo de delincuentes con conocimientos avanzados. Además, estos delitos no solo afectan a individuos, sino también a empresas, instituciones y gobiernos, causando daños económicos, violaciones a la privacidad y la seguridad, así como también el compromiso de la integridad de la información.

Los ciberdelincuentes utilizan diversas técnicas y herramientas para llevar a cabo sus actividades ilegales. Pueden explotar vulnerabilidades en sistemas informáticos, enviar

correos electrónicos fraudulentos para engañar a las personas y obtener su información confidencial, o utilizar programas maliciosos para infectar computadoras y robar datos. Lo que representa un desafío para las autoridades y la seguridad cibernética, ya que los ciberdelincuentes suelen operar en un entorno global y pueden ser difíciles de identificar y perseguir. Esto ha llevado al desarrollo de legislación específica y a la cooperación internacional para combatir estos delitos, así como al fortalecimiento de la seguridad de la información, la concientización sobre las buenas prácticas en línea y el desarrollo de tecnologías de seguridad para proteger los sistemas y los datos.

Por ello, vemos constantemente que hay nuevos desafíos para la aplicación de la ley, ya que los delincuentes pueden operar de manera anónima y a menudo traspasan las fronteras nacionales, dificultando su persecución y enjuiciamiento. Asimismo, la rápida evolución tecnológica y las nuevas formas de delito digital requieren una constante actualización de las leyes y la capacitación de los profesionales encargados de combatir esta nueva forma de criminalidad.

Las autoridades, a nivel nacional e internacional, están tomando medidas para enfrentar y prevenir la criminalidad informática, lo que se ha vuelto un reto y ha creado una nueva división entre las personas sobre ser el criminal o la víctima. Debido a ello, se promulgan leyes y regulaciones específicas, se establecen unidades especializadas en las fuerzas del orden y se fomenta la cooperación internacional para intercambiar información, recopilar pruebas y llevar a los delincuentes ante la justicia.

1.1.1. El delito informático como reto

El delito informático es una realidad presente en el mundo digital actual que se ha convertido en un reto significativo para las autoridades y la sociedad en general. A medida que la tecnología continúa avanzando y la interconexión digital se expande, los delincuentes han

encontrado nuevas oportunidades para cometer actos ilícitos en el ámbito cibernético. Su alcance y gravedad exigen respuestas efectivas tanto a nivel legal como tecnológico.

Por ello, este tipo de delito presenta desafíos únicos que ha motivado la necesidad de acudir al derecho penal en todos los países que cuentan con la tecnología para su desarrollo. Pues, los delincuentes informáticos pueden operar de manera global y anónima, traspasando las fronteras nacionales, dificultando su identificación y captura. Además, los métodos utilizados por estos delincuentes son cada vez más sofisticados, lo que requiere una constante actualización y adaptación de las leyes y los sistemas de seguridad.

Uno de los mayores retos en la lucha contra el delito informático es la capacidad de las autoridades para mantenerse al día con las últimas tendencias y técnicas utilizadas por los delincuentes. Esto implica la necesidad de contar con expertos en seguridad cibernética, investigadores capacitados y herramientas tecnológicas avanzadas para detectar, investigar y prevenir estos delitos. Pero, si se parte desde términos generales, Bramont-Arias (1997) propone que se puede analizar este fenómeno desde dos perspectivas:

a. **Los delitos patrimoniales** dirigidos contra el sistema informático se refieren a conductas delictivas donde el objetivo principal es el ataque al soporte informático, incluyendo tanto el hardware como los componentes lógicos del software.

b. **Los delitos que se cometen a través del sistema informático**, es decir, utilizando este como una herramienta que facilita, asegura o agrava los efectos de otros delitos tradicionales. En estos casos, el sistema informático se convierte en un instrumento utilizado por los delincuentes para llevar a cabo actividades ilícitas

Con ello se sustenta que es necesario, para combatir este desafío, que haya una colaboración y cooperación entre diferentes países y jurisdicciones. Dado que el delito informático

trasciende las fronteras nacionales, es fundamental establecer mecanismos efectivos de intercambio de información, asistencia mutua y coordinación entre las autoridades de diferentes países.

Además, la concientización y la educación de la sociedad en general juegan un papel crucial en la prevención del delito informático. Es esencial que las personas estén informadas sobre las posibles amenazas en línea para que adopten medidas de seguridad adecuadas y estén alerta ante posibles actividades delictivas.

Una serie de retos que encontramos a nivel individual e institucional que provoca el delito informático son:

1. **Complejidad tecnológica:** Los avances tecnológicos constantes brindan a los ciberdelincuentes nuevas herramientas y técnicas para llevar a cabo sus actividades delictivas. Esto dificulta la detección y prevención de los delitos informáticos, así como la identificación de los perpetradores.

2. **Carácter transnacional:** El delito informático no conoce fronteras y puede ser perpetrado desde cualquier parte del mundo hacia cualquier otro lugar. Esto complica la cooperación y la coordinación entre diferentes jurisdicciones para investigar y enjuiciar a los delincuentes informáticos.

3. **Anonimato y dificultad para atribuir responsabilidades:** Los delincuentes informáticos pueden ocultar su identidad y utilizar técnicas de ocultamiento para evitar ser rastreados. Esto dificulta la atribución de responsabilidades y la persecución legal de los delincuentes.

4. **Escala y alcance masivo:** Los delitos informáticos pueden afectar a un gran número de personas o instituciones de manera simultánea. Los ataques de *ransomware*, por ejemplo, pueden paralizar sistemas informáticos y causar daños a gran escala.

5. **Vulnerabilidades y desafíos de seguridad:** A medida que aumenta la dependencia de la tecnología, también aumentan las vulnerabilidades y los desafíos de seguridad. Los delincuentes informáticos aprovechan estas debilidades para acceder a sistemas y datos sensibles.

6. **Falta de concienciación y educación**: Muchas personas y organizaciones carecen de una comprensión adecuada de los riesgos y las mejores prácticas de seguridad cibernética. La falta de concienciación y educación en este sentido facilita el éxito de los ataques informáticos.

7. **Costos económicos y daños a la reputación**: Los delitos informáticos pueden tener un alto costo económico para las víctimas, ya sea a través de la pérdida de datos, el robo de información financiera o el impacto en la continuidad del negocio. Además, estos delitos pueden dañar la reputación de una organización o individuo.

Enfrentar estos retos requiere una combinación de medidas legales, tecnológicas y de concienciación. Esto incluye la implementación de legislación actualizada, la mejora de las medidas de seguridad cibernética, la cooperación internacional, la educación sobre seguridad en línea y la concienciación general sobre los riesgos y las mejores prácticas en el uso de la tecnología.

El delito informático como un reto requiere un enfoque integral que abarque la legislación adecuada, la capacitación de profesionales especializados, la colaboración internacional y

la concientización de la sociedad. Solo a través de un esfuerzo conjunto y continuo será posible hacer frente a este desafío y garantizar un entorno digital seguro y protegido.

1.1.2. El criminal informático y la víctima

En la sociedad se han creado distintos estereotipos como producto de los diversos eventos que suceden con recurrencia, debido a ello encontramos dos roles fundamentales en los delitos informáticos: el criminal informático y la víctima. Estas dos posiciones surgieron frente a los delitos que debían ser representados por dos posiciones que se interrelacionan por el mismo deseo de tener algo. Por lo que, son una relación dependiente que se complementa de manera violenta porque hay un sujeto perjudicado.

El delincuente informático, también conocido como ciberdelincuente o hacker malintencionado, es aquel individuo o grupo que lleva a cabo actividades delictivas en el ámbito digital. Estas personas aprovechan las vulnerabilidades de los sistemas informáticos, las redes de comunicación y los dispositivos electrónicos para cometer una variedad de delitos, como el acceso no autorizado, el robo de datos, el fraude en línea, la distribución de *malware* y muchos otros.

Los criminales informáticos utilizan una amplia gama de técnicas y herramientas para llevar a cabo sus delitos. Esto puede incluir el uso de *malware*, el *phishing*, el *hacking* de sistemas, el robo de datos, el sabotaje informático, entre otros métodos. Su intención es aprovechar las vulnerabilidades en la seguridad de sistemas y redes para obtener acceso no autorizado, causar daño o robar información valiosa.

Bramont-Arias (1997) menciona que no es necesario que el delincuente sea una mente maestra especialista de la informática o personas con gran inteligencia. Pero, no se puede

negar que en la actualidad hay delincuentes profesionales dentro de este ámbito que trabajan en una red de crimen organizado, posiblemente parte del espionaje internacional.

Pero, Pérez y Mezzasalma (2009) proponen que en esta forma de delincuencia se involucra como criminales a expertos altamente capacitados en cometer el delito y eliminar cualquier rastro de evidencia, lo que dificulta o incluso imposibilita su investigación; se diferencia de los demás delincuentes. Pues, poseen destrezas en el ámbito de la informática y, por lo general, debido a su posición laboral, se encuentran en lugares estratégicos donde tienen acceso fácil a la información.

Las actividades delictivas de los criminales informáticos pueden tener graves consecuencias, como la pérdida de datos, el robo de identidad, el fraude financiero, el sabotaje de sistemas y el daño a la reputación de personas o empresas. Combatir y prevenir la actividad de los criminales informáticos requiere esfuerzos continuos en materia de legislación, seguridad cibernética, educación y cooperación internacional.

Las víctimas en los delitos informáticos son aquellos sujetos pasivos que sufren las consecuencias negativas de la actividad delictiva. Las víctimas pueden ser individuos particulares, empresas, organizaciones gubernamentales o incluso gobiernos enteros.

Convencionalmente, Pérez y Mezzasalma (2009) sustenta el concepto tradicional de que la víctima es un sujeto pasivo, quien sufre las consecuencias de la conducta y acciones que realiza el delincuente como sujeto activo. Además, la víctima está predispuesta a ser atacada según las características que tenga o como se le identifique (personas, instituciones, gobiernos, etc.), por los sistemas que generalmente utilizan y están conectados a otros.

Aunque, Bramont-Arias (1997) asume que debe haber un sentido de la autorresponsabilidad en la víctima. Ya que, las empresas, en el marco del desarrollo continuo de la sociedad

en una economía de mercado, tienen como objetivo llegar al público con sus productos o servicios. En este sentido, las computadoras se convierten en herramientas clave que facilitan y aceleran este proceso. Debido a esta dependencia en el uso de tecnología, las empresas se convierten en víctimas frecuentes de los delitos informáticos, especialmente aquellas que cuentan con un cierto potencial económico. Esta característica se alinea con las características propias de la delincuencia de cuello blanco o socioeconómica, a la cual también pertenece la delincuencia informática.

Las víctimas de delitos informáticos pueden experimentar diversas consecuencias negativas, que pueden incluir:

1. **Pérdida económica**: Los delincuentes informáticos pueden robar información financiera, como números de tarjetas de crédito o contraseñas de cuentas bancarias, y utilizarla para realizar transacciones fraudulentas o vaciar cuentas bancarias. Esto puede provocar pérdidas económicas significativas para las víctimas.

2. **Falsificación de identidad**: Mediante técnicas de *phishing*, *malware* u otros métodos, los delincuentes informáticos pueden obtener información personal de las víctimas, como nombres, direcciones, números de seguridad social, entre otros. Esta información se utiliza para cometer fraudes o suplantar la identidad de las víctimas.

3. **Daño a la reputación**: Los delitos informáticos pueden tener un impacto negativo en la reputación de individuos o empresas. Por ejemplo, la publicación de información sensible o comprometedora en línea puede dañar la imagen de una persona, mientras que el acceso no autorizado a sistemas empresariales puede resultar en la divulgación de información confidencial o en la pérdida de la confianza de los clientes.

4. **Pérdida de datos**: El acceso no autorizado o el ataque de *ransomware* pueden llevar a la pérdida o bloqueo de datos importantes para individuos o empresas. Esto puede tener consecuencias graves, como la interrupción de operaciones comerciales, la pérdida de información valiosa o la violación de la privacidad de las personas.

5. **Impacto emocional y personal**: Ser víctima de un delito informático puede causar estrés, ansiedad y angustia emocional. Las víctimas pueden sentirse vulneradas en su privacidad, violadas en su intimidad y pueden experimentar un sentimiento de violación de su seguridad personal.

Es importante recalcar que las víctimas de delitos informáticos pueden ser tanto individuos como empresas de cualquier tamaño. Por ello, es importante tener en cuenta que las víctimas de delitos informáticos pueden variar ampliamente, desde usuarios comunes de Internet hasta grandes corporaciones. Además, las consecuencias para las víctimas pueden ser significativas y duraderas, afectando tanto su bienestar personal como su estabilidad financiera, o incluso la seguridad nacional en el caso de ataques cibernéticos a gran escala.

1.2. Aspectos político-criminales en los delitos informáticos

El fenómeno informático ha generado tantos beneficios como desafíos. Por un lado, ha facilitado el acceso a la información, la globalización de los negocios, la mejora de la eficiencia en los procesos y el avance en la investigación científica. Por otro lado, también ha planteado preocupaciones sobre la privacidad, la seguridad de la información, la brecha digital y el impacto en el empleo y la desigualdad.

Esto se debe a la recopilación y el uso indebido de la información personal, así como los ciberataques y el robo de datos, estos delitos plantean riesgos significativos para la privacidad y la seguridad de los individuos y las organizaciones. Los delitos que encontramos en este

fenómeno representan una amenaza para la seguridad y pueden causar daños económicos y emocionales a las personas afectadas. Por ello, Bramont-Arias (1997) destaca los siguientes aspectos, los cuales le dan un aspecto criminológico:

a. La información que se encuentra almacenada en las computadoras vienen a tener un significado de poder. La informática amplifica el poder de aquellos que utilizan la información, sin embargo, simultáneamente genera y aumenta las desigualdades, y cuestiona los derechos y garantías individuales que deben existir en un Estado que se considera social y democrático bajo el imperio de la ley.

b. En general, la comisión de delitos informáticos se detecta que las víctimas resultan ser una persona jurídica, pero no presentan la respectiva denuncia debido a la mala imagen que les puede dar.

c. Tiene graves consecuencias económicas para la víctima. Sin embargo, las denuncias con las que se procede tienen la finalidad de privar la libertad al delincuente y, por otro lado, encender las alarmas de los demás ciudadanos para que tomen precauciones.

Debido a ello, los aspectos político-criminales en los delitos informáticos se refieren a las implicaciones políticas y criminológicas asociadas a este tipo de delitos. Pues, estos aspectos involucran tanto los desafíos que enfrentan las autoridades y los sistemas de justicia en la persecución y prevención de los delitos informáticos, como las respuestas políticas y legislativas que se requieren para abordar eficazmente esta forma de criminalidad.

En primer lugar, los delitos informáticos presentan desafíos significativos para las autoridades y los sistemas de justicia, por su naturaleza transnacional y la capacidad de los delincuentes informáticos para operar de manera anónima y remota; de este modo se dificulta su identificación, persecución y enjuiciamiento. Además, la rápida evolución

tecnológica y la sofisticación de las técnicas utilizadas por los delincuentes requieren que las autoridades estén constantemente actualizadas y capacitadas en seguridad cibernética.

En segundo lugar, los delitos informáticos también plantean interrogantes políticas y criminológicas relacionadas con la legislación y las políticas públicas. Es fundamental contar con marcos legales sólidos y actualizados que aborden de manera adecuada los delitos informáticos, estableciendo definiciones claras, tipificaciones precisas y sanciones proporcionales. Además, se requiere una cooperación y coordinación efectiva entre los diferentes actores, tanto a nivel nacional como internacional, para combatir de manera eficaz esta forma de criminalidad.

Por ello, González (2007) sugiere que en relación con la intervención penal en internet y las redes de transmisión de datos, existen actualmente dos enfoques diferentes. Por un lado, hay quienes defienden la incorporación de nuevos bienes jurídicos en la protección penal, los cuales han surgido como consecuencia de la generalización y consolidación de los medios y procedimientos informáticos. Estos bienes jurídicos serían considerados lo suficientemente importantes como para justificar la intervención penal. Esta postura parte de la premisa implícita de que las disposiciones penales existentes actualmente resultan insuficientes para abordar los problemas y desafíos que presenta Internet y las redes de transmisión de datos. Por otro lado, existe un sector que aboga por agotar las posibilidades de protección que ofrece el marco legal vigente, basándose en los bienes jurídicos "tradicionales". Esto implica utilizar las normas penales existentes para abordar los delitos informáticos, sin perjuicio de realizar las modificaciones concretas necesarias cuando sea preciso.

Asimismo, los aspectos político-criminales también implican el análisis de las causas y los factores que contribuyen al surgimiento y la expansión de los delitos informáticos. Esto

implica examinar los aspectos socioeconómicos, culturales y tecnológicos que pueden influir en la aparición de estos delitos, así como las motivaciones y las oportunidades que encuentran los delincuentes en el entorno digital.

Los aspectos político-criminales en los delitos informáticos abarcan los desafíos que enfrentan las autoridades y los sistemas de justicia, así como las respuestas políticas y legislativas necesarias para abordar esta forma de criminalidad. Es fundamental contar con marcos legales actualizados, capacitar a los profesionales en seguridad cibernética y promover la cooperación internacional para hacer frente de manera efectiva a los delitos informáticos. Además, se debe analizar a fondo las causas y los factores que contribuyen a la aparición de estos delitos en el entorno digital, debido a ello, se encuentran la manera de tipificar estos delitos según su clasificación y las características. Para ello, nos basaremos en los criterios de dos estudiosos: Lima (1984) y Téllez (1996).

1.2.1. Clasificación de delitos informáticos

Téllez (1996) los clasifica en base a dos criterios:

I. **Como instrumento o medio**: las conductas criminales que dependen de las computadoras como medio del trabajo ilícito (Ej: falsificación de documento vía computarizada: tarjetas de créditos, cheques, etc.).

II. **Como fin u objetivo**: las conductas criminales que van dirigidas en contra de los recursos que tiene una entidad física (Ej: secuestro de soportes magnéticos con información valiosa, para ser utilizadas con fines delictivos).

Lima (1984) presenta la siguiente clasificación de "delitos electrónicos":

I. **Como método**: Son las conductas criminales en donde los individuos utilizan métodos electrónicos para hacer cosas ilícitas.

II. **Como medio**: Se refiere a las conductas criminales en donde para realizar un delito utilizan una computadora como medio de comunicación.

III. **Como fin**: Las conductas criminales dirigidas contra la víctima es dañarla y perjudicarla profundamente.

1.2.2. Características de delitos informáticos

Téllez Valdez sostiene las siguientes características:

I. Solo determina la cantidad de personas con conocimientos técnicos específicos pueden llegar a cometerlos.

II. Son conductas criminales del tipo "cuello blanco", en cuanto al sujeto que los comete atento que generalmente los comete alguien con cierto *status* socioeconómico no vinculado con la pobreza.

III. Generalmente se realizan cuando la víctima está trabajando.

IV. Provocan pérdidas bancarias y daño emocional.

V. Hay una gran cantidad de casos y pocas denuncias por la falta de regulación. Incluso, se supone que no hay denuncias por el miedo al descrédito de la entidad atacada.

VI. Son difíciles de demostrar.

Sin embargo, a raíz de la pandemia del COVID-19 hubo un impacto importante en la ciberdelincuencia. Con el aumento del uso de la tecnología y la dependencia de las plataformas digitales durante el confinamiento y el distanciamiento social, los ciberdelincuentes han aprovechado esta situación para llevar a cabo ataques y estafas relacionadas en mayor escala. Esto se refuerza en el estudio de Gutiérrez-Oquendo (2023) que fundamenta como la ciberdelincuencia se da a nivel nacional e internacional, por ello resulta alarmante que este tipo de criminalidad está experimentando un crecimiento exponencial y alarmante. Ya que, su principal objetivo es económico por lo fácil que resulta hacer los robos de cuentas. En consecuencia, se tienen cifras altas de víctimas y, a su vez, una gran variedad de tipos de delitos informáticos.

CAPÍTULO II

TIPOS DE DELITOS INFORMÁTICOS EN EL DERECHO PERUANO

Desde que la OCDE publicó en 1986 un informe sobre los "Delitos de Informática: análisis de la normativa jurídica", se mencionaban las leyes existentes y las propuestas de reforma en diferentes países, y se sugería una lista mínima de ejemplos de actividades indebidas que los países podrían prohibir y penalizar en sus leyes penales (Lista Mínima). Estos ejemplos incluyen el fraude y la falsificación informática, la manipulación de datos y programas de computadora, el sabotaje informático, el acceso no autorizado, la interceptación no autorizada y la reproducción no autorizada de programas de computadora protegidos (Acurio, s.f.).

A partir de ello comenzaron a surgir listas sobre la utilización indebida que no era autorizada en el uso de computadoras o programas protegidos. Incluso, se empieza a tomar en consideración el Manual de las Naciones Unidas para la prevención y control de delitos informáticos que buscaba advertir sobre la problemática mayor cuando los delitos son inconvenientes en escala internacional, al constituir una forma de crimen trasnacional.

Pues, para Acurio (s.f.), tanto los terroristas como las Organizaciones Delictivas Transnacionales están aprovechando los avances tecnológicos para llevar a cabo sus actividades delictivas utilizando las redes de telecomunicaciones como medio de expansión. Por lo que, es fundamental que los organismos encargados de controlar estas conductas perjudiciales tomen medidas para detener esta situación. Lo que hace necesario que la acción y medidas para tener en cuenta no se limiten a nivel local, sino que se promueva la cooperación tanto a nivel interinstitucional como internacional en este ámbito informático.

De esta manera es más fácil identificar las acciones del criminal cibernético o hacker porque se configura una base de datos que los identifica. Aunque, Pajuelo (2010) advierte que esto podría generar confusiones para que se configuren estos delitos contra el patrimonio, por la ambigüedad que pueda haber entre las acciones de los sujetos activos (criminal) y pasivos (víctima).

Bramont-Arias (1997) sustenta que desde el inicio no ha habido una definición apropiada para el concepto de delito informático que sea aceptada en su totalidad por el derecho penal, lo que también ha dificultado comprender los comportamientos delictivos y reducirlos a un grupo. Esto demuestra el complejo proceso por el que se trata de desvincular los delitos para no confundir las relaciones entre las características delictivas que comparten.

A pesar de ello, en el derecho peruano existen diversos tipos de delitos informáticos tipificados en la legislación para combatir la problemática que aqueja a los ciudadanos y entidades que sufren diversas situaciones de atentado cibernético. Un delito se configura en relación con una causa que tiene efectos negativos (engañar, perjudicar o robar). Por lo que, Bramont-Arias (1997) expone que se debe analizar cada elemento de la estafa para poder comprobar si estos son aplicables al delito informático:

a. El estafador manipula y engaña a la víctima para que esta le de los bienes que pretenden ser robados.

b. Hay un error que se refiere al falso conocimiento de la realidad, o sea, se trata de un engaño que ciega a la víctima para que esta disponga de su patrimonio y sea perjudicada.

c. La víctima entrega voluntariamente su patrimonio debido al engaño y error, sumándole la conducta engañosa del sujeto activo (criminal).

d. La disposición de bien provoca un perjuicio económico en la víctima o en segundas personas que dependen de es bien patrimonial, ya que la estafa atenta al patrimonio.

En consecuencia, la legislación peruana ha tenido que modificar constantemente el Código Penal peruano con los delitos informáticos para adaptarse a los avances tecnológicos y las nuevas formas de delincuencia cibernética. La última versión que se tiene es la del año 2013, pues se introdujo una importante modificación al Código Penal peruano con la promulgación de la Ley N° 30096. Esta ley amplió y actualizó el catálogo de delitos informáticos y sus sanciones, con el fin de enfrentar de manera más efectiva la ciberdelincuencia. Además, se establecieron disposiciones específicas para la protección de los datos personales y la privacidad en el ámbito digital.

Los delitos informáticos más relevantes en el marco legal peruano son los siguientes:

2.1. Acceso indebido a sistemas o datos informáticos

Este delito se refiere generalmente a la acción de acceder a sistemas, redes o datos informáticos sin la autorización o permiso adecuado, violándose el derecho a la privacidad. Prácticamente, este delito consiste en vulnerar las medidas de seguridad y entrar de manera no autorizada a sistemas o datos protegidos. Lo que puede implicar el uso de técnicas

como la violación de contraseñas, el aprovechamiento de vulnerabilidades en el sistema, el uso de credenciales de acceso robadas o cualquier otra acción de ingreso no autorizado.

Este delito puede tener diversas intenciones, como el robo de información confidencial, la obtención de datos personales, el sabotaje o alteración de sistemas, el espionaje industrial o el daño a la reputación de una persona o empresa. Según Acurio (s.f.), se divide en los siguientes métodos:

2.1.1. Las puertas falsas (Trap Doors):

Son funcionalidades ocultas o puertas traseras creadas intencionalmente en un sistema informático o *software*. Estas puertas falsas suelen ser desarrolladas por los propios creadores del sistema con el propósito de acceder de manera no autorizada a la información o funciones del sistema, sin que los usuarios legítimos o los administradores del sistema sean conscientes de su existencia. Asimismo, Acurio (s.f.) refiere que este método es la práctica de emplear interrupciones en la lógica de los programas, con el fin de espiar el proceso complejo para saber si los resultados son correctos.

2.1.2. La llave maestra (Superzapping):

Se trata de un programa de infiltración que es capaz de poder abrir cualquier archivo, así esté protegido, con la capacidad de otorgar el poder para realizar cambios en la estructura de la base de datos, así como para acceder, modificar o eliminar cualquier dato almacenado en ella, sin importar las restricciones o permisos de acceso establecidos para los usuarios regulares del sistema. Esto incluye la capacidad de eludir los mecanismos de seguridad y auditoría implementados, lo que representa un riesgo considerable para la integridad y confidencialidad de los datos.

2.1.3. Pinchado de líneas (Wiretapping):

Se refiere a la práctica de interceptar de manera ilegal las comunicaciones telefónicas o electrónicas de una persona sin su consentimiento o sin una autorización legal. Esta acción consiste en escuchar, grabar o monitorear conversaciones privadas a través de la intervención en las líneas de comunicación, como cables telefónicos, redes telefónicas o sistemas de comunicación electrónica. Además, Acurio (s.f.) también postula que consiste en recuperar información que queda circulando por las líneas telefónicas.

2.1.4. Piratas informáticos (hackers):

Los hackers son individuos expertos en el ámbito de la informática y la seguridad informática. Sin embargo, se puede tener diferentes connotaciones según el significado del contexto. En general se pueden identificar tres tipos especiales de hacker:

1. **Hackers éticos (*white-hat hackers*)**: Son expertos en seguridad informática que utilizan sus habilidades para identificar y solucionar vulnerabilidades en sistemas y redes. Su objetivo es mejorar la seguridad y protección de los sistemas informáticos y colaborar con empresas o instituciones para prevenir ataques cibernéticos.

2. **Hackers maliciosos (*black-hat hackers*)**: Son individuos que utilizan sus habilidades en informática con fines maliciosos. Su objetivo es obtener acceso no autorizado a sistemas, robar información confidencial, causar daños o cometer actividades ilegales en línea. Estos hackers son considerados delincuentes cibernéticos.

3. **Hackers éticos con motivaciones grises (*gray-hat hackers*)**: Este tipo de hackers tienen un enfoque intermedio entre los hackers éticos y los hackers maliciosos. Si bien pueden utilizar sus habilidades para identificar vulnerabilidades y notificar a los

propietarios de los sistemas, a menudo lo hacen sin su consentimiento y con intenciones de obtener reconocimiento o beneficios personales.

En muchos países, incluido Perú, el acceso indebido a sistemas o datos informáticos se encuentra tipificado como un delito en la legislación correspondiente, y puede acarrear sanciones legales, como multas y penas de prisión, dependiendo de la gravedad del caso y las leyes aplicables. Este delito se encuentra tipificado en el artículo 207-A del Código Penal Peruano.

Es importante destacar que el acceso indebido a sistemas o datos informáticos es una violación de la privacidad y la seguridad, se considera un acto ilegal y perjudicial. Para prevenir este tipo de delito, es esencial mantener medidas de seguridad adecuadas, como el uso de contraseñas fuertes, la actualización de software y sistemas, y la protección de datos sensibles.

2.2. Daños informáticos

Los daños informáticos se refieren a las acciones maliciosas o perjudiciales realizadas en sistemas informáticos, redes o dispositivos, que causan un perjuicio o afectación en su funcionamiento, integridad o disponibilidad. Estos daños pueden ser intencionales o accidentales, los cuales pueden ser realizados por ciberdelincuentes, empleados negligentes o cualquier persona que interactúe con sistemas informáticos de manera inapropiada. Ya que, según Robles et al. (2016), estos delitos son considerados de alta tecnología, lo que diferenciaría al cibercriminal de los demás delincuentes promedios, debido al manejo de computadoras y programas a través del mundo virtual de internet que requiere de un conocimiento específico. A todo ello, se debe tener en cuenta que los cibercriminales tienen la facilidad de actuar por la falta de conocimientos de las personas comunes, para resguardar sus ordenadores y operaciones financieras.

Los daños informáticos pueden manifestarse de diversas formas, incluyendo:

1. **Alteración de datos**: Consiste en modificar, borrar o corromper datos almacenados en sistemas informáticos, lo que puede llevar a la pérdida o manipulación de información importante o sensible.

2. **Destrucción de sistemas**: Implica causar daño físico o lógico a los sistemas informáticos, ya sea a través de la eliminación de archivos o programas esenciales, la sobrecarga de los recursos del sistema o la manipulación de configuraciones clave.

3. **Interferencia en el funcionamiento**: Se refiere a acciones que interrumpen o afectan el funcionamiento normal de los sistemas informáticos, como ataques de denegación de servicio (DoS), que inundan los recursos del sistema para hacerlo inaccesible para los usuarios legítimos.

4. **Deterioro de la disponibilidad**: Consiste en acciones que limitan o impiden el acceso legítimo a los sistemas informáticos, ya sea bloqueando el acceso o tomando el control de los mismos.

Estas transgresiones pueden tener consecuencias significativas, tanto para individuos como para organizaciones. Estas consecuencias pueden incluir pérdida de datos, interrupción de servicios, costos financieros, daño a la reputación y violación de la privacidad.

En muchos países, los daños informáticos están tipificados como delitos y son penalizados por la legislación correspondiente. En Perú, el artículo 207-C del Código Penal peruano se encarga de contemplar este delito. Además, según Bramont-Arias (1997), el mismo comportamiento que daña el patrimonio de las víctimas, justifica que se puedan sancionar penalmente dichas conductas.

2.3. Interceptación y/o captación de datos

Se refiere a la acción de obtener, sin autorización, información o datos que están siendo transmitidos a través de medios electrónicos o sistemas de comunicación. Esta actividad consiste en acceder ilegalmente a la comunicación electrónica de terceros con el fin de obtener información exclusiva o íntima. Asimismo, Villavicencio (2014) manifiesta que la naturaleza de este delito es de peligro abstracto, lo que significa que basta con demostrar la acción de interceptar los datos para considerar el delito consumado. Por lo tanto, se trata de un delito de mera actividad, ya que la simple acción de interceptar datos informáticos es suficiente para que se considere consumado el delito.

La interceptación y/o captación de datos puede llevarse a cabo de diferentes formas:

1. **Escuchas telefónicas**: Consiste en intervenir y grabar comunicaciones telefónicas sin el consentimiento de las partes involucradas.

2. **Intercepción de correos electrónicos**: Implica acceder y leer correos electrónicos privados que no están destinados al receptor.

3. **Monitoreo de comunicaciones en redes**: Se refiere a la interceptación de datos transmitidos a través de redes informáticas, como el acceso no autorizado a conversaciones en redes sociales, servicios de mensajería instantánea o chats en línea.

4. **Captación de tráfico de red**: Consiste en el análisis y obtención de datos que viajan a través de una red, como contraseñas, información personal o datos confidenciales.

Este método es considerado un delito en muchos sistemas jurídicos, ya que viola la privacidad y la confidencialidad de las comunicaciones. Las leyes de diferentes países establecen regulaciones y sanciones para combatir este tipo de actividad y proteger los

derechos individuales. En el caso de Perú, este delito se encuentra tipificado en el artículo 207-B del Código Penal.

Es importante destacar que existen casos en los que la interceptación y/o captación de datos puede ser legal y estar sujeta a ciertos requisitos, como en investigaciones criminales llevadas a cabo por autoridades competentes y bajo el marco legal establecido. Sin embargo, en la mayoría de los casos, la interceptación y/o captación de datos sin autorización es considerada una violación a la privacidad y es penalizada por la ley.

2.4. Sabotaje informático

Se refiere a la acción intencional de dañar, alterar, interrumpir o destruir sistemas informáticos o redes de computadoras. En Perú, el artículo 207-D del Código Penal lo establece como delito de fraude informático. Este delito se refiere a la obtención de beneficios económicos mediante el uso de medios. No obstante, Robles, F. et al. (2016) mencionan que, al examinar detenidamente el Código Penal peruano, podemos observar múltiples delitos tipificados que incorporan o podrían incluir la utilización de medios electrónicos o informáticos en su comisión. La distinción conceptual se centra en el bien jurídico principal protegido, ya que, mientras que en los delitos informáticos se protege principalmente la información, en los delitos computacionales el bien jurídico protegido puede abarcar cualquier otro aspecto.

Existen varias formas de sabotaje informático, incluyendo:

1. **Ataques de denegación de servicio (DoS)**: Consisten en inundar un sistema o red con una gran cantidad de tráfico o solicitudes, lo que provoca que se vuelva inaccesible para los usuarios legítimos.

2. ***Malware***: Los programas maliciosos, como virus, gusanos, troyanos o *ransomware*, se utilizan para infectar sistemas y causar daños o robar información.

3. **Ataques de ingeniería social**: En lugar de aprovechar vulnerabilidades técnicas, estos ataques se basan en manipular a las personas para obtener acceso no autorizado a sistemas o información confidencial.

4. **Manipulación de datos**: Consiste en modificar, borrar o corromper información almacenada en sistemas informáticos, lo que puede causar daños operativos o financieros.

5. ***Hacking* ético**: Aunque no se considera sabotaje informático en sí mismo, el hacking ético implica encontrar y exponer vulnerabilidades en sistemas informáticos con el fin de mejorar su seguridad.

Es importante destacar que el sabotaje informático es ilegal en todas las naciones y puede tener graves consecuencias legales para quienes lo lleven a cabo. En muchos países, existen leyes específicas para proteger los sistemas informáticos y castigar a los infractores.

2.5. Suplantación de identidad

La suplantación de identidad, también conocida como "usurpación de identidad" o "robo de identidad", es un delito en el cual una persona se hace pasar por otra, asumiendo su identidad con el propósito de cometer fraude, obtener beneficios económicos o llevar a cabo actividades ilegales. En Perú es considerado como un delito grave que se encuentra tipificado en el artículo 207-E del Código Penal peruano, por los cargos de creación, uso o distribución de programas informáticos falsificados o adulterados con el objetivo de cometer fraudes, estafas u otros delitos. Según Bramont-Arias (1997), este delito empezó a

raíz del robo de documentos que representaban la identidad de las personas y tenía eficacia en el ámbito del tráfico jurídico.

La suplantación de identidad puede ocurrir de varias formas, incluyendo:

1. **Robo de información personal:** Los delincuentes pueden obtener acceso a información personal de una persona, como nombres, direcciones, números de seguro social, números de tarjetas de crédito, entre otros, y utilizar esa información para hacerse pasar por la víctima.

2. ***Phishing***: Esta técnica consiste en enviar correos electrónicos, mensajes de texto o realizar llamadas telefónicas fraudulentas que aparentan ser de empresas legítimas, solicitando a la víctima que proporcione información personal, como contraseñas o números de cuenta bancaria.

3. **Tarjetas de crédito falsas**: Los delincuentes pueden crear tarjetas de crédito falsificadas utilizando la información de otra persona, realizando compras o extracciones de dinero en nombre de la víctima.

4. **Suplantación en línea**: Los delincuentes pueden crear perfiles falsos en redes sociales o sitios web para hacerse pasar por otra persona y llevar a cabo actividades fraudulentas, difamatorias o acosadoras.

Se considera que los efectos de la suplantación de identidad pueden ser devastadores para las víctimas, ya que pueden resultar en pérdida de dinero, daño a la reputación, problemas legales y emocionales. Por ello, para protegerse contra la suplantación de identidad, es importante tomar medidas de seguridad, cómo proteger adecuadamente la información personal, utilizar contraseñas fuertes y únicas para cada cuenta, tener cuidado al compartir información en línea y estar alerta ante posibles signos de suplantación de identidad, como

cargos no autorizados en cuentas bancarias o notificaciones de cuentas creadas en su nombre sin su conocimiento.

2.6. Pornografía infantil en medios informáticos

Se refiere a la producción, distribución y consumo de material pornográfico que involucra a niños o adolescentes menores de edad. Este tipo de material abusivo y explotador muestra a niños participando en actividades sexuales o exhibiendo sus cuerpos de una manera sexualmente explícita. En Perú, este delito se encuentra tipificado en el artículo 183-B del Código Penal Peruano, por los cargos de producción, reproducción, posesión, distribución, exhibición, oferta o facilitación de material pornográfico que involucre a menores de edad.

Lamentablemente, la pornografía infantil ha proliferado en medios informáticos de la era digital debido a la facilidad de distribución y acceso a través de Internet. Los delincuentes sexuales utilizan medios informáticos, como sitios web prohibidos, redes sociales, foros en línea, servicios de mensajería y plataformas de intercambio de archivos, para compartir, comercializar y obtener material pornográfico que involucre a menores de edad.

Es importante destacar que la producción, distribución, posesión y consumo de pornografía infantil es un delito grave en la mayoría de los países. La explotación de niños con fines sexuales es una forma de abuso infantil y violación de los derechos humanos. Estos actos dañan a los niños y pueden tener un impacto duradero en su bienestar físico, emocional y psicológico. Robles, F. et al. (2016) apoyan esta postura, ya que es un delito que atenta la psique humana y el desarrollo de la sexualidad del menor que es utilizado como objeto de placer y fuente de dinero.

Las autoridades y organizaciones internacionales trabajan en conjunto para combatir la pornografía infantil en medios informáticos. Se establecen leyes y regulaciones más estrictas, se realizan investigaciones para identificar y perseguir a los delincuentes. Se promueve la conciencia y educación para prevenir el abuso y proteger a los niños.

2.7. Fraude informático

El fraude informático es un término que engloba diversas actividades ilegales y fraudulentas que se llevan a cabo mediante el uso de tecnologías informáticas y redes electrónicas. Implica el uso indebido de la tecnología con el propósito de obtener beneficios económicos ilícitos, causar daños o perjuicios a individuos, empresas o instituciones. Además, Acurio (s.f.) advirtió que, con el avance de la tecnología, surgirían nuevas formas de falsificación o alteración fraudulenta de documentos de uso comercial utilizando fotocopiadoras computarizadas en color que utilizan rayos láser, lo que aumentaría los casos de fraude. Esta generación de fotocopiadoras permitió realizar reproducciones de alta resolución, modificar documentos e incluso crear documentos falsos sin necesidad de contar con un original. Los resultados obtenidos eran de una calidad tal que solo un experto podría distinguirlos de los documentos auténticos.

Así vemos que el fraude informático abarca una amplia gama de actividades fraudulentas, algunas de las cuales ya se han mencionado: phishing, malware, estafas en línea, robo de identidad, fraude de tarjetas (débito o crédito). Por lo que, es un delito grave y puede tener consecuencias financieras, legales y personales significativas para las víctimas. En Perú, este delito se encuentra tipificado en el artículo 207-D del Código Penal Peruano, por los cargos de obtención de un beneficio económico indebido utilizando medios informáticos, como la manipulación de datos, la suplantación de identidad, el uso de programas maliciosos, entre otros.

Ya que, la Ley N° 30096 prescribe que aquellas personas que intencional e ilegítimamente busca obtener un beneficio ilícito para sí mismo o para otro a expensas de terceros, mediante acciones como el diseño, introducción, alteración, eliminación, supresión o clonación de datos informáticos, así como cualquier interferencia o manipulación en el funcionamiento de un sistema informático, será castigada con una pena de prisión que oscilará entre tres y ocho años, y una multa de sesenta a ciento veinte días. Por ello, Robles et al. (2016) sustenta que es un delito del tipo doloso porque las características del criminal no son comunes en los delincuentes, estos tienen habilidades que usan conscientemente para manejar los sistemas informáticos y dañarlos.

Para protegerse contra el fraude informático, es importante tener precaución al proporcionar información personal en línea, utilizar contraseñas seguras, mantener actualizado el *software* de seguridad en los dispositivos y estar alerta ante posibles signos de fraude, como transacciones sospechosas o solicitudes de información confidencial no solicitadas.

2.8. Otros delitos informáticos reconocidos en la legislación peruana

Los siguientes delitos vienen a ser los más recientes que se encuentran dentro de las prevenciones que se actualizaron la Ley 30096 para proceder ante posibles situaciones de emergencia; considerándolos en casos muy específicos entre otros.

2.8.1. Abuso de mecanismos y dispositivos informáticos

En la legislación peruana, el abuso de mecanismos y dispositivos informáticos se encuentra tipificado como un delito informático. Este delito se refiere al uso inadecuado o malicioso de los mecanismos y dispositivos informáticos con el objetivo de cometer acciones ilegales o perjudiciales. Además, Robles et al. (2016) expone que la conducta típica que tienen las

personas que cometen este delito se basa en actuar deliberadamente para crear, proyectar, vender y ofrecer, ilegítimamente, mecanismos informáticos con la intención de perjudicar.

Algunas conductas que pueden considerarse como abuso de mecanismos y dispositivos informáticos incluyen:

a. **Manipulación de datos**: Alterar, borrar o modificar información almacenada en sistemas informáticos o bases de datos sin autorización.

b. **Uso fraudulento de dispositivos**: Utilizar dispositivos informáticos, como tarjetas de crédito falsas o clonadas, para cometer estafas o realizar transacciones ilegales.

c. **Suplantación de identidad en medios informáticos**: Hacerse pasar por otra persona o entidad utilizando medios electrónicos o digitales, con el fin de obtener beneficios económicos o perjudicar a terceros.

d. **Uso no autorizado de sistemas o redes informáticas**: Acceder o utilizar sistemas o redes informáticas sin el consentimiento del propietario o administrador, con el propósito de obtener información o causar daños.

El abuso de mecanismos y dispositivos informáticos está tipificado en la Ley de Delitos Informáticos y su Reglamento en Perú. Las sanciones para este delito pueden variar dependiendo de la gravedad de la conducta y el daño causado, pudiendo incluir multas, penas privativas de libertad u otras medidas punitivas. Pasión por el Derecho (2021) expone que este delito forma parte del Artículo 10 en la que postula la pena privativa de libertad que va entre 1 y 4 años con treinta a noventa días-multa, para los sujetos que ofrecen o prestan servicio que contribuyen a este propósito.

De esta manera, mediante las leyes que regulan la sociedad, se busca proteger la integridad, seguridad y confidencialidad de la información en el entorno digital, así como prevenir el uso indebido de los recursos informáticos.

2.8.2. Interferencia telefónica

En la legislación peruana, la interferencia telefónica se encuentra tipificada y actualizada como un delito y está contemplada en el Artículo 162 Código Penal Peruano. Este delito se refiere a la intervención ilegal en las comunicaciones telefónicas, ya sea mediante la escucha o grabación de conversaciones sin el consentimiento de las partes involucradas. El espacio Pasión por el Derecho (2021) señala que en la actualización de esta ley se agregaron penalizaciones mucho más estrictas y extensas con respecto a la pena privativa de libertad, multas y otras medidas punitivas, dependiendo de la gravedad de la conducta y las circunstancias específicas del caso.

La interferencia telefónica puede tener diferentes formas, como:

a. **Escucha telefónica**: Consiste en acceder de manera ilegal a una conversación telefónica sin el conocimiento ni consentimiento de las personas involucradas. Esto implica interceptar la comunicación y escuchar.

b. **Grabación de conversaciones**: Se refiere a la acción de registrar o grabar una conversación telefónica sin el consentimiento de las personas que participan en ella. Esto puede realizarse utilizando dispositivos de grabación o *software* especializado.

Es importante destacar que la interferencia telefónica sin autorización, llamada coloquilamente "chuponeo" telefónico, es una violación de la privacidad y los derechos de las personas. La ley busca proteger la confidencialidad de las comunicaciones y prevenir el uso indebido de la información obtenida a través de este delito.

2.8.3. Extorsión

En la legislación de Perú, la extorsión se considera un delito y está tipificada en el Artículo 1 de la Ley 27697 del Código Penal Peruano. Ya que, la extorsión es un acto ilícito grave que penaliza a cualquier persona que, mediante el uso de violencia, amenazas o coacción, busca obtener beneficios económicos o ventajas indebidas de otra persona o entidad.

En el contexto de delitos informáticos, la extorsión puede llevarse a cabo a través de medios electrónicos o digitales. Algunas formas comunes de extorsión informática incluyen:

a. **Extorsión por medio de correos electrónicos o mensajes**: Los delincuentes pueden enviar mensajes amenazantes a través de correos electrónicos, mensajes de texto, chats en línea o redes sociales, exigiendo dinero u otros beneficios a cambio de no revelar información comprometedora o difamar a la víctima.

b. ***Ransomware***: Es una forma de extorsión informática en la cual los delincuentes infectan los sistemas informáticos de las víctimas y cifran o bloquean el acceso a los datos. Luego, exigen un rescate en forma de dinero o criptomonedas para desbloquear o descifrar los archivos.

c. **Sextorsión**: En este caso, los delincuentes obtienen material sexualmente explícito de la víctima a través de Internet o redes sociales y luego amenazan con difundirlo públicamente si no se paga un rescate.

Debido a ello, se espera que las víctimas denuncien el delito a las autoridades competentes, recopilar evidencia relevante, evitar ceder a las demandas de los delincuentes y buscar asesoramiento legal adecuado.

2.8.4. Ciberterrorismo

El terrorismo informático se refiere a la realización de acciones con el propósito de desestabilizar un país o presionar a un gobierno, mediante el empleo de métodos que se clasifican como delitos informáticos, particularmente los relacionados con el sabotaje. Es importante destacar que esto no excluye la utilización de otros tipos de delitos informáticos. Acurio (s.f.) menciona que un ataque de terrorismo informático requiere de menos recursos humanos y financiamiento económico en comparación con un ataque terrorista convencional.

CAPÍTULO III

LEGISLACIÓN PERUANA SOBRE DELITOS INFORMÁTICOS

La legislación peruana se refiere al conjunto de leyes, normas y regulaciones que rigen en el territorio de la República del Perú para mantener el orden y la armonía. Es el marco legal que establece los derechos, obligaciones y normas de conducta que deben seguir los ciudadanos, las empresas y las instituciones dentro del país. Por lo que, es elaborada y modificada de acuerdo con los procedimientos establecidos por la Constitución Política del Perú. Además, está sujeta a revisiones y actualizaciones periódicas para adaptarse a los cambios sociales y económicos que son acompañados por el desarrollo avanzado de las tecnologías.

Por ello, la finalidad de la legislación peruana es establecer un marco normativo que promueva el orden, la justicia, el respeto a los derechos humanos, el desarrollo económico y social, y la protección de los intereses del Estado y de los ciudadanos peruanos. En consecuencia, vemos el cambio constante que han readaptado a la Ley del Código Penal peruano para los delitos informáticos.

En Perú, el marco legal específico para los delitos informáticos comenzó a tomar forma con la promulgación de la Ley N° 27208 en el año 2000, conocida como la "Ley de Firmas y Certificados Digitales". Esta ley estableció los fundamentos legales para la validez y seguridad de las transacciones electrónicas y la utilización de firmas y certificados digitales.

Posteriormente, en el año 2004, se promulgó la Ley N° 28237, conocida como la "Ley contra los Delitos Informáticos". Esta ley estableció los delitos informáticos y sus sanciones correspondientes. Algunos de los delitos contemplados en esta ley incluyen la falsificación de datos informáticos, el acceso no autorizado a sistemas o redes informáticas, el sabotaje informático, la interceptación ilícita de comunicaciones, entre otros.

En el año 2013, se introdujo una importante modificación al Código Penal peruano con la promulgación de la Ley N° 30096, conocida como la "Ley de Delitos Informáticos", que consta de siete capítulos que especifican la disposición para la cual fueron creados. Esta ley amplió y actualizó el catálogo de delitos informáticos y sus sanciones, con el fin de enfrentar de manera más efectiva la ciberdelincuencia. Además, se establecieron disposiciones específicas para la protección de los datos personales y la privacidad en el ámbito digital.

Asimismo, este marco legislativo del derecho informático y los aspectos generales de esta ley, vemos como se comprende de distintos elementos que lo conforman como los artículos, las características, los agentes (sujetos involucrados), el agravio, el objeto de delito, la conducta, el procedimiento para ejecutar el delito y la adaptabilidad de cambiar, se debe adecuar a las necesidades válidas que justifique el ciudadano. Pero también se tiene en cuenta, idealmente, tener casos que ejemplifiquen como antecedente.

Sin embargo, se debe tener en cuenta que todo este proceso se da en protección del patrimonio como bien jurídico protegido, el cual pertenece al sujeto pasivo que es atentado.

Esto se da porque el patrimonio es un derecho fundamental que se encuentra protegido por el derecho. Refiriéndose al conjunto de bienes, derechos y obligaciones que posee una persona o entidad, y que tienen un valor económico. Por lo tanto, el derecho tiene como objetivo principal salvaguardar y preservar el patrimonio de las personas y asegurar su adecuada protección contra posibles amenazas y delitos.

Por ello, vemos que se relaciona con el ámbito penal, ya que existen delitos específicos que afectan directamente al patrimonio, como el robo, el hurto, la estafa, la apropiación indebida, el fraude, entre otros. Estos delitos implican la sustracción, daño o manipulación ilegal de los bienes patrimoniales de una persona, con el propósito de obtener un beneficio económico ilícito. Gracias a ello, encontramos que los delitos son tipificados de acuerdo con la gravedad que ocasionan, de este modo se garantiza la seguridad y la integridad de los bienes y derechos que conforman el patrimonio de las personas.

3.1. El derecho informático

El derecho informático, también conocido como derecho de la informática o derecho de las tecnologías de la información, es una rama del derecho que se ocupa de los aspectos legales y jurídicos relacionados con el uso de las tecnologías de la información y la comunicación (TIC), así como de la protección de los datos y la regulación de las actividades informáticas; se le relaciona bastante con el derecho penal. Pues, en la actualidad nos enfrentamos a "La Era Informática" que, a pesar de tener beneficios para el desarrollo humano, también trae consigo efectos negativos de la tecnología como la ciberdelincuencia que viene a efectuarse por los medios virtuales.

Por ello es necesario contar con un marco legal efectivo, regulado con el apoyo de instituciones capacitadas en el tema y actualizado para combatir este tipo de delincuencia que ha emergido junto con la tecnología, con el fin de proteger a los individuos, las

organizaciones y los sistemas informáticos. Esto es un efecto de la dependencia social hacia las TIC.

El derecho informático abarca una amplia gama de temas, incluyendo:

1. **Protección de datos:** Regula la recopilación, almacenamiento, procesamiento y transmisión de datos personales, estableciendo principios y requisitos para garantizar la privacidad y seguridad de la información.

2. **Propiedad intelectual:** Trata sobre la protección de los derechos de autor, patentes, marcas y otros aspectos relacionados con la propiedad intelectual en el entorno digital.

3. **Comercio electrónico:** Establece las normas y regulaciones para las transacciones comerciales realizadas a través de medios electrónicos, como contratos electrónicos, firma electrónica, protección al consumidor en línea, entre otros.

4. **Delitos informáticos:** Regula las conductas delictivas realizadas a través de medios informáticos, como el acceso no autorizado, la interceptación de datos, el fraude informático, el ciberacoso, la pornografía infantil, entre otros.

5. **Gobierno electrónico:** Se refiere a la aplicación de las tecnologías de la información en los procesos administrativos y gubernamentales que se dan por los medios digitales, como la implementación de servicios en línea, la participación ciudadana digital y la transparencia en la gestión pública.

6. **Protección de la privacidad:** Establece los derechos y las restricciones para la recolección, uso y divulgación de información personal, así como el manejo de la privacidad en el entorno digital.

El derecho informático es una disciplina en constante evolución debido al rápido avance de las tecnologías de la información y la comunicación. Los profesionales del derecho informático se encargan de interpretar, análisis del trabajo, autoridades a cargo y aplicar las leyes existentes en el ámbito digital. También proponen nuevas regulaciones y adaptaciones legales para abordar los desafíos y problemáticas emergentes en el entorno digital.

3.2. Aspectos generales según la Ley N° 30096 de delitos informáticos

Como ya se ha mencionado en los capítulos previos, nos basamos en la última actualización de la Ley para delitos informáticos que abarca los siguientes elementos a considerar para el estudio de casos.

3.2.1. El patrimonio

En Perú, el patrimonio es un concepto del bien jurídico fundamental que se encuentra protegido por el sistema legal del país. El patrimonio peruano comprende el conjunto de bienes, derechos y obligaciones de una persona, tanto naturales como jurídicas, y está regulado principalmente por el Código Civil y otras leyes pertinentes.

El Código Civil peruano establece los principios y normas que rigen la adquisición, posesión, disfrute, transferencia y protección del patrimonio. Reconoce diferentes tipos de bienes, como bienes muebles, bienes inmuebles, bienes tangibles e intangibles, entre otros. Asimismo, establece los derechos y obligaciones relacionados con el patrimonio, incluyendo la capacidad de disposición y administración de los bienes.

En el ámbito penal, el Código Penal peruano contempla delitos que afectan el patrimonio de las personas y que están tipificados y sancionados de acuerdo con la legislación vigente. Algunos ejemplos de estos delitos son el robo, la estafa, el hurto, la apropiación ilícita, el

fraude, entre otros. Estos delitos implican acciones ilegales que perjudican directamente el patrimonio de las personas y se encuentran penados por la ley.

3.2.2. Análisis del tipo objetivo

Para diferenciar un delito informático objetivo que no genere ambigüedades, se debe tener en cuenta un enfoque metodológico y sistemático para comprender y examinar los aspectos relevantes del delito. Pero, también se debe tener en cuenta unos pasos previos:

1. **Recopilación de información:** Reúne todos los datos disponibles relacionados con el delito informático en cuestión. Esto puede incluir informes de incidentes, registros de actividades, evidencia digital, declaraciones de testigos, entre otros.

2. **Identificación del delito:** Determina la naturaleza y la tipología del delito informático. Puede ser un acceso no autorizado, un fraude, una intrusión, un sabotaje, un robo de informción, entre otros. Comprende los elementos esenciales del delito y las leyes pertinentes aplicables en tu jurisdicción.

3. **Análisis de la evidencia digital:** Examina la evidencia digital recolectada, como registros de servidores, registros de acceso, correos electrónicos, archivos digitales, registros de transacciones, entre otros. Este análisis puede requerir el apoyo de expertos en informática forense o seguridad cibernética.

4. **Identificación de la cadena de eventos:** Reconstruye la secuencia de eventos relacionados con el delito. Esto implica determinar cómo se llevó a cabo el delito, los métodos utilizados, los sistemas o redes afectadas y las vulnerabilidades explotadas.

5. **Evaluación del impacto:** Evalúa el impacto del delito informático en términos de daños financieros, pérdida de datos, interrupción de servicios, violación de la

privacidad, reputación afectada, entre otros aspectos relevantes. Cuantifica el alcance de los perjuicios causados.

6. **Identificación del autor o los responsables:** Si es posible, busca identificar al autor o los responsables del delito informático. Esto puede requerir una investigación más profunda y la colaboración con organismos de aplicación de la ley o expertos en seguridad informática.

7. **Documentación del análisis:** Registra todos los hallazgos, evidencias y conclusiones del análisis en un informe detallado. Esto servirá como base para futuras acciones legales, investigaciones o medidas de seguridad.

Es importante tener en cuenta que el análisis de un delito informático puede ser complejo y requerir conocimientos técnicos especializados. En muchos casos, es recomendable buscar la asistencia de expertos en seguridad cibernética o profesionales forenses para llevar a cabo un análisis exhaustivo y preciso.

a. **Características del delito** Es importante destacar que las características son generales y pueden variar dependiendo tanto del delito específico como de las circunstancias particulares. Por lo que, para obtener una comprensión más precisa y detallada de los delitos informáticos en Perú, es recomendable consultar algunos caracteres particulares del delito de criminalidad informática que postula Bramont Arias (1997), las cuales se han mantenido en el tiempo.

- **El objeto material:** En términos generales se refiere al objeto de delito que viene a ser un bien patrimonial; lo que se interpreta como un bien material aprehensible, tangible, entre otras características que hacen posible su hurto. Sin embargo, con respecto al contexto informático surge una problemática, debido a que la realidad del presente

es distinta al contexto inicial en el que surgieron las primeras leyes. Pues, ahora se trata con datos almacenados en computadoras o nubes de internet que solo manejan información como bien inmueble, esto no encajaría con las características tradicionales sobre la sustracción de un bien.

Debido a ello, se parte de dos conceptos autónomos que rescata Bramont-Arias (1997) que se basan en el material tangible y el valor monetario. El primero justifica que, si bien la información como tal no es un bien tangible, se le puede dar corporeidad al archivar en un medio tangible como un USB, un disco o una memoria; así ya no tendría problemas en considerar la información como bien tangible. El segundo justifica que se puede considerar un bien mueble al dinero contable, escritural o documental. Esta postura parte de la manipulación que se hace del dinero desde las computadoras según el valor económico que le brinda el mercado.

- **El comportamiento típico:** El comportamiento se refiere a la apropiación del bien mueble que es despojado de su lugar inicial. Por lo que, se entiende que como el desplazamiento físico del bien. Sin embargo, en el ámbito criminalístico de la informática se tiene la posibilidad de sustraer la información sin la necesidad de que haya un desplazamiento físico. En consecuencia, Bramont Arias (1997) expone que este carácter ha tomado un significado distinto, entendiéndose que este traslado se refiere a que el bien se encuentra bajo el control del sujeto activo.

  Aunque, se debe tener en cuenta que la sustracción de información se puede realizar ahora con una simple copia o memorización. De ahí parte la idea de que este delito en realidad daña el derecho al secreto de los datos almacenados o privacidad que se quieren mantener en reserva de terceros.

- **Métodos con los que se ejecuta los comportamientos típicos:** Estos métodos se caracterizan por ser particulares en su ejecución:

  - **Método de transferencia electrónica de fondos:** Se basa en el uso de medios electrónicos (teléfono, computadora, Tablet, etc.) para efectuar el robo de una cuenta o institución financiera. Esto se refiere al traslado del dinero de una cuenta a otra, sin importar el destino. Bramont-Arias (1997) propone que esta transferencia es un método del reflejo de un asiento contable, pues se supone que vendría a ser una transacción aparentemente normal, pero es un robo.

  - **Método de sistemas telemáticos:** Se entiende como la informática entre equipos tecnológicos que están a distancia pero que igual pueden tratar la información. Por lo que, Bramont-Arias (1997) sustenta que el empleo de la telemática dentro de la cibercriminalidad comprende cualquier equipo automático de procesamiento de datos para hurtar la información, con el fin de tener beneficios económicos; puede clasificarse como un delito de uso o de daños si se destruye la información.

  - **Método invasivo de claves:** Se refiere al uso malversado de claves secretas que fueron sustraídas por medios informáticos que han sido hackeados. Bramont-Arias (1997) menciona que viene a ser una violación de la clave esta transgresión de hurtar las claves secretas, va desde los cajeros automáticos hasta las cuentas digitales que se tienen en internet. Pero si se utiliza la violencia para conseguir la clave del sujeto pasivo, entonces eso pasaría a ser un delito de robo como tal.

b. **Objeto del delito** El objeto material de un delito informático no necesariamente es un bien mueble en el sentido tradicional. En el contexto de los delitos informáticos, el objeto material puede ser la información, los datos electrónicos, los sistemas

informáticos o cualquier otro elemento digital que sea susceptible de ser manipulado, accedido o afectado de manera ilícita.

Aunque, si bien la doctrina y jurisprudencia han definido el concepto de bien mueble como un objeto del mundo exterior con valor económico, susceptible de apoderamiento material y desplazamiento. Sin embargo, en el caso de los delitos informáticos, el enfoque se centra más en la naturaleza de la información y los sistemas involucrados.

Por ello, Bramont-Arias (1997) justifica que el valor económico a menudo se deriva de la información misma, como datos confidenciales, secretos comerciales, información financiera o propiedad intelectual. Además, el acceso no autorizado, la manipulación o la destrucción de sistemas informáticos y datos diversos, pueden causar perjuicios económicos considerables.

c. **Resultado del delito** Una de las características más significativas de la información es que trasciende la frontera del espacio y el tiempo, por ello no tiene límites en su uso. Por ejemplo, es normal que haya continuas transferencias entre distintas entidades bancarias alrededor del mundo. Por otro lado, las acciones de manipulación informática muestran una conducta que se distingue por ser de bajo riesgo, o sea, se pueden llevar a cabo desde el propio domicilio del perpetrador, incluso a larga distancia o más allá de las fronteras del país donde se originarán los efectos. Existe una separación temporal entre el acto ilícito y sus consecuencias.

Bramont-Arias (1997) menciona que esta situación nos lleva a nuevas problemáticas que complican la determinación de la relación de causalidad entre la conducta del sujeto activo y el resultado (negativo) que ocasiona. Esto nos llevaría a un segundo problema sobre el conocimiento que se tiene de las altas tecnologías, debido a que son insuficientes en conocerlas y tener medidas de seguridad.

Entonces, estos factores hacen que se dificulte poder prever los resultados finales de los delitos y las conductas para procesarlos. Asimismo, la propia deficiencia de las autoridades no ayuda a que se solucione esta problemática. En consecuencia, se refuerza la necesidad de contar con la intervención de peritos en informática capaces de solucionar y confrontar la ciberdelincuencia.

d. Participantes del delito Los participantes vienen a ser el sujeto activo y el sujeto pasivo que se han presentado en los capítulos previos. Por lo que, conocemos que el sujeto activo viene a ser cualquier individuo, no debe tener necesariamente las habilidades informáticas. Sin embargo, según Bramont-Arias (1997) se puede diferenciar dos grupos de delitos por parte del sujeto activo:

1. Es cuando el sujeto actúa sobre un sistema informático ajeno, en el que se ve este agente como un extraño perjudicial.

2. Es cuando los delitos se refieren a situaciones en las que el propietario o titular del sistema afectado es quien realiza la manipulación fraudulenta en perjuicio de terceros, como entidades bancarias, compañías de seguros, empresas diversas o la administración tributaria.

Este sujeto activo también puede ser un experto de alto nivel en programación, manipulación y ejecución de información. Sin embargo, dado el aumento de la especialización y la división de funciones que hay entre las diversas personas involucradas en poner orden, es razonable suponer que la presencia de varios autores mediatos en un acto delictivo no será difícil combatir.

Por otro lado, se tiene el sujeto pasivo que como bien se presentó va a ser la víctima por ser el titular de un bien jurídico protegido (patrimonio) que termina siendo afectado.

Puede ser una persona natural o jurídica, pero se apunta normalmente a empresas grandes o personas con un gran patrimonio.

3.3. Autoridades encargadas de la persecución y prevención de delitos informáticos

En Perú, existen varias autoridades encargadas de la persecución y prevención de delitos informáticos. Estas autoridades desempeñan un papel fundamental en la investigación, detección y sanción de los delitos informáticos, así como en la implementación de medidas de prevención y seguridad cibernética. A continuación, se presentan las principales autoridades involucradas:

3.3.1. Ministerio Público

El Ministerio Público es la entidad encargada de la persecución penal en Perú. A través de la Fiscalía Especializada en Delitos Informáticos y de Alta Tecnología, se lleva a cabo la investigación y el procesamiento de los delitos informáticos. Esta entidad trabaja en estrecha colaboración con la Policía Nacional y otros organismos pertinentes. Entre sus funciones básicas, según Romero (2005), están:

- Atender las solicitudes y peticiones de acción judicial en defensa de la legalidad y los derechos públicos protegidos por el derecho.
- Custodiar la independencia de los órganos jurisdiccionales y de la administración de la justicia en el país.
- Incorporar los procesos judiciales a la sociedad.
- Guiar la investigación del delito desde el inicio. Por lo que la Policía Nacional está bajo los mandamientos del Ministerio Público.

- Ejercer la acción penal de oficio o a petición.

- Pronunciar el dictamen previo a las resoluciones judiciales en los casos contemplados por la ley.

- Iniciar la formación de leyes e informar de los vacíos legales al Congreso o al presidente de la República.

Entendiéndose que la finalidad del Ministerio Público en Perú es promover la justicia, proteger los derechos de los ciudadanos y perseguir el delito. Actúa como una institución autónoma e independiente, cuyo propósito es defender el orden jurídico y garantizar la imparcialidad en la administración de justicia.

3.3.2. Policía Nacional del Perú (PNP)

La PNP tiene unidades especializadas que se encargan de investigar y combatir los delitos informáticos, como La Dirección de Investigación de Delitos de Alta Tecnología (DIVINDAT) es una de las unidades especializadas que se dedica específicamente a la investigación de delitos informáticos y cibernéticos. Entre sus funciones básicas, según Romero (2005), están:

- Función preventiva para mantener la seguridad y armonía pública.

- Función investigativa que opera en base a delitos y faltas.

- Función protectora que defiende los derechos y patrimonios públicos y/o privados de los ciudadanos.

- Función de auxilio frente a las necesidades de la ciudadanía.

- Función conciliadora frente a los problemas de baja categoría que vienen a ser infracciones legales.

- Las que sean asignadas por la Constitución Política del Perú (1993).

Así pues, la finalidad de la Policía Nacional del Perú es salvaguardar la seguridad y el bienestar de la sociedad peruana, combatiendo la delincuencia, manteniendo el orden público y protegiendo los derechos de las personas. Su labor es fundamental para garantizar la convivencia pacífica y la tranquilidad en el país.

3.3.3. El Ministerio de Justicia y Derechos Humanos de Perú

Es un organismo del Poder Ejecutivo encargado de formular y ejecutar las políticas públicas en materia de justicia y derechos humanos. Su función principal es la de asesorar al presidente de la República en la toma de decisiones relacionadas con el ámbito de la justicia. El Ministerio de Justicia, por su parte, tiene la responsabilidad de brindar apoyo y supervisión en la administración de justicia, así como en la formulación de políticas y proyectos relacionados con la reforma del sistema judicial, la defensa legal del Estado, la promoción y protección de los derechos humanos, entre otros temas relacionados. Entre sus funciones principales esta:

1. **Formulación de políticas:** Crea políticas públicas en materia de justicia y derechos humanos. Esto implica diseñar estrategias y programas para promover la justicia, fortalecer el sistema de justicia, garantizar el acceso a la justicia y proteger los derechos fundamentales de los ciudadanos.

2. **Supervisión y coordinación**: Se refiere a las actividades de las entidades y organismos del sistema de justicia. Esto incluye el Poder Judicial, el Ministerio Público, el Poder Judicial, el Instituto Nacional Penitenciario (INPE), entre otros. El objetivo es asegurar

el cumplimiento de las políticas y normativas establecidas en el ámbito de la justicia y los derechos humanos.

3. **Modernización del sistema de justicia:** Se basa en actualizar y reforzar el sistema de justicia en el país. Esto incluye la implementación de tecnologías de la información y comunicación en el ámbito judicial, la mejora de la gestión procesal, la capacitación y actualización de los operadores de justicia, entre otras acciones.

4. **Derechos humanos:** Esto implica la elaboración de políticas y programas en materia de derechos humanos, así como la cooperación con organismos nacionales e internacionales para su promoción y protección. También se ocupa de la atención a las víctimas de violaciones de derechos humanos.

5. **Asesoramiento legal al Estado:** Incluye la revisión y elaboración de proyectos de ley, la defensa del Estado en litigios, la interpretación de normas jurídicas, entre otros.

6. **Cooperación internacional:** El ministerio participa en la cooperación internacional en el ámbito de la justicia y los derechos humanos. Establece relaciones de cooperación con otros países y organismos internacionales, participar en redes y foros internacionales, así como recibir asistencia técnica en temas de justicia y derechos humanos.

En resumen, la finalidad del Ministerio de Justicia y Derechos Humanos de Perú es promover y garantizar el acceso a la justicia, proteger y promover los derechos humanos, y contribuir a la construcción de una sociedad justa, equitativa y respetuosa de los derechos fundamentales de todos los ciudadanos peruanos.

3.3.4. Poder Judicial

Es responsable de impartir justicia en el país. Los casos de delitos informáticos son sometidos a los tribunales correspondientes, donde los jueces se encargan de analizar las pruebas presentadas, escuchar a las partes involucradas y dictar sentencias en conformidad con la legislación vigente. Los funcionarios que lo constituyen, según Romero (2005), son:

- Presidente de la Corte Superior
- Vocales superiores
- Jueces
- Personal del apoyo

Estas autoridades actúan en función de la administración de justicia y resolución de conflictos. Estas funciones son:

1. **Administración de justicia:** Es responsable de administrar justicia de manera imparcial e independiente. Esto implica resolver controversias legales, aplicar las leyes y garantizar el cumplimiento de los derechos y obligaciones de los ciudadanos.

2. **Juzgamiento y resolución de casos:** Tiene la función principal de juzgar y resolver casos en todas las materias que se encuentren dentro de su competencia. Los jueces y tribunales se encargan de analizar las pruebas, evaluar los argumentos de las partes y emitir sentencias o resoluciones judiciales.

3. **Garantía de derechos fundamentales:** Tiene la responsabilidad de proteger y garantizar los derechos fundamentales consagrados en la Constitución y en los tratados

internacionales de derechos humanos. Los jueces deben velar por el respeto de estos derechos en el ejercicio de sus funciones.

4. **Control de legalidad:** El poder judicial ejerce el control de legalidad sobre los actos de las autoridades y organismos del Estado. Esto implica revisar la legalidad de las actuaciones de los poderes públicos y garantizar el respeto al principio de legalidad en el ejercicio del poder.

5. **Aplicación de normas y jurisprudencia:** El poder judicial aplica las normas legales y la jurisprudencia establecida por las instancias superiores. Los jueces interpretan las leyes y precedentes judiciales para resolver los casos que se presentan ante ellos de manera coherente y uniforme.

6. **Imparcialidad e independencia:** Debe actuar de manera imparcial e independiente, sin verse influenciado por intereses políticos, económicos o de otra índole. Los jueces deben tomar decisiones basadas en el análisis de la evidencia y los argumentos legales, sin discriminación ni favoritismo.

En conclusión, la finalidad del Poder Judicial es garantizar la imparcialidad, la independencia y la eficiencia en la administración de justicia. Su objetivo principal es proteger los derechos y libertades de los ciudadanos, resolver conflictos y aplicar la ley de manera justa y equitativa, contribuyendo así a la paz social y al Estado de derecho en la sociedad.

3.3.5. Ministerio de Transportes y Comunicaciones (MTC)

El MTC tiene un rol relevante en la prevención y regulación de los delitos informáticos. A través de su Dirección General de Gobierno Digital, se promueven políticas y medidas para garantizar la seguridad cibernética, proteger la infraestructura crítica y fomentar la ciberseguridad en el ámbito público y privado. Sus funciones principales son las siguientes:

1. **Inclusión digital:** El MTC promueve la inclusión digital y trabaja en la reducción de la brecha digital que existe en el país. Esto implica implementar programas y políticas para garantizar el acceso a las TIC en áreas rurales y comunidades alejadas.

2. **Ciberseguridad:** Aunque no es una función exclusiva del MTC, la entidad colabora en la implementación de políticas y acciones para fortalecer la seguridad cibernética en el ámbito de las comunicaciones y la infraestructura de tecnologías de la información.

3. **Desarrollo de las comunicaciones:** El MTC promueve el desarrollo de las comunicaciones en el país, incluyendo las telecomunicaciones, la radiodifusión y la tecnología de la información. Esto implica la asignación de frecuencias, la regulación de los servicios de telecomunicaciones, la promoción de la banda ancha y el impulso de la inclusión digital.

Es importante destacar que estas son algunas de las principales autoridades encargadas de la persecución y prevención de delitos informáticos en Perú. Además, existen otros organismos, como el Organismo Supervisor de la Inversión en Telecomunicaciones (OSIPTEL) y el Organismo Supervisor de la Inversión Privada en Telecomunicaciones (OSIPTEL), que también desempeñan un papel relevante en la regulación y supervisión de la seguridad cibernética en el ámbito de las telecomunicaciones. Su labor contribuye al crecimiento económico, la integración social y el bienestar de la sociedad peruana.

3.4. Caso cibernético

3.4.1. Caso BCP: Cibercriminales lograron acceder a datos de sus clientes.

El Banco de Crédito informó que en 2018 sufrió un ciberataque que permitió a individuos inescrupulosos acceder a información personal, cuentas, números de tarjetas y saldos de un grupo de sus clientes. (Redacción EC, 2019). Aunque aseguran que no se sustrajeron

claves ni dinero, surge la incógnita de qué ocurrió con esos datos filtrados. Es importante destacar que los datos fueron publicados en la Deep web, lo cual representa un alto riesgo, ya que, al estar expuestos de forma libre, existe un mayor riesgo debido a los posibles fines con los que los cibercriminales puedan utilizar esta información.

Esta filtración de datos expone a muchas personas, incluyendo su nombre, número de teléfono, dirección y ocupación. Estos datos podrían ser utilizados para extorsión o suplantación de identidad. La repercusión negativa es que se espera un aumento en el número de estafas y actividades delictivas en línea.

El Banco de Crédito ha informado que ha reforzado sus sistemas de seguridad y ha cerrado la brecha de intrusión para evitar futuros incidentes.

CAPÍTULO IV

TRATAMIENTO JURÍDICO DE LOS DELITOS INFORMÁTICOS EN EL DERECHO PERUANO

4.1. Contexto

La globalización ha impactado profundamente las instituciones y los cimientos de nuestra sociedad en todos los aspectos, hasta el punto de sugerir la aparición de una sociedad paralela, virtualizada o digitalizada, cuya principal fuente de generación y desarrollo se da en el Internet. Este medio ha abierto numerosas posibilidades debido a sus características peculiares, como su fácil acceso, el anonimato de los usuarios, la falta de regulación, su desarrollo caótico, la inseguridad y su rápido crecimiento.

Esta tecnología no solo ofrece beneficiospara la educación, el gobierno, las empresas, entre otros, sino también a problemas serios como la aparición de nuevas formas de delito, como el robo de fondos, la pornografía infantil, la trata de blancas, el chantaje, el acoso y la extorsión. Estos problemas han llevado al surgimiento de términos como cibercrimen, ciberdelitos, ciberdelincuencia y ciberterrorismo, que se agrupan bajo el término "delitos informáticos" y han causado un gran impacto que transgrede nuestra sociedad.

Por ejemplo, desde cualquier lugar del mundo y en cualquier momento, un usuario de una computadora conectada a Internet puede convertirse en un actor activo del progreso que no necesariamente estará regulado. Puede negociar, comprar, vender, subastar, informarse, proporcionar información, comunicarse y, en algunos casos, cometer delitos. Ante la aparición de estas nuevas tecnologías, en consecuencia, el derecho enfrenta desafíos casi insuperables, que deben abordarse desde una perspectiva transfronteriza, ya que esta red no conoce límites geográficos. Esto plantea desafíos reales para los abogados y profesionales del derecho en la actualidad.

Es complicado regular una materia en constante desarrollo, donde los avances informáticos generan nuevas formas de interacción humana y donde estos avances, lejos de detenerse en un punto específico de su evolución, parecen extenderse elásticamente hacia lo desconocido. El tradicional inmovilismo de las normas jurídicas, que requieren procesos complicados de creación, se muestra impotente para regular un sector en constante movimiento que parece querer evadir cualquier regulación.

En nuestro país, a pesar de los avances en materia jurídica y persecución de estos cibercrímenes, los esfuerzos por controlar este crecimiento delictivo siguen siendo insuficientes debido a la naturaleza transnacional de este tipo de delitos y a la dificultad de identificar a los delincuentes debido a su facilidad para esconderse detrás de un seudónimo o alias. Actualmente, contamos con una unidad de policía informática equipada con tecnología que permite perseguir algunos tipos de delitos, como lo demuestran los resultados obtenidos al desmantelar bandas organizadas, como los "ciber injertos del oriente", que utilizaban el envío de correos electrónicos para obtener datos confidenciales de las víctimas, como cuentas bancarias y contraseñas, y luego realizaban transacciones ilícitas de fondos con sus cómplices. A nivel mundial, existen muchos ejemplos de bandas que incluso operan con equipos más sofisticados que la propia policía informática.

Por lo tanto, se analiza la problemática general de los delitos informáticos en el entorno peruano y, consecuentemente, su tratamiento dentro del ámbito del derecho, examinando las legislaciones de países vecinos, convenios, normas internacionales, entre otros. Esta problemática se divide en:

- ¿Cómo se ajusta el ordenamiento jurídico vigente a estos nuevos fenómenos de la delincuencia informática?

- ¿Cuáles son los nuevos intereses colectivos que deben ser objeto de tutela jurídica?

- ¿Es necesario el desarrollo de una nueva rama autónoma del derecho, atendiendo muy especialmente, al valor que posee la información en la sociedad actual?

En respuesta se propone como hipótesis que la ausencia de un tratamiento jurídico de los delitos informáticos en el derecho peruano se debe a la falta de conocimiento de estos delitos y a la subvaloración que el gobierno de turno y los legisladores le dan al tema.

4.2. Objetivos

4.2.1. Objetivo general

Estudiar la ausencia de un tratamiento jurídico de los delitos informáticos en el derecho peruano, la falta de conocimiento de estos delitos y a la subvaloración tanto del gobierno de turno como de los legisladores le dan al tema.

4.2.2. Objetivos específicos

- Plantear que el ordenamiento jurídico peruano vigente sea ajustado a estos nuevos fenómenos de la delincuencia informática.

- Conocer los nuevos intereses colectivos que deben ser objeto de tutela jurídica.

- Plantear la necesidad del desarrollo de una nueva rama autónoma del derecho, atendiendo muy especialmente, al valor que posee la información en la sociedad actual.

4.3. Variables

Tabla 1. *Variables*

Variables	Indicadores
Variable independiente	
Ausencia de un tratamiento jurídico de los delitos informáticos en el derecho peruano	Congreso de la república peruana Código Civil Código Penal Proyectos de ley elaborados por los legisladores Normas jurídicas emitadas en el Perú en materia informática
Variables dependientes	
1ra variable dependiente	
Desconocimiento de estos delitos	Proyectos de ley elaborados y planteados Tipos de leyes aprobadas Participación en grupos de investigación en la materia Apoyo a la policía informática Equipamento en el estado peruano para perseguir delitos informáticos
2da variable dependiente	
Subvaloración que el gobierno de turno y los legisladores le dan al tema	Actitud sobre el valor los delitos informáticos en el Perú

4.4. Tipo y diseño de investigación

La presente investigación es de tipo jurídica con la tipología jurídica – descriptiva – exploratoria y socio – jurídica. Asimismo, la presente investigación se encuentra dentro del nivel de investigación aplicada en el derecho, dentro del área del derecho penal. Por ser de naturaleza jurídica se ubica dentro de la rama de las ciencias humanas con implicancias en el derecho, por ende, está inmersa dentro del diseño de la ciencia aplicada. En cuanto al análisis y exposición de resultados se ciñe al tipo cualitativo.

4.5. Métodos aplicados

En las ciencias jurídicas, los métodos de investigación son excepcionales y específicos por tratarse de una ciencia particular dentro de la clasificación de las ciencias humanas, en la presente investigación se utilizó el método dogmático y exegético, en conjunto con el de análisis y síntesis.

4.6. Ámbito y tiempo de la investigación

La investigación elaborada corresponde al ámbito del territorio nacional, específicamente a todos aquellos usuarios peruanos que usan las redes para realizar todo tipo de actividades cotidianas. En cuanto al tiempo, la presente investigación corresponde al año 2011.

4.7. Resultados

Dentro de los diversos casos que se encuentran generalmente en los delitos informáticos, se recogieron los más resaltantes por traspasar las fronteras de un país, lo que plantea nuevos retos. En primer lugar, para los diversos operadores de la administración de justicia, abogados, jueces, peritos, entre otros; en segundo para los legisladores, toda vez que las soluciones tienen que partir de la esfera global, de tal modo que los delitos se puedan sancionar sin tomar en cuenta las barreras geográficas y de tiempo.

En ese entender, los diversos grupos regionales y organizaciones mundiales como la Comunidad Andina de Naciones o la Organización de Naciones Unidas están planteando la tratativa de delitos como la pornografía infantil a nivel de todo el globo terráqueo para que se pueda perseguir y sancionar desde cualquier parte del mundo.

Si bien es cierto, en nuestro país tenemos un poco de avance, ya que como se vio legislativamente ya está tipificado el delito de pornografía infantil, la protección a las bases

de datos, tenemos regulado la propagación del SPAM, entre otros. Sin embargo, siguen siendo insuficientes debido al raudo avance tecnológico que día en día incrementa las posibilidades de todas estas tecnologías, tanto para actividades que permiten el desarrollo de la humanidad como la educación, el trabajo, el comercio, como también para el desarrollo delictivo en la humanidad, por lo que a diario aparecen nuevas modalidades.

Seguidamente exponemos algunos casos conocidos en la generalidad de delitos informáticos, que requieren de alguna tipificación específica según el código penal peruano.

4.7.1. Tipificación de delitos informático en el ordenamiento jurídico peruano

En el ordenamiento jurídico peruano, se tipifican los siguientes delitos que tienen aplicación directa en el campo informático, y que consideramos están dentro del concepto general de los delitos informáticos.

a. **Delito de Violación a la Intimidad** En el Código Penal peruano está tipificado en el artículo 154 el Delito de violación a la intimidad, y establece que: *"el que viola la intimidad de la vida personal y familiar ya sea observando, escuchando o registrando un hecho, palabra, escrito o imagen, valiéndose de instrumentos, procesos técnicos u otros medios será reprimido con pena privativa de libertad no mayor de dos años. La pena será no menor de uno ni mayor de tres y de treinta a ciento veinte días cuando el agente revele la intimidad conocida de la manera antes prevista".*

   El artículo 157 del Código Penal precisa que *"el que indebidamente, organiza, proporciona o emplea cualquier archivo que tenga datos referentes a las convicciones políticas o religiosas y otros aspectos de la vida íntima de una o más personas será reprimido con pena privativa de libertad no menor de un año ni mayor de cuatro años. Si el agente es funcionario o servidor público y comete delito en ejercicio del cargo, la pena será no menor de tres años ni mayo de seis e inhabilitación". Las bases de datos computarizadas consideramos que están dentro del precepto de "cualquier archivo que tenga*

datos", en consecuencia, está tipificado el delito de violación a la intimidad utilizando la informática y la telemática a través del archivo, sistematización y transmisión de archivos que contengan datos privados que sean divulgados sin consentimiento.

b. Delito de Hurto agravado por Transferencia Electrónica de Fondos, telemática en general y empleo de claves secretas. El artículo 185 del Código Penal peruano establece que aquel que *"... para obtener provecho, se apodera ilegítimamente de un bien total o parcialmente ajeno, sustrayéndolo del lugar donde se encuentra, será reprimido con pena privativa de libertad no menor de uno ni mayor de tres años. Se equipara al bien mueble la energía eléctrica, el gas, el agua y cualquier otro elemento que tenga valor económico, así como el espectro electromagnético".*

El artículo 186 del Código Penal, segundo párrafo numeral 3 - modificado por la ley 26319- dispone además *"la pena será no menor de cuatro años ni mayor de ocho si el hurto es cometido mediante la utilización de sistemas de transferencia electrónica de fondos, de la telemática en general, o la violación del empleo de claves secretas"*. El delito de hurto agravado por transferencia electrónica de fondos tiene directa importancia en la actividad informática.

El sistema de transferencia de fondos, en su conjunto, se refiere a la totalidad de las instituciones y prácticas bancarias que permiten y facilitan las transferencias interbancarias de fondos. El desarrollo de medios eficientes de transmisión de computadora a computadora de las órdenes de transferencia de fondos ha fortalecido el sistema. Los niveles de calidad y seguridad de las transferencias interbancarias de fondos se han ido acrecentando conforme el avance de la tecnología, no obstante, la vulnerabilidad a un acceso indebido es una "posibilidad latente" por tanto además de los sistemas de seguridad de *hardware*, *software* y comunicaciones ha sido necesario que la norma penal tenga tipificada esta conducta criminal.

Uno de los medios de transferencia electrónica de fondos se refiere a colocar sumas de dinero de una cuenta a otra, ya sea dentro de la misma entidad financiera o una cuenta en otra entidad de otro tipo, ya sea pública o privada. Con la frase "telemática en general" se incluyen todas aquellas transferencias u operaciones cuantificables en dinero que pueden realizarse en la red informática ya sea con el uso de Internet, por ejemplo, en el Comercio Electrónico o por otro medio. Cuando se refiere a "empleo de claves secretas" se está incluyendo la vulneración de *password*, de niveles de seguridad, de códigos o claves secretas.

c. **Delito de Falsificación de Documentos Informáticos.** El Decreto Legislativo 681 modificado por la Ley 26612, es la norma que regula el valor probatorio del documento informático, incluyendo en los conceptos de microforma y micro duplicado tanto al microfilm como al documento informático. El artículo 19 de esta norma establece que: *"la falsificación y adulteración de microformas, micro duplicados y microcopias sea durante el proceso de grabación o en cualquier otro momento, se reprime como delito contra la fe pública, conforme las normas pertinentes del Código Penal".*

Las microformas que cumplidos los requisitos técnicos (equipos y *software* certificados que garantizan inalterabilidad, fijeza, durabilidad, fidelidad e integridad de documentos micro grabados) y formales (que procesos de micrograbación sean autenticados por un depositario de la fe pública, por ejemplo, el fedatario juramentado en informática) sustituyen a los documentos originales para todos los efectos legales.

En el Código Penal Peruano (C.P.), entre los delitos contra la fe pública, que son aplicables a la falsificación y adulteración de microformas digitales tenemos los siguientes:

I. Falsificación de documentos. "El que hace, en todo o en parte, un documento falso o adultera uno verdadero que pueda dar origen a derecho u obligación o servir para

probar un hecho con el propósito de utilizar el documento, será reprimido, si de su uso puede resultar algún perjuicio, con pena privativa de libertad no menor de dos ni mayor de diez años..." (Artículo 427 del C.P.). Tratándose de microformas digitales su falsificación y/o adulteración son sancionados con la misma pena.

II. Falsedad ideológica "El que inserta o hace insertar, en instrumento público, declaraciones falsas concernientes a hechos que deben probarse con el documento, con el propósito de emplearlo como si la declaración fuera conforme a la verdad será reprimido si de uso puede resultar algún perjuicio, con pena privativa de libertad no menor de tres ni mayor de seis años..." (Artículo 428 del C.P.). Hay que tener en cuenta que la microforma digital de un documento público tiene su mismo valor, por tanto, puede darse el caso de falsedad ideológica de instrumentos públicos contenidos en microformas digitales.

III. Omisión de declaración que debe constar en el documento. "El que omite en un documento público o privado declaraciones que deberían constar o expide duplicados con igual omisión al tiempo de ejercer una función y con el fin de dar origen a un hecho u obligación, será reprimido con pena privativa de libertad no menor de uno ni mayor de seis" (Artículo 429 del C.P.). Para que tenga valor probatorio y efecto legal una microforma digital tiene que cumplir requisitos formales y técnicos. El requisito formal consiste en que debe ser autenticado por depositario de la fe pública (fedatario juramentado o notario) el proceso técnico de micro grabación y que las copias de esos documentos deben ser certificados, por lo cual una omisión de las declaraciones que por ley deben incluirse podría configurar esta figura delictiva [Núñez, 1999].

d. Delito de Fraude en la administración de personas jurídicas en la modalidad de uso de bienes informáticos. Puesto que en el patrimonio de la persona están incluidos tanto bienes materiales (*hardware*) como inmateriales (*software*, información, base de datos, etc.) esta figura delictiva puede aplicarse al campo informático según interpretación del artículo 198º inciso 8 del Código Penal, establece que : "*será reprimido con pena privativa de libertad no menor de uno ni mayor de cuatro años el que, en su condición de fundador, miembro del directorio o del consejo de administración o del consejo de vigilancia, gerente, administrador o liquidador de una persona jurídica, realiza, en perjuicio de ella o de terceros, cualquiera de los actos siguientes: Usar en provecho propio o de otro, el patrimonio de la persona*" (inciso 8). Esta figura podría aplicarse, en este orden de ideas, tanto al uso indebido de software, información, datos informáticos, hardware u otros bienes que se incluyan en el patrimonio de la persona jurídica.

e. Delito contra los derechos de autor de software Con respecto a los delitos contra los derechos de autor de software, debe tenerse en cuenta que "...*sobre la naturaleza jurídica y la tutela que apunta el derecho de autor sobre el software hay acuerdo general. Y no puede ser de otro modo, debido a la trascendencia que tiene, dado que la transgresión de índole penal a la actividad intelectual constituye no sólo una agresión a la propiedad del autor y afecta los intereses de la cultura, sino que conforma también un ataque al derecho moral sobre la paternidad de la obra*".

Con la dación del Decreto Legislativo 822, se modificó el Código Penal y se han aumentado las penas, con respecto a la legislación peruana anterior, así tenemos:

I. Que el artículo 217º del Código Penal Peruano establece que *"será reprimido con pena privativa de libertad no menor de dos ni mayor de seis años y con treinta a noventa días-multa, el que, con respecto a una obra, o una grabación audiovisual o una imagen fotográfica expresada en*

cualquier forma, realiza cualquiera de los siguientes actos, sin la autorización previa y escrita de autor o titular de los derechos".

a. La modifique total o parcialmente.

b. La reproduzca total o parcialmente, por cualquier medio o procedimiento.

c. La distribuya mediante venta, alquiler o préstamo público.

d. La comunique o difunda públicamente por cualquiera de los medios o procedimientos reservados al titular del respectivo derecho.

e. La reproduzca, distribuya o comunique en mayor número que el autorizado por escrito.

Aquí se están garantizando bajo la protección los derechos patrimoniales; en los contratos de licencia de uso de *software* se contemplan el respeto de estos derechos y también en la Ley de Derecho de Autor que anteriormente hemos tratado. La autorización previa y escrita del titular, generalmente en la actividad empresarial se instrumenta en una licencia de uso de *software*.

II. Que el Artículo 218º del Código Penal Peruano dispone que *"la pena será privativa de libertad no menor de dos ni mayor de ocho años y sesenta a ciento veinte días-multa"* cuando:

a. Se dé a conocer a cualquier persona una obra inédita o no divulgada, que haya recibido en confianza del titular del derecho de autor o de alguien en su nombre, sin el consentimiento del titular.

b. La reproducción, distribución o comunicación pública se realiza con fines de comercialización, o alterando o suprimiendo, el nombre o seudónimo del autor, productor o titular de los derechos.

c. Conociendo el origen ilícito de la copia o reproducción, la distribuya al público, por cualquier medio, la almacene, oculte, introduzca al país o la saca de éste.

d. Se ponga de cualquier otra manera en circulación dispositivos, sistemas, esquemas o equipos capaces de soslayar otro dispositivo destinado a impedir o restringir la realización de copias de obras, o a menoscabar la calidad de las copias realizadas; o capaces de permitir o fomentar la recepción de un programa codificado, radiodifundido o comunicado en otra forma al público, por aquellos que no estén autorizados para ello.

e. Se inscriba en el Registro del Derecho de Autor la obra, como si fuera propia, o como de persona distinta del verdadero titular de los derechos.

Los supuestos tratados en este artículo se refieren tanto a derecho morales como patrimoniales, que por su gravedad (atentar contra el derecho de paternidad, comercializar o distribuir copias ilegales, registrar en forma indebida el *software*) se amplía la pena hasta ocho años. En la anterior legislación la pena mayor por este tipo de delitos era de cuatro años, actualmente se ha aumentado a ochos años. Estos tipos penales, parten del supuesto que no hay consentimiento o autorización del titular de los derechos para ello; de existir una licencia de uso y cumplirse con sus términos y condiciones, no se tipificaría este delito.

III. Que el Artículo 219º del Código Penal Peruano, establece que: "será reprimido con pena privativa de libertad no menor de dos ni mayor de ocho años y sesenta a ciento

ochenta días-multa, el que, con respecto a una obra, la difunda como propia, en todo o en parte, copiándola o reproduciéndola textualmente, o tratando de disimular la copia mediante ciertas alteraciones, atribuyéndose o atribuyendo a otro, la autoría o titularidad ajena".

La apropiación de autoría ajena, de reputarse una obra que no es de uno como propia, también se aplica al *software*, más aún con las opciones tecnológicas para su copia, que incluyen equipos de cómputo, cada vez más sofisticados y el uso de herramientas en Internet.

IV. Que el Artículo 220º del Código Penal Peruano, dispone que: " será reprimido con pena privativa de libertad no menor de cuatro ni mayor de ocho años y noventa a trescientos sesentaicinco días-multa:

a. Quien se atribuya falsamente la calidad de titular originario o derivado, de cualquiera de los derechos protegidos en la legislación del derecho de autor y derechos conexos y, con esa indebida atribución, obtenga que la autoridad competente suspenda el acto de comunicación, reproducción o distribución de la obra, interpretación, producción, emisión o de cualquier otro de los bienes intelectuales protegidos.

b. Si el agente que comete cualquiera de los delitos previstos, posee la calidad de funcionario o servidor público.

Una de las preocupaciones de los creadores de *software*, al registrar su obra en el Registro Nacional de Derecho de Autor de INDECOPI, es que se tiene que entregar, entre otros requisitos, el programa fuente, se cuestionan qué sucede si lo copian sin su consentimiento. Dado que el depósito es intangible, los funcionarios

que cometieron estos delitos estarían dentro de este tipo penal y podrían ser pasibles de pena privativa de libertad hasta ocho años.

f. **Ley de pornografía infantil** Una Ley contra la pornografía infantil no debe buscar tan sólo la sanción a quién haya utilizado, producido o comercializado este tipo de imágenes o videos de un menor de edad siendo abusado sexualmente, sino que debe, por encima de todo, tratar de impedir que estos abusos y explotación sexual siga creciendo.

En tal sentido nuestra legislación peruana establece, Código Penal, establece:

Artículo 183-A.- Pornografía infantil

"El que posee, promueve, fabrica, distribuye, exhibe, ofrece, comercializa o publica, importa o exporta por cualquier medio incluido la internet, objetos, libros, escritos, imágenes visuales o auditivas, o realiza espectáculos en vivo de carácter pornográfico, en los cuales se utilice a personas de catorce y menos de dieciocho años de edad, será sancionado con pena privativa de libertad no menor de cuatro ni mayor de seis años y con ciento veinte a trescientos sesenta y cinco días multa.

Cuando el menor tenga menos de catorce años de edad la pena será no menor de seis ni mayor de ocho años y con ciento cincuenta a trescientos sesenta y cinco días multa.

Si la víctima se encuentra en alguna de las condiciones previstas en el último párrafo del artículo 173, o si el agente actúa en calidad de integrante de una organización dedicada a la pornografía infantil la pena privativa de libertad será no menor de ocho ni mayor de doce años.

De ser el caso, el agente será inhabilitado conforme al artículo 36, incisos 1, 2, 4 y 5."

4.7.2. Exposición de casos

I. Fraudes en internet Las agencias de noticias han difundido estos días la denuncia de 5.000 fraudes en Internet durante una semana [Noticias sobre internet, 2006].

Las denuncias de estos fraudes hoy en día son más frecuentes en todas partes del mundo, por ejemplo, en España han sido canalizadas a través de Nomasfraude.es, iniciativa promovida y apoyada por el Instituto Nacional de Tecnologías de la Información (INTECO), la Asociación de Internautas y Panda Software.

Figura 1. Fraudes de correo electrónico

Nota. Tomado de Flores (2011).

I.I. El *phishing* bancario, uno de los fraudes más intensivos

a. **Phishing bancario (caso BBVA 2008)** que afecta a clientes de diversas entidades bancarias, en el ejemplo se considera al BBVA con un asunto llamativo Detectado varios casos de *phishing* bancario, tenemos un ejemplo que afecta al BBVA [Asociación de internautas, 2008] y sus clientes, el procedimiento es el clásico correo electrónico

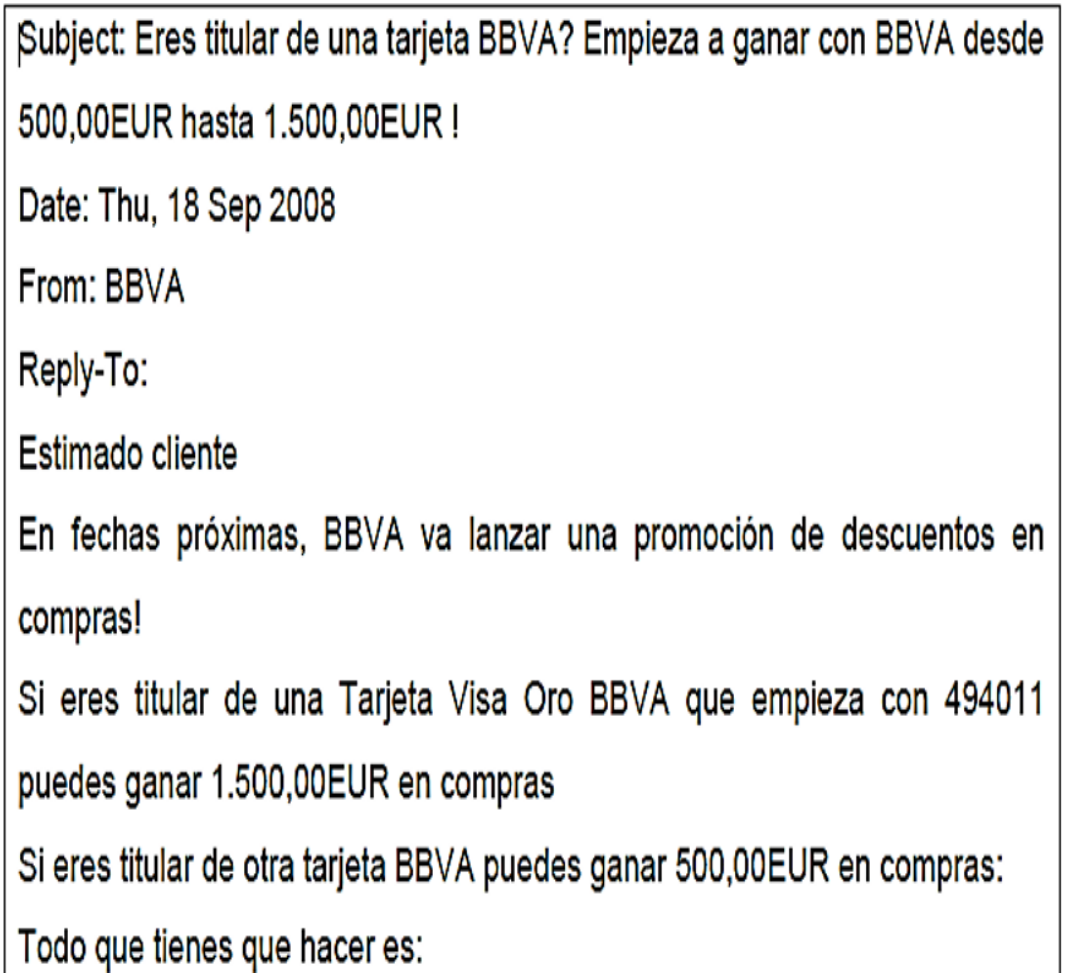
que simula ser enviado por la entidad bancaria y hacer creer al cliente que es una notificación de la entidad para verificar sus datos.

El asunto del correo trampa es: ¿Eres titular de una tarjeta BBVA? ¡Empieza a ganar con BBVA desde 500,00 EUR hasta 1.500,00 EUR!

Los datos obtenidos son enviados a: asia.europe2z@yahoo.es 18-09-2008 - Con el siguiente correo electrónico los ciber-delincuentes, este caso se comete el delito por medio de la ingeniería social, por tanto, de este modo se engaña a los clientes de las entidades bancarias.

En la Figura 2, se muestra el mensaje que se recibe:

Figura 2. Ejemplo de correo estafa


Subject: Eres titular de una tarjeta BBVA? Empieza a ganar con BBVA desde 500,00EUR hasta 1.500,00EUR !

Date: Thu, 18 Sep 2008

From: BBVA

Reply-To:

Estimado cliente

En fechas próximas, BBVA va lanzar una promoción de descuentos en compras!

Si eres titular de una Tarjeta Visa Oro BBVA que empieza con 494011 puedes ganar 1.500,00EUR en compras

Si eres titular de otra tarjeta BBVA puedes ganar 500,00EUR en compras:

Todo que tienes que hacer es:

1. Haga click en el siguiente enlace para completar el formulario de 1,500.00EUR o de 500,00EUR
2. El importe de 1,500.00EUR o de 500,00EUR va estar abonado en su Tarjeta como máximo 2-4 días laborales

Un servicio de BBVA

Haga click aquí para empezar a completar el formulario

Gracias por confiar en BBVA

Departamento de Validación de BBVA.

Nota. Tomado de Flores (2011).

Si la posible víctima pulsa sobre los enlaces del correo trampa este nos enviara a una web que suplanta la imagen de la entidad bancaria BBVA y donde solicitan las claves bancarias, tal como muestra la Figura 3:

Una vez completado el formulario, se nos envía el siguiente mensaje (Figura 3):

Figura 3. Mensaje de *phishing* bancario

Gracias por registrar su tarjeta "BBVA.net"
En breve recibira un email con la informacion para acesso a "BBVA.net" Online, Cierre esta ventana por su seguridad

Nota. Tomado de Asociación de internautas (s.f.)

Aunque muchos usuarios piensen que este tipo de trampa es muy conocida, todavía hay miles de internautas y clientes de la banca online que "caen" en ellas, cada día son mejores las falsificaciones y los nombres del dominio son muy parecidos al verdadero usado por la entidad bancaria.

Figura 4. *Phishing* bancario

Nota. Tomado de Asociación de internautas (s.f.)

En la imagen 5 se muestran datos del script que se envía al ciberdelincuente, cuando la víctima cae en la trampa.

Figura 5. Ejemplo de script estafa

```
        $aaa="asia.europe2z@yahoo.es";
$tex="Nueva BBVA Num[]";
$msg = "
Nombres y Apellidos : $_POST[name]
Direccion : : $_POST[dir]
Telefono de contacto : $_POST[tel]
Codigo Postal : $_POST[post]
Provincia : $_POST[prov]
Pais : $_POST[pais]
Direccion de correo electronico : $_POST[cor]
NÃºmero de tarjeta: $_POST[numtarjeta]
Pin: $_POST[pin]
Vencimiento: $  POST[ven]
```

Nota. Tomado de Flores (2011).

b. Otros *phishing* por medio de anuncios de premios El gerente general del Banco de la Nación, Julio César del Castillo, informó sobre la aparición de nuevos correos electrónicos fraudulentos anuncian supuestos premios a sus clientes y pedidos de "actualización de base de datos", a través de Internet o vía telefónica.

"Nuestra División de Fraudes ha detectado la presencia de nuevos mensajes electrónicos fraudulentos remitidos a los clientes de nuestra institución. Estos correos son enviados por delincuentes informáticos con la finalidad de que nuestros clientes brinden información confidencial", advirtió.

"*Cuando piden actualización de datos, los delincuentes colocan advertencias como que la cuenta del cliente será „dada de baja en una fecha límite, en caso de que no cumpla con enviar la información solicitada. Eso es totalmente falso*", agregó Castillo.

"*Al respecto, Del Castillo aclaró que el Banco de la Nación jamás solicita datos personales, ni número de tarjeta, claves, DNI, fecha de nacimiento, entre otros, de sus clientes, a través de Internet o vía telefónica.*" [tuteve.tv, 2011]

De igual modo mucho se utiliza por ejemplo a los canales de televisión como ATV, América TV, entre otros, y empresas como Telefónica del Perú y Claro enviando mensajes de este tipo para capturar datos de cuentas personales. Para mayor información anexamos la Figura 6.

Figura 6. Estafas y engaños por internet 1

Nota. Tomado de Flores (2011).

Aunque el *phishing* representa el 80 % de los nuevos casos de fraude por Internet, algunos de ellos utilizando técnicas nuevas de engaño o confusión, hay otras formas o tipos de fraude como las intrusiones en sus sistemas informáticos a través de los *scam*, troyanos y gusanos, virus o estafas con tarjetas de crédito.

Figura 7. Estafas y engaños por internet 2

Nota. Tomado de Flores (2011).

I.II. Caso *pharming* (Mi Banco 2009)

Uno de los peligros más importantes en Internet es el *pharming* que consiste en la manipulación de las direcciones DNS en la máquina de un usuario, una simple modificación en nuestro fichero *host* puede engañarnos y conseguir que ciertas páginas web que visitemos no sean realmente las originales [Asociación de internautas, 2008]

El 25 de febrero de 2009 se presentó el siguiente caso de *pharming* al banco peruano "Mi Banco", utilizando la dirección IP 68.178.187.69.

Esta banca que tiene el servicio de banca por Internet, verificando el código de la página falsa el botón "Aceptar" nos dirige a www.daumstudy.com//bbs/guard... donde se guardan los datos enviados que son el tipo de servicio, el número de la tarjeta y la clave de 6 dígitos ingresada por el teclado en pantalla, para luego reenviarnos a la página real de autenticación de Mi banco.

Figura 8. Caso *Pharming* Mi banco

Nota. Tomado de Flores (2011).

I.III. Sabotaje informático

USD 10 millones en pérdidas por sabotaje informático [Rodríguez]. Oslo (PM-Press). Luego de haber sido despedido, un programador de Omega Engineering decidió vengarse de la compañía borrando todo su *software*.

La delincuencia informática constituye un problema cada vez más grave a nivel mundial, al grado tal que países como Estados Unidos han designado incluso comisiones especiales destinadas a establecer el potencial de daño que representan los terroristas con conocimientos de informática.

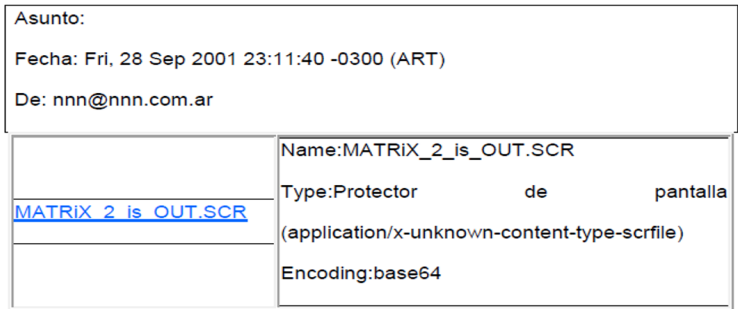
Sin embargo, los informes sobre la materia existentes hasta el momento dan cuenta de que el sector más afectado es el corporativo, que anualmente sufre cuantiosas pérdidas a nivel mundial debido al sabotaje informático. El último caso corresponde a la compañía Omega Engineering, que recientemente se vio expuesta a la ira vengativa de su ex programador Timothy Lloyd, quien luego de haber sido despedido borró todo el *software* cargado en las computadoras de la compañía.

El sabotaje fue realizado mediante una "bomba lógica" que Lloyd activó diez días después de haber perdido el trabajo. La acción debería de significar 15 años de prisión para el saboteador, además del pago de millonarias multas e indemnizaciones.

I.IV. Virus informáticos y *malware*

Delito que tiene como medio favorito el uso del correo electrónico, por donde se remiten a través de archivos adjuntos, otro medio es cuando la víctima hace descargas por internet. Se muestran algunos casos.

Figura 9. Ejemplo de correo con archivos de estafa I

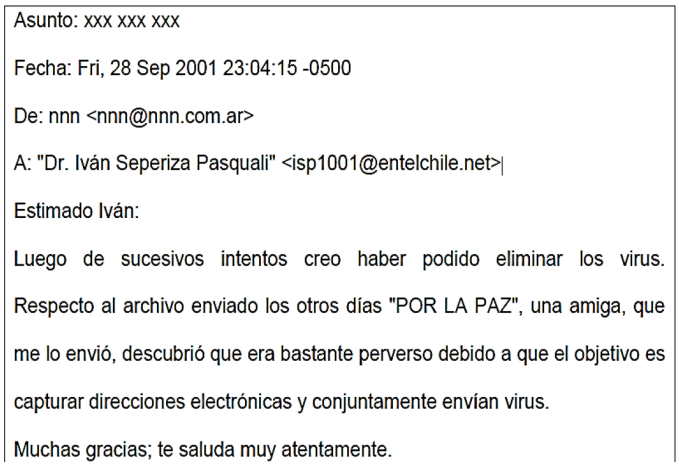


Nota. Tomado de Flores (2011).

Como se observa en la Figura 9, en este mensaje se escondieron los datos reales del remitente, sin embargo, se hace notar que esta persona nos remite un archivo adjunto que aparenta ser un protector de pantalla. Al abrirlo y ejecutarlo, y no falta quien lo haga, da paso al virus gusano.

En busca de conocer las razones por las que se remitió el archivo adjunto (virus) en esta práctica el afectado se puso en contacto con el responsable del envió, y en la Figura 10 se muestra lo que se le indico (Seperiza, 2000):

Figura 10. Ejemplo de correo con archivos de estafa II



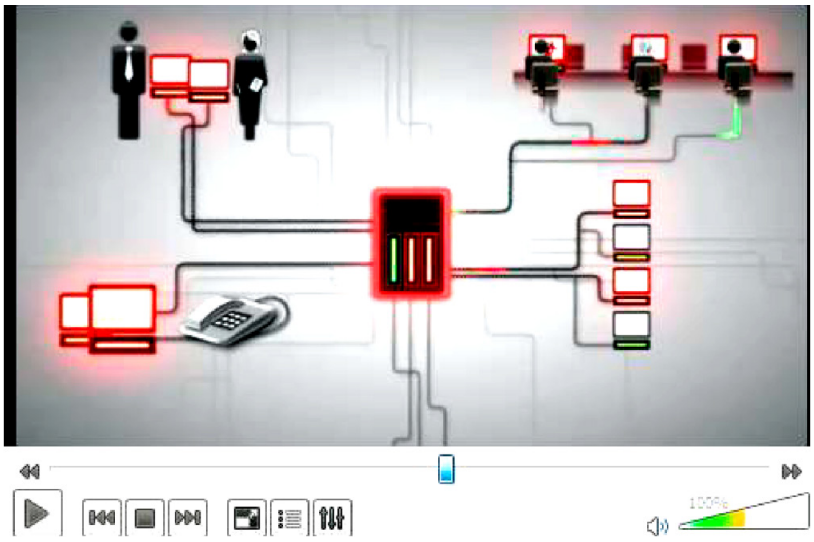
Nota. Tomado de Flores (2011).

Por otro lado, los que te envían virus engañan poniendo todo tipo de rostros, hasta el espiritual, con tal de lograr su propósito de infectar con el virus.

Frecuentemente envían cadenas por la Paz, de ayuda, de apoyo a una causa o de noticias en las que normalmente un usuario estaría interesado, como por ejemplo "Estados Unidos está a punto de dictar la guerra", los usuarios ingenuos una vez recibido el mensaje se lo reenvían a todos sus contactos creyendo armar una cadena por la paz, y al mismo tiempo reenvían un atractivo archivo ejecutable "Por la paz.exe", que resulta siendo el virus, no era la declaración de guerra de Estados Unidos, sino más bien termina siendo la guerra para su pobre computadora.

Como ejemplo ponemos la imagen 11, de video sobre virus y ataques infomáticos.

Figura 11. Virus informático



Nota. Tomado de Flores (2011). Este es el video https://www.youtube.com/watch?v=tYX56tZOX18

I.V. Robo de identidad y acoso

En cuanto al robo de identidad, estos casos se presentan frecuentemente en las redes sociales, expongo a continuación el caso de Willy Zegarra, conocido profesor de la provincia de San Román, el docente en mención supuestamente por medio de una cuenta de Facebook publica información denigrante en contra de sí mismo.

Figura 12. Robo de identidad en perfil de Facebook

Nota. Tomado de Flores (2011).

Salta a la vista que, en este caso, la persona de Willy Zegarra no se registró, al menos no con la información que se presenta en esta cuenta. Sino que una tercera persona inescrupulosamente se registró con sus datos y comete el delito contra el honor de la persona, el mismo que se encuentra tipificado en nuestro Código Penal en el Libro Segundo artículos 130 al 138.

Como se observa en la imagen se muestra incluso fotos tergiversadas del agraviado. Al publicar esta información se puede seleccionar a vista de quienes podría estar, pudiendo ser sólo amigos, amigos de mis amigos, y todo el mundo.

En este caso la portada está a disposición de los millones de usuarios de Facebook, es decir todo el mundo, y el contenido se encuentra disponible para solo amigos de la red de Willy que son 157 usuarios, tal como muestra la figura 13.

Figura 13. Amigos en facebook de la víctima de robo de identidad

Nota. Tomado de Flores (2011).

Realizando un análisis de los comentarios encontramos comentarios de diversos tipos, algunos a favor o en contra, otras de indignación por el actuar del autor de la cuenta. Estos comentarios tienen fecha y hora de emisión, por tanto, se hace notar que el caso es real.

Figura 14. Comentarios hacia la víctima 1

Nota. Tomado de Flores (2011).

Figura 15. Comentarios hacia la víctima 2

Nota. Tomado de Flores (2011).

Figura 16. Comentarios hacia la víctima 3

Nota. Tomado de Flores (2011).

Finalmente presentamos una foto (Fig. 17) publicada en el muro de Willy completamente denigrante con frases obscenas.

Figura 17. Foto trucada del Robo de identidad

Nota. Tomado de Flores (2011).

Este es el modo más frecuente de ataque a las personas, que en el mejor de los casos desconocen de su existencia por tanto no constituye en preocupación, sin embargo, al tomar conocimiento lo mínimo que se espera es un resarcimiento por el honor mellado.

Existen miles de casos como el de Willy Zegarra, donde él tiene imagen y presencia en las redes sociales, pero sin participar directamente.

I.VI. Casos de la Policía informática

a. Banda "Los Cibersecos" Extorsión Internacional Vía Internet

Figura 18. Banda Los Cibersecos

Nota. Tomado de Flores (2011).

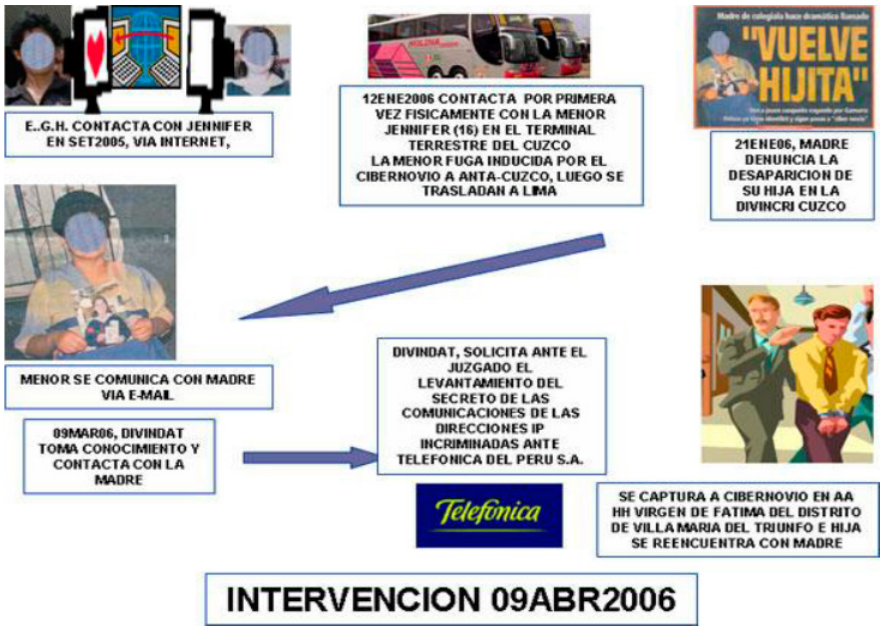
b. Caso El ingeniero

Figura 19. Caso el Ingeniero

Nota. Tomado de Flores (2011).

c. Cybernovio

Figura 20. Cybernovio



Nota. Tomado de Flores (2011).

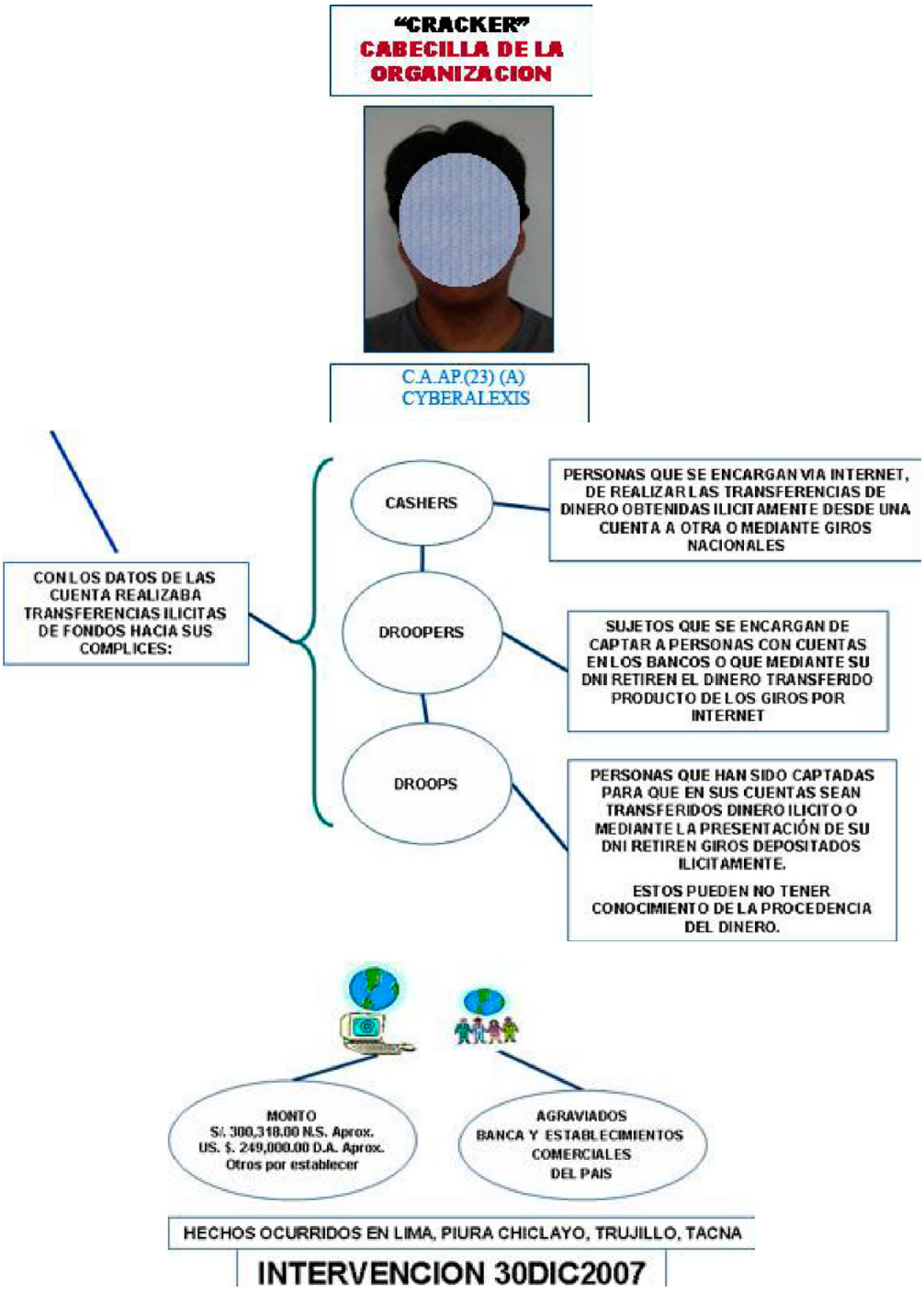
d. Caso extorsión

Figura 21. Caso extorsión

Nota. Tomado de Flores (2011).

e. Banda "Cyberdestructores" Modalidad Phishing

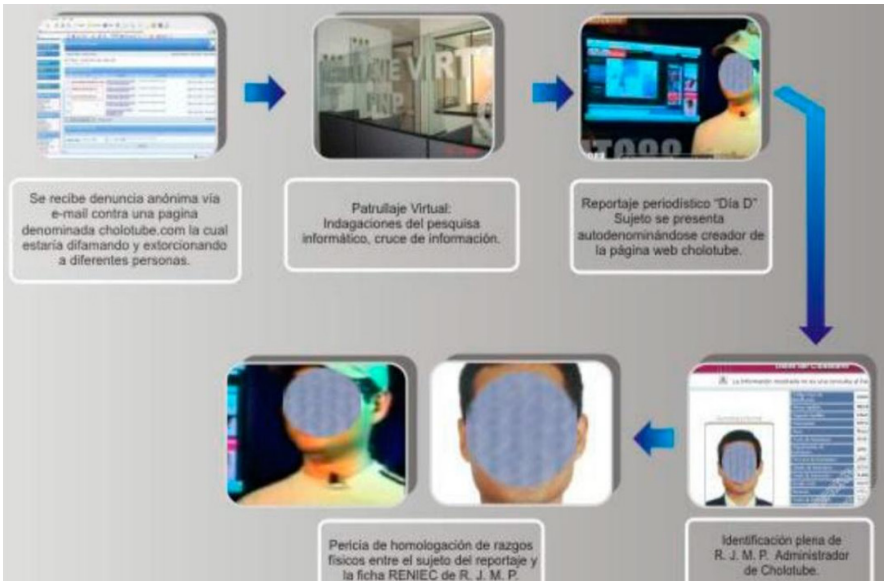
Figura 22. Cyberdestructores



Nota. Tomado de Flores (2011).

f. Caso "Contador" Modalidad Keyloggers

Figura 23. Caso contador



Nota. Tomado de Flores (2011).

g. Caso los Eta-Cholos

Figura 24. Caso Eta-Cholos

Nota. Tomado de Flores (2011).

I.VII. Caso Anonymous

Anonymous atacó la página web del Ministerio de Energía y Minas. [El Comercio, 2011] La ofensiva del colectivo de hackers fue denominada operación "Agua Primero". Sus integrantes apoyan la cancelación del proyecto minero Conga.

Anonymous dirigió un ataque en contra de la página web oficial del Ministerio de Energía y Minas (MEM), en una medida que marcaría el inicio de sus acciones de apoyo a la cancelación definitiva del proyecto minero Conga que pretende llevarse a cabo en Cajamarca y que fue suspendido tras una serie de protesta de la población.

El colectivo de hackers había anunciado la operación "Agua Primero, mina después" – identificada en Twitter con el hashtag #OpAguaPrimero- argumentando que buscaba "hacer entrar en razón" a las autoridades para que cuiden mejor los recursos hídricos. Según el plan inicial, el proyecto Conga buscaba explotar recursos minerales que se encontraban bajo cuatro lagunas naturales.

Hace tres meses, Anonymous inhabilitó una serie de portales del Estado Peruano a través de un ataque de degeneración de servicio DDOS, el mismo que habría realizado esta ocasión para dejar fuera de línea al portal del MEM.

4.8. Conclusiones y recomendaciones

4.8.1. Conclusiones

1. El ordenamiento jurídico vigente en Perú se encuentra en algunos aspectos desfasados, en sus diversas ramas penal, civil, administrativa, tributaria, entre otros. Por ejemplos en derecho civil falta establecer las nuevas relaciones contractuales y la solución de conflictos que se van presentando entre particulares producto de este nuevo entorno,

como es en el caso del comercio electrónico o en las redes sociales, y faltando determinar las formas de identificar a los usuarios para evitar el anonimato en las redes.

2. Desde el derecho tributario, por ejemplo, hoy es posible el comercio de bienes no solo tangibles sino también intangibles entre usuarios de diversos países y estos aspectos tributarios no están reconocidos en nuestro país.

3. En la rama del derecho penal, estas nuevas formas delictivas están ganando terreno por lo que resulta difícil elaborar estadísticas sobre este tipo de delitos, sin embargo, la cifra es muy alta; y no es fácil descubrirlo y sancionarlo, pero los daños económicos son altísimos; existe una gran indiferencia de la opinión pública sobre los daños ocasionados a la sociedad; la sociedad no considera delincuentes a los sujetos que cometen este tipo de delitos, no los segrega, no los desprecia, ni los desvaloriza, por el contrario, el autor o autores de este tipo de delitos se considera a sí mismos —respetables—, por su grado de conocimiento y habilidades en el manejo de estas herramientas.

4. En el mundo moderno, el acceso a la información es un derecho que puede ejercerse libremente por cualquier persona, sin embargo, a través de los medios informáticos se han tergiversado ese derecho de acceso a la información, de tal modo que hoy se cometen los llamados delitos informáticos afectando otros derechos como la intimidad, el patrimonio económico, la libre competencia o inclusive la seguridad de un Estado.

5. Atendiendo estas nuevas formas de interactuar por el uso herramientas informáticas y electrónicas para diversas actividades usuales, hoy en día urge hacer una distinción de esta materia, por la existencia de las más variadas conductas delictuosas relacionadas con la información, y por ende vinculadas a los delitos informáticos que en algunos casos pueden configurar otro tipo de delitos más graves.

6. Debido a que no existe una rama especifica que estudie los delitos informaticos, entonces las víctimas están desprotegidas, la falta de preparación por parte de las autoridades para comprender, investigar y aplicar el tratamiento jurídico adecuado a esta problemática; el temor por parte de las empresas de denunciar este tipo de ilícitos por el desprestigio que esto pudiera ocasionar a su empresa y las consecuentes pérdidas económicas, entre otros más, son parte de ese vacío en su estudio y tratamiento jurídico.

4.8.2. Recomendaciones

De acuerdo a la primera conclusión planteada manifestando de que nuestro ordenamiento jurídico peruano se encuentra desfasado, anexamos la propuesta de Ley, denominada "Ley especial sobre delitos informáticos Perú", la misma que si bien es cierto no abarca todas las ramas del derecho, se ha enfocado en el tema principal de la presente investigación que son los delitos informáticos, y en especial la protección a los sistemas de información que contienen justamente los datos, que es la información como bien jurídico tutelado.

Esta propuesta no se ha elaborado tomando cada posibilidad y variación de los delitos informáticos como se expuso en el marco teórico, y en los casos, sino más bien tratando de cuidar los sistemas informáticos en términos generales, ya que este nivel de criminalidad traspasa fronteras, entonces se tiene que abordar desde una perspectiva internacional y reprimirla en ese sentido, ya que los usuarios están esparcidos por todo el mundo y, en consecuencia, existe una posibilidad muy grande de que el agresor y la víctima estén sujetos a leyes nacionales diferentes. Además, si bien los acuerdos de cooperación internacional y los tratados de extradición bilaterales intentan remediar algunas de las 155 dificultades ocasionadas por los delitos informáticos, sus posibilidades son limitadas, además de que en algunos países como el nuestro no existe legislación alguna sobre esta clase de conductas ilícitas lo que empeora más la situación de las víctimas de estas conductas ilícitas.

REFERENCIAS BIBLIOGRÁFICAS

Acurio, S. (s.f.). *Delitos informáticos: generalidades*. Repositorio UDGVirtual. DOI: http://biblioteca.udgvirtual.udg.mx/jspui/handle/123456789/599

Asociación de Internautas. (s.f.). *Phishing bancario que afecta a clientes del BBVA con asunto llamativo y donde descubrimos al ciber-delincuente*. https://seguridad.internautas.org/html/4415.html

Bramont-Arias, L. (1997). *El delito informático en el Código penal peruano*. Fondo Editorial de la Pontificia Universidad Católica del Perú. https://repositorio.pucp.edu.pe/index/handle/123456789/181585

Código Penal peruano [actualizado 2023]. LP: Pasión por el derecho (8 de julio de 2023). DOI: https://lpderecho.pe/codigo-penal-peruano-actualizado/

El Comercio (03 de diciembre de 2019). BCP reconoce que sufrió ataque informático en el 2018. *El Comercio*. https://elcomercio.pe/economia/negocios/bcp-reconoce-que-sufrio-ataque-informatico-en-el-2018-banco-de-credito-del-peru-nndc-noticia/#:~:text=El%20Banco%20de%20Cr%C3%A9dito%20de%20Per%C3%BA%20%28BCP%29%20reconoci%C3%B3,esta%20sustracci%C3%B3n%20no%20incluy%C3%B3%20las%20claves%20de%20tarjetas.

Flores, E. (2011). *Tratamiento jurídico de los delitos informáticos en el derecho peruano.* [Tesis de doctorado. Universidad Andina Néstor Cáceres Velásquez].

González, J. (2007). Precisiones conceptuales y político-criminales sobre la intervención penal en internet. *Cuadernos penales José Marías Lidón*, 4, 13-40. DOI: *2007-Delitos_ informaticos20190618-52109-6fm00r-libre.pdf (d1wqtxts1xzle7.cloudfront.net)

Gutiérrez-Oquendo, H. (2023). Visualizar principales características y métodos de la delincuencia informática, a partir de la lucha mundial contra el COVID-19. *Publicaciones E Investigación*, *17*(1), 1-13. DOI: https://hemeroteca.unad.edu.co/index.php/publicaciones-e-investigacion/article/view/5968

Hernández, L. (2009). El delito informático. *Eguzkilore: Cuaderno del Instituto Vasco de Criminología*, 23, 227-243. DOI: https://addi.ehu.es/bitstream/handle/10810/24953/18-Hernandez.indd.pdf?sequence=1

Lima, M. (1984). *Delitos electrónicos*. Ediciones Porrua.

Muñoz, C. (2010). *Consideraciones político criminales en torno a la delincuencia informática y el delito de daños*. [Tesis de Maestría. Universidad de Panamá]. Ley de delitos informáticos (Ley 30096) [actualizado 2021] | LP (lpderecho.pe)

Pajuelo, C. (2010). Ensayo crítico de la gestión dogmática del bien jurídico tutelado en los delitos informáticos. *Revista Jurídica*, 325-335. DOI: https://www.revistajuridicaonline.com/wp-content/uploads/2010/11/28_325a336_ensayo_critico.pdf

Pasión por el Derecho (13 de abril de 2021). Ley de delitos informáticos (Ley 30096) [actualizado 2021]. DOI: Ley de delitos informáticos (Ley 30096) [actualizado 2021] | LP (lpderecho.pe)

Peralta, R. (2022). *Los delitos informáticos y los datos en sistemas informáticos*. [Tesis de licenciatura. Universidad Peruana de Las Américas]. http://repositorio.ulasamericas.edu.pe/handle/upa/2572

Pérez, M., & Mezzasalma, M. (2009). *Delitos informáticos: cuestiones dogmáticas y desafíos político criminales de la modernidad tardía*. [Tesis. Universidad Nacional de la Pampa]. https://repo.unlpam.edu.ar/handle/unlpam/1071

Reyna, L. (2016). Criminalidad informática, crimen organizado e internacionalización del delito. Ley contra el crimen organizado (Ley No. 30077), 197-236. DOI: *Criminalidad_informatica-libre.pdf (d1wqtxts1xzle7.cloudfront.net)

Robles, F. et al. (2016). Delitos informáticos y por medios electrónicos en el derecho penal peruano. DOI: *DELITOS_INFORMATICOS_Y_POR_MEDIOS_ELECTRONICOS20191229-71566-vdejex-libre.pdf (En d1wqtxts1xzle7.cloudfront.net)

Romero, L. (2005). *Marco conceptual de los delitos informáticos*. [Tesis de maestría. Universidad Nacional Mayor de San Marcos]. https://cybertesis.unmsm.edu.pe/handle/20.500.12672/2675

Téllez, J. (1996). *Derecho Informático*. Editorial Mc Graw Hill, segunda edición.

Villavicencio Terreros, F. (2014). Delitos Informáticos. *Ius et veritas*, 24(49), 284-304. https://revistas.pucp.edu.pe/index.php/iusetveritas/article/view/13630

Vinelli, R. (2021). Los delitos informáticos y su relación con la criminalidad económica. *Ius Et Praxis*, 53, 95-110. https://revistas.ulima.edu.pe/index.php/Ius_et_Praxis/article/view/4995


EDITORIAL
TERCER SOL
MEXICO