UNIVERSIDAD METROPOLITANA DEL ECUADOR

FACULTAD DE CIENCIAS SOCIALES, HUMANIDADES Y EDUCACIÓN

CARRERA DE DERECHO

SEDE QUITO

ENSAYO PREVIO A LA OBTENCIÓN DEL TÍTULO DE ABOGADO DE LOS TRIBUNALES DE JUSTICIA DE LA REPÚBLICA DEL ECUADOR

TEMA:

LOS CIBERDELITOS EN EL SISTEMA JUDICIAL PENAL ECUATORIANO CON ÉNFASIS EN LA INTELIGENCIA ARTIFICIAL

AUTORA:

MARÍA GABRIELA CASCANTE SALTOS

TUTOR:

DR. HERMES GILBERTO SARANGO AGUIRRE

QUITO - 2024

CERTICADO DE TUTOR

Dr. Hermes Gilberto Sarango Aguirre, en calidad de asesor del trabajo de Investigación designado por disposición del Director de Carrera de Derecho de la UMET, certifico que la señorita, María Gabriela Cascante Saltos, portador de la cédula de ciudadanía No. 172742773-2, ha culminado el trabajo de investigación, con el tema "LOS CIBERDELITOS EN EL SISTEMA JUDICIAL PENAL ECUATORIANO CON ÉNFASIS EN LA INTELIGENCIA ARTIFICIAL", quien ha cumplido con todos los requisitos legales exigidos, por lo que se aprueba el trabajo. Se hace especial énfasis en verificar que no se haya incluido en el trabajo textos sin la correspondiente referencia bibliográfica. En caso de que se determine la existencia de plagio académico, el autor asume la responsabilidad total y exclusiva por tal acto.

Es todo cuanto puedo decir en honor a la verdad, facultando al interesado hacer uso de la presente, así como también se autoriza la presentación para la evaluación por parte del jurado respectivo.

María Gabriela Cascante Saltos

Atentamente,

DR. HERMES GILBERTO SARANGO AGUIRRE

C.C.1105924417

TUTOR

CERTIFICADO DE AUTORÍA DE TRABAJO DE TITULACIÓN

MARÍA GABRIELA CASCANTE SALTOS, estudiante de la Universidad Metropolitana del Ecuador ¨UMET¨, de la carrera de Derecho, declaro en forma libre y voluntaria que el presente Ensayo que versa sobre: "**Los ciberdelitos en el sistema judicial penal ecuatoriano con énfasis en la inteligencia artificial"**, así como las expresiones vertidas en este documento son de autoría de la compareciente, quien ha realizado la investigación con base a la recopilación bibliográfica, consultas en revistas científicas, documentos en sitios web. En consecuencia, se asume la responsabilidad del ensayo y la originalidad al remitir a las fuentes bibliográficas respectivas para fundamentar el contenido expuesto.

Atentamente,

MARÍA GABRIELA CASCANTE SALTOS

C.I: 1727427732

AUTORA

CESIÓN DE DERECHOS

MARÍA GABRIELA CASCANTE SALTOS, en calidad de autora y titular de los derechos morales y patrimoniales del trabajo de titulación **"Los ciberdelitos en el sistema judicial penal ecuatoriano con énfasis en la inteligencia artificial"**, modalidad Examen Complexivo, de conformidad con el Art., 114 del CÓDIGO ORGÁNICO DE LA ECONOMÍA SOCIAL DE LOS CONOCIMIENTOS, CREATIVIDAD E INNOVACIÓN, cedo a favor de la Universidad Metropolitana una licencia gratuita, intransferible y no exclusiva para el uso no comercial de la obra con fines académicos. Se conserva a favor todos los derechos de la autora sobre la tesis, establecidos en la normativa citada. Así mismo, autorizó a la Universidad Metropolitana para que realice la digitalización y publicación de este trabajo de titulación en el repositorio virtual, de conformidad a lo dispuesto en el Art., 144 de la Ley Orgánica de Educación Superior.

La autora declara que la obra objeto de la presente autorización es original en su forma de expresión y no infringe el derecho de autor de terceros, asumiendo la responsabilidad por cualquier reclamación que pudiera presentarse por esta causa y liberando a la Universidad de toda responsabilidad.

Atentamente,

MARÍA GABRIELA CASCANTE SALTOS

C.I: 1727427732

AGRADECIMIENTO

Gratitud la llevó en cada paso de mi vida en especial a Dios por otorgarme unos padres tan maravillosos, a mi padre quien me acompaña desde el cielo, Abdón Bolívar Cascante López por su ejemplo de trabajo y enseñarme a dar siempre lo mejor de mí persona, a mi madre María Saltos por su infinito amor quien me ha enseñado a no rendirme jamás. Asimismo, a mis hermanos mayores, María Fernanda y Carlos Alberto, por ser mis compañeros de infancia y convertirse en mis mejores amigos de vida. El amor, respeto y admiración que les tengo es infinito.

De igual manera, agradezco:

A mi tutor el docente Hermes Sarango quien se convirtió en un gran guía, consejero, motivador y gracias a sus conocimientos impartidos he podido aplicar todas sus sugerencias y recomendaciones en el presente ensayo.

Agradezco a la Universidad Metropolitana por todo el aprendizaje adquirido por parte de todos los docentes de la carrera de Derecho, quienes en cada semestre impartieron sus conocimientos y gracias a ellos se adquirieron bases fundamentales para el futuro ejercicio profesional de la abogacía.

ÍNDICE GENERAL

ÍNDICE DE TABLAS

RESUMEN

En la actualidad, el ciberdelito presenta una amenaza dinámica en el ámbito digital, este fenómeno se caracteriza por el uso de tecnologías de la información y las comunicaciones en actividades delictivas, los cuales afectan de manera significativa y colosal a las personas naturales y jurídicas, incluso causando perjuicios económicos. Los ciberdelincuentes, aprovechando la interconexión global y la creciente dependencia de la sociedad en la tecnología, despliegan tácticas sofisticadas para perpetrar actos delictivos causando daños en los sistemas informáticos. Las categorías de la ciberdelincuencia han evolucionado con la expansión de la inteligencia artificial, planteando desafíos significativos para la seguridad digital; mientras que la IA impulsa avances tecnológicos, también se convierte en una herramienta poderosa para perpetrar ciberataques más sofisticados, por lo cual es necesario una combinación de medidas de ciberseguridad, marcos legales actualizados, cooperación internacional y conciencia pública. Es así como, el presente ensayo estuvo encaminado bajo un marco metodológico en base a un enfoque jurídico analítico y sociológico, el cual se enfatiza en analizar e interpretar definiciones, antecedentes y demás en relación con el ciberdelito y su avance en la actualidad; también se aplicó la investigación bibliográfica por medio de libros, revistas, sitios webs relacionados con el tema del ciberdelito y su interrelación con la inteligencia artificial. Este estudio se enfocó en la indagación de bases teóricas a fin de conocer por medio de definiciones, conceptos, características sobre el tema propuesto, así también se analizó de cerca la intersección entre la ciberdelincuencia y la inteligencia artificial y como el ámbito legal, explorando cómo las leyes existentes se enfrentan a la complejidad de los delitos cibernéticos.

Palabras clave: delito, ciberdelitos, inteligencia artificial, normativas legales.

ABSTRACT

Currently, cybercrime presents a dynamic threat in the digital sphere; this phenomenon is characterized by the use of information and communications technologies in criminal activities, which significantly affect people and companies, even causing economical harm. Cybercriminals, taking advantage of global interconnection and society's growing dependence on technology, deploy sophisticated tactics to perpetrate criminal acts by causing damage to computer systems. Cybercrime categories have evolved with the expansion of artificial intelligence, posing significant challenges for digital security, as AI drives technological advances, it also becomes a powerful tool to perpetrate more sophisticated cyberattacks, which is why a combination is necessary of cybersecurity measures, updated legal frameworks, international cooperation and public awareness. Thus, this essay was directed under a methodological framework based on an analytical legal approach which emphasizes the analysis and interpretation of definitions, antecedents and others in relation to cybercrime and its advancement today, the bibliographic research through magazines, websites related to the topic of cybercrime. This study focused on the investigation of theoretical bases in order to know through definitions, concepts, characteristics about the proposed topic, and the intersection between cybercrime and artificial intelligence and how the legal field was also closely analyzed, exploring how existing laws address the complexity of cybercrime.

Keywords: crime, cybercrimes, artificial intelligence, legal regulations.

INTRODUCCIÓN

El avance tecnológico en la era digital ha generado cambios de orden positivos los cuales han sido aprovechados de manera eficiente por las distintas sociedades del mundo entero y han enriquecido un conocimiento infinito y sin límites, y a su vez representan un apoyo para el crecimiento de las naciones, no obstante, estos avances también suelen ser utilizados por grupos criminales organizados que atentan de manera cibernética produciendo afectaciones en plataformas digitales; lo que estos buscan es cometer robos, estafas, fraudes de forma masiva vulnerando los recursos de las personas, empresas, fundaciones, organizaciones gubernamentales.

El desafío de enfrentar y mitigar los delitos cibernéticos los cuales son delitos penales que involucran de manera directa los medios electrónicos, se ha convertido en un problema sin precedentes en el sistema judicial del Ecuador, de ahí la importancia y necesidad de comprender, abordar y mitigar los ciberdelitos lo que se busca es salvaguardar la seguridad, la justicia y la integridad de la sociedad.

A medida que Ecuador se ha incorporado en el uso de la era digital, su interdependencia y uso de la tecnología ha dado lugar a un entorno favorable para los ciberdelincuentes, es así como la complejidad y potencia de los delitos cibernéticos, desde los ataques de piratas informáticos, suplantación de identidad hasta el fraude y la intimidación en línea, desafían las capacidades tradicionales del sistema de justicia penal. Estas problemáticas plantean interrogantes críticos sobre la adaptabilidad de las leyes y los procesos judiciales, así como sobre la eficacia de las estrategias existentes para combatir una forma de delincuencia que no respeta fronteras geográficas.

Por ello, la amenaza que representan los delitos cibernéticos es diverso y abarca tanto los sistemas informáticos por parte de los gobiernos, así como el robo financiero a personas naturales y personas jurídicas, a plataformas e incluso entidades financieras. Y, es así como toda la combinación de ingeniería social, ransomware, ciber espionaje y el creciente alcance de la web oscura crea una red criminal digital compleja y desafiante. En este contexto, los métodos de los delincuentes cambian con el progreso tecnológico,

creando una carrera armamentista constante entre las fuerzas del orden y los ciberdelincuentes.

Por otro lado, la inteligencia artificial, de aquí en adelante denominada por sus siglas IA y el ciberdelito han experimentado cambios significativos en las últimas décadas, convirtiendo a la tecnología de punta en un arma preferida para la ciberdelincuencia, así también, al enfrentar distintos desafíos y oportunidades, puesto que la inteligencia artificial no se emplea únicamente para protegerse contra las amenazas cibernéticas, sino también como un instrumento importante para que los ciberdelincuentes planifiquen y lleven a cabo ataques.

Es así como, el sistema de justicia penal ecuatoriano en las últimas décadas enfrenta una gran problemática al tratar de combatir una forma de delincuencia que no respeta fronteras geográficas, puesto que no se debe a la ausencia de normativas legales claras que dificulta la identificación y el procesamiento de este tipo de delincuencia, sino también a la falta de dirección, conocimiento y respaldo de las entidades como la Fiscalía General del Estado, Policía Nacional, Unidad de Ciberdelitos, por mencionar algunas y por ello se han generado dudas sobre la capacidad del sistema legal y para responder de manera efectiva ante los ciberdelitos.

Por consiguiente, dados los parámetros anteriormente mencionados es que en el presente estudio se ha planteado como objetivo general, analizar la intersección entre los ciberdelitos y la inteligencia artificial, para ello se cuentan con objetivos específicos para apoyar el estudio y análisis del objetivo principal, que consisten en estudiar los cuerpos legales como la Constitución de la República del Ecuador, el Código Orgánico Integral Penal, el Código Orgánico General de Procesos para identificar el ámbito legal cómo las leyes existentes se enfrentan a la complejidad de los delitos cibernéticos.

Adicional, como otro objetivo específico, investigar doctrina relacionada a la IA y los ciberdelitos con la finalidad de entender cómo se va conjugando con la normativa jurídica vigente en Ecuador. Por lo tanto, el desarrollo del presente ensayo se enfocará en primera instancia en indagar lo relacionado al tema “Los ciberdelitos en el sistema judicial penal ecuatoriano con énfasis en la inteligencia artificial” por medio del análisis

de fuentes teóricas con el propósito de conocer por medio de definiciones, conceptos, características y antecedentes sobre el tema propuesto.

Es importante señalar que este ensayo estará enmarcado bajo el enfoque jurídico analítico y sociológico, los cuales se enfatizan en analizar e interpretar definiciones, antecedentes y demás en relación con el ciberdelito y la inteligencia artificial. Así también, se aplicará la investigación documental mediante fuentes bibliográficas tales como revistas, sitios webs, en definitiva, material jurídico relacionado con el tema del ciberdelito en el sistema judicial penal.

DESARROLLO

Conceptos

> La inteligencia no es una dimensión única, sino un espacio profusamente estructurado de capacidades diversas para procesar la información. Del mismo modo la inteligencia artificial utiliza muchas técnicas diferentes para resolver una gran variedad de tareas. Y está en todas partes. (Boden, 2017)

Ante ello, se verifica que la inteligencia artificial imita a la inteligencia humana lo cual permite la creación de diferentes aristas para el procesamiento de información, con la gran ventaja de que las máquinas, aplicaciones, softwares, programas, entre otros, no se agotan ni presentan las necesidades y cuidados que presentamos los seres humanos. Sin embargo, todos los programas relacionados a la inteligencia artificial, de aquí en adelante IA, no conducen a una sana crítica y es ahí cuando la IA presenta una problemática.

En el sistema procesal ecuatoriano la sana crítica está vinculada directamente con el manejo de la prueba dentro de un proceso, sea penal o civil. Es así como, el Código Orgánico General de Procesos (COGEP) lo expresa de la siguiente forma a la sana crítica (Tabla 1):

Tabla 1. La sana crítica en el COGEP

Art. 164.- Valoración de la prueba.	Art. 166.- Prueba nueva. (Reformado por el Art. 30 de la Ley s/n, R.O. 517-S, 26-VI-2019)	Art. 177.- Forma de la prueba testimonial.
Para que las pruebas sean apreciadas por la o el juzgador deberá solicitarse, practicarse e incorporarse dentro de	Se podrá solicitar prueba no anunciada en la demanda, contestación a la demanda, reconvención y contestación a la reconvención, hasta	Toda prueba testimonial mediante declaración será precedida del juramento rendido ante la o el juzgador. La o el declarante deberá estar asistido por su defensora

los términos señalados en este Código. La prueba deberá ser apreciada en conjunto, de acuerdo con las reglas de la sana crítica, dejando a salvo las solemnidades prescritas en la ley sustantiva para la existencia o validez de ciertos actos. La o el juzgador tendrá obligación de expresar en su resolución, la valoración de todas las pruebas que le hayan servido para justificar su decisión.	antes de la convocatoria a la audiencia de juicio o única, siempre que se acredite que no fue de conocimiento de la parte a la que beneficia o que, habiéndola conocido, no pudo disponer de la misma. La o el juzgador podrá aceptar o no la solicitud de acuerdo con su sana crítica.	o defensor, bajo sanción de nulidad. Se seguirán las siguientes reglas: (…) 6. Las respuestas evasivas o incongruentes, así como la negativa a declarar y toda la prueba debidamente actuada será valorada íntegramente por la o el juzgador conforme con las reglas de la sana crítica, siempre que la ley no requiera que se prueben de otra forma.

Fuente: (Ecuador, Asamblea Nacional, 2015)

La sana crítica y las máximas de experiencia tienen un factor vinculante entre ambas puesto que tienen que ver con la lógica, el sentido común que se llega a desarrollar en el trayecto jurídico que se obtiene en el ejercicio de la abogacía. Por ejemplo, un problema socio jurídico en Ecuador es la corrupción, en los últimos años se ha vivido una ola de juicios políticos tales como: Caso Sobornos, Caso Caminito, entre otros. En los cuales se debe valorizar la prueba, la normativa, fuentes del derecho y así mismo los jueces deben usar la sana crítica para el dictamen de la sentencia. Por consiguiente, en el Código Orgánico Integral Penal, el artículo 616.1, respecto a las reglas para la exhibición de contenido digital donde se incorpore la prueba digital dentro de un proceso judicial y/o expediente fiscal, señala:

> 1. El contenido digital debe estar almacenado en cualquier elemento óptico o sistemas de almacenamiento como discos, cintas, memoria extraíble, entre otros.
>
> 2. El contenido digital será exhibido y/o reproducido en su formato original por cualquier medio tecnológico que lo permita, previa acreditación de quien lo presenta a través del testimonio de la o el perito correspondiente, quien dará cuenta de la cadena de custodia, integridad y autenticidad conforme a las técnicas digitales forenses.
>
> El contenido digital que haya sido obtenido mediante Asistencia Penal Internacional ingresará al Centro de Acopio del Sistema Nacional de Investigación Integral, Medicina Legal y Ciencias Forenses o el que haga sus veces, para el sometimiento a las respectivas pericias de ser necesario; y, en la etapa de juicio serán presentadas conforme a las reglas del presente artículo. En todo momento se garantizará la cadena de custodia. (Ecuador, Asamblea Nacional, 2014)

Por otro lado, de acuerdo con (Acurio, 2015, pág. 42), la definición más acertada sobre los ciberdelitos es el uso de las tecnologías y la información que reposan en las diferentes plataformas digitales las cuales son manipuladas por ciber delincuentes quienes llevan a cabo actividades delictivas; estos ciberataques pueden variar desde ataques en sistemas y redes hasta la propagación de software malicioso (incluido el robo de datos confidenciales y su manipulación).

De igual forma (Acurio, 2015, pág. 42) añade, que los ciberdelincuentes, a menudo operan en el anonimato del ciberespacio para llevar a cabo sus actividades, lo que tiene resultados devastadores para las personas como para las instituciones, por ello los ciberdelitos exigen respuestas multifacéticas que incluyan la mejora constante de las medidas de seguridad digital, una legislación actualizada y la colaboración internacional para combatir las amenazas transfronterizas.

Otro aspecto fundamental según (Meléndez, 2018), los ciberdelitos son actos que perjudican a la sociedad, estos suelen darse por medio de fraudes en línea, amenazas virtuales, entre otras; los delitos cibernéticos comprenden actividades como estafas financieras, phishing, suplantación de identidad, ciberacosos, entre otros.

Asimismo el autor (Meléndez, 2018) advierte y recomienda sobre actos de los ciberdelincuentes quienes utilizan tácticas ingeniosas para engañar a individuos y

organizaciones, comprometiendo la privacidad y la seguridad en el ciberespacio, este tipo de actos generan la necesidad y resalta la importancia para que los usuarios de la web tengan conciencia digital, así como conocimiento sobre prácticas seguras en línea y la implementación de tecnologías avanzadas de detección y prevención de posibles ataques cibernéticos.

Para (Vega, 2022), los ciberdelitos adquieren aspectos dañinos como las amenazas virtuales, las estafas financieras, la suplantación de identidad, y el ciberacoso, ya que, por medio del ciberespacio, los individuos y las organizaciones son vulnerables a la manipulación de la información por parte de ciberdelincuentes que aplican técnicas avanzadas para socavar la privacidad y la seguridad de las personas.

Por lo tanto, el sistema legal debe estar en constante actualización a fin de enfrentar los desafíos generados por el ciberdelito, como el contar con mejores mecanismos y de igual manera capacidad para investigar de forma efectiva los delitos cibernéticos y así armar una red de apoyo internacional; también se enfatiza en concientizar a la ciudadanía sobre los peligros del delito cibernético y promover medidas eficaces de seguridad en línea para minimizar sus riesgos.

Antecedentes y evolución del ciberdelito

Respecto a la evolución de los delitos cibernéticos, (Jiménez, 2022) indica, se ha caracterizado por cambios rápidos y complejos en las últimas décadas, junto con las fuerzas de seguridad y las organizaciones judiciales de todo el mundo enfrentan desafíos cada vez mayores. En sus primeras manifestaciones, el delito centraba principalmente en la actividad de hackers y virus informáticos, las cuales causaron muchas pérdidas financieras a grande escala a personas y empresas las cuales tuvieron que adoptar medidas de seguridad sofisticadas a fin de mitigar los riesgos informáticos.

De igual manera (Larrotta, 2023) manifiesta, que la innovación tecnológica fue incursionándose en la sociedad y con el tiempo se fue haciendo cada vez más necesaria la utilización de plataformas digitales en donde se procesan datos de manera masiva por parte de individuos y empresas, dicha información fue tentadora para ser amenazada de manera cibernética; al inicio dichos delitos fueron relativamente simples, por medio de la

utilización de virus que buscaban interrumpir sistemas informáticos o simplemente difundir caos.

Argumenta (Larrotta, 2023), con el auge de la conectividad global, el panorama de la ciberdelincuencia evolucionó hacia la búsqueda de beneficios financieros, dando lugar a tácticas como la suplantación de identidad, el robo de datos y los fraudes en línea, la monetización de la ciberdelincuencia se convirtió en un poderoso delito que ha impulsado el desarrollo de métodos más avanzados y que cada vez son mucho más frecuentes.

En resumen, el ciberdelito ha sido un fenómeno multifacético y dinámico, que ha pasado de simples actos de desorden digital a complejas actividades delictivas con implicaciones globales, además, este cambio demuestra no sólo la inventiva de los ciberdelincuentes, sino también, la necesidad de medidas integrales y colaborativas para combatir esta amenaza emergente en el siglo XXI.

Así también, es importante indagar sobre la inteligencia artificial para lo cual según él (Parlamento Europeo, 2021) considera que, la IA es una rama de la tecnología informática que se concentra en la creación de sistemas que pueden realizar tareas para humanos, este concepto se basa en el desarrollo de algoritmos y modelos que permiten a las máquinas aprender, razonar y tomar decisiones sin intervención humana. La IA es un sistema de realidad mixta que incluye aprendizaje automático, visión por computadora y procesamiento del lenguaje natural.

Por otro lado, para (Torra, 2019) la inteligencia artificial está diseñada principalmente para imitar las capacidades cognitivas humanas, permitiendo a las máquinas adquirir conocimientos, modificar el comportamiento en función de la experiencia y resolver problemas de manera eficiente, las tareas que realizan los sistemas que utilizan inteligencia artificial incluyen reconocer patrones, tomar decisiones, traducir idiomas, resolver problemas de manera inmediata, es decir este avance tecnológico está transformando la forma interactuar de las personas con la tecnología abriendo nuevas oportunidades en diversos campos.

Para complementar, según (Rodríguez, 2023), la interrelación que existe entre la inteligencia artificial y la ciberdelincuencia es amplia, es utilizada para ejecutar ataques más complejos y para perpetrar actividades ilegales de manera más sofisticada, el uso

de la IA en las actividades que ejecutan los ciberdelincuentes les permite aumentar su eficiencia y evitar ser detectados, la implementación de algoritmos de aprendizaje automático en ataques de suplantación de identidades avanzados es una práctica bien conocida, ya que, al analizar datos públicos y privados, la IA puede crear mensajes de phishing falsos y hacerlos parecer más auténticos.

Actualidad

De acuerdo con, (Mayer, 2018, pág. 167), en los últimos años, el ciberdelito se ha convertido en una actividad cada vez más peligrosa debido a la naturaleza de los sistemas informáticos, las redes sociales e internet, según la tendencia, cada día las personas pasan más tiempo en la web y esto permite que tengan acceso a información personal, la cual es utilizada por los ciberdelincuentes.

Desde una perspectiva penal, la introducción o exposición de datos o información en el ciberespacio da como resultado un aumento de los recursos legales que los ciberdelincuentes pueden utilizar como medidas de represalia, en la era digital con respecto a los delitos estos han evolucionado, en el pasado los casos más frecuentes de ciberdelitos estaban dados por medio de la intimidación y/o acoso en redes, la invasión a la privacidad y fraudes menores; no obstante, en la actualidad los escenarios son distintos, ya que los actos criminales por vía cibernética son cada vez mayores y afectan de manera masiva a individuos y empresas por medio de la utilización de sistemas sofisticados.

Para (Saltos, Robalino, & Pazmiño, 2021, pág. 344) otra característica de los ciberdelitos puede ser por medio de la utilización de la función de anonimato para ocultar su identidad en el ciberespacio, además, el proceso de globalización facilita la persecución de ataques internacionales y su recurrencia. Los ciberdelincuentes pueden operar desde cualquier parte del mundo, aprovechando la falta de fronteras digitales.

Así también, señala (Narváez Montenegro & Recalde Machado, 2018, pág. 4) la complejidad de los delitos cibernéticos es el resultado de la sofisticación tecnológica que involucra una gama de técnicas e intrusiones en los sistemas, los cuales permiten la ejecución de los ataques de suplantaciones de identidad. La interconexión de dispositivos y la creciente dependencia de la tecnología generan que la ciberseguridad

requiera plataformas mucho más desarrolladas para que no se puedan cometer actividades delictivas.

De acuerdo con (Juca, 2023), los ciberdelitos abarcan una amplia gama de actividades delictivas que involucran el uso de tecnologías de la información y la comunicación. A continuación, se presenta una explicación más extensa de algunos de los tipos de ciberdelitos, los cuales más adelante se clasificarán en la Tabla 2 del presente ensayo:

1. Acceso no autorizado y piratería Informática: El acceso a sistemas, redes o dispositivos informáticos sin autorización se considera no autorizado. El acto de piratería implica manipular sistemas para obtener datos confidenciales, alterar datos o causar daños.

2. Ataques de denegación de servicio: Los ciberataques tienen como objetivo inundar un sistema, servicio o red con tráfico malicioso, lo que lleva al acceso no autorizado a esos recursos, los servicios en línea pueden suspenderse temporalmente.

3. Phishing**:** El phishing implica software falso, que se engaña a las personas para que proporcionen datos confidenciales, como contraseñas o datos de tarjetas de crédito. Es común que los ciberdelincuentes utilicen correos electrónicos, mensajes de texto o sitios web falsificados que imitan entidades reales.

4. Ransomware**:** Cuando el ransomware ataca un sistema, bloquea el archivo o imposibilita el acceso y exige el reabastecimiento de la información. Este tipo de extorsión digital tiene el potencial de afectar tanto a usuarios individuales como a grandes empresas.

5. Fraude en línea**:** Las estafas en línea implican una variedad de prácticas, como el fraude con tarjetas de crédito, donde los delincuentes obtienen ilegalmente datos financieros, y el fraude en subastas electrónicas.

6. Ciber espionaje**:** El ciber espionaje es el robo de información confidencial o no divulgada con fines políticos, económicos y militares es un delito importante. Individuos, grupos o gobiernos son todos posibles culpables.

7. Acoso en línea (ciberacoso)**:** Se trata del uso de dispositivos electrónicos para acosar, intimidar o calumniar a las personas. Las opciones disponibles incluyen amenazas, insultos en las redes sociales o la difusión continua de mensajes no solicitados.

8. Pornografía infantil en línea**:** La distribución, posesión o producción de material que involucra a menores en actividades sexualmente explícitas es ilegal y un grave delito cibernético.

9. Ingeniería social**:** La ingeniería social implica manipular a individuos para extraer información confidencial a través de medios psicológicos, esto se conoce como manipulación psicológica. El phishing o la coerción pueden dar lugar a la divulgación de contraseñas.

10. Violaciones de datos: Acceso a bases de datos que contienen información personal para luego divulgarla o explotarla. Una brecha en la protección de datos puede tener un impacto significativo en la privacidad y seguridad de las personas.

Desde el punto de vista doctrinario, (Palladino Pellón & Asociados, 2016) señala, el delito es un término legal utilizado para describir el comportamiento o acto que es ilegal y tiene consecuencias, éste atenta contra los principios establecidos en una ley y se considera una conducta que afecta negativamente a la sociedad. La omisión de un delito denota la violación de derechos y la alteración del orden social, considerándose una actividad ilícita, los delitos se definen y clasifican en códigos penales, que especifican los tipos de conducta punibles por ley y las multas o medidas correctivas asociadas.

Ahora, con respecto a la prevención del delito (Cusson, 2020) indica, este describe la implementación de planes e iniciativas destinadas a disminuir los delitos penales y al mismo tiempo fortalecer la seguridad nacional, este enfoque intenta abordar los factores tanto individuales como comunitarios que conducen al comportamiento delictivo, entre las distintas opciones abarca programas educativos, esquemas de alerta temprana, mayor alumbrado público, aplicación de la ley en los vecindarios, agentes de policía mejorados y políticas sociales específicas que aborden las causas profundas del crimen.

Asimismo, (Cusson, 2020) señala, el control del delito implica garantizar zonas seguras, aumentar la conciencia pública y fomentar la participación de la comunidad en la protección de los intereses individuales, la prevención del delito tiene como objetivo promover sociedades más seguras y resilientes abordando las causas profundas del delito y la justicia social.

Dados los antecedentes, conceptos y características se procede a analizar uno de los aspectos importantes, referente al derecho a la intimidad mismo que es el derecho que se ve más vulnerado de manera directa e indirecta hacia las víctimas sea una persona natural o jurídica, por tanto, se han tomado conceptos doctrinarios ya que el derecho a la intimidad está directamente ligado a los ataques de la ciberdelincuencia.

Para (Martínez, 2016, pág. 412) señala, la protección del espacio personal y el derecho a la privacidad o intimidad están ambos protegidos por la ley y los principios éticos, este derecho abarca la capacidad de salvaguardar datos personales, comunicaciones y actividades del acceso no autorizado, ya sea por parte de individuos, empresas o el gobierno, este concepto enfatiza la importancia de la intimidad para defender la dignidad humana y la libertad de cada individuo, en diversos ordenamientos jurídicos, este derecho es aplicable a la intimidad en el hogar y a las comunicaciones, así como a la información médica y a la identidad personal.

En la actualidad, la creciente amenaza del delito cibernético está entrelazada con el derecho a la privacidad o intimidad, es así como los avances en tecnología y conectividad mundial han generado numerosas ventajas, pero también han generado importantes preocupaciones con respecto a la protección y sensibilidad de la información personal, el objetivo de este apartado es la correlación entre el delito cibernético y la protección de la intimidad, examinando cómo las violaciones de seguridad digital afectan la información de las personas y qué medidas se han tomado para abordar estos riesgos.

Tal como lo señala (Salvador, 2022, pág. 42) el derecho a la privacidad se ve directamente amenazado por los ataques de delitos cibernéticos, el acceso y el robo de información personal, como datos de tarjetas de crédito o cuentas bancarias a pagar, puede ocurrir a través de una penetración no autorizada en el sistema informático, el acceso no autorizado puede provocar graves daños financieros y emocionales a las

víctimas, además de la pérdida de privacidad personal, además, la falta de autodeterminación puede generar vulnerabilidad y afectar la confianza en las plataformas en línea y los servicios digitales.

Desde otra perspectiva, (Salvador, 2022, pág. 43) determina, el robo de identidad, los ataques de software malignos y las filtraciones masivas de datos son parte del delito cibernético; la vulnerabilidad compartida de estas acciones es la capacidad de acceder, manipular o revelar información personal sin consentimiento, lo que podría potencialmente comprometer la privacidad, el acceso indebido a datos confidenciales socava el derecho fundamental a la privacidad, debilitando así la confianza y la autonomía de las personas en las plataformas digitales, es así que, estos tipos de ataques no sólo tienen implicaciones económicas, sino que también expone información de orden privada lo que se considera como una violación a la intimidad.

Por consiguiente, (Salvador, 2022, pág. 45) añade, este tipo de problemáticas han impulsado el establecimiento de marcos legales específicos para la protección de datos en el dominio digital, por lo que es necesario establecer estándares estrictos para garantizar la privacidad y seguridad de la información personal, estas regulaciones no sólo penalizan a las personas que violan los derechos de privacidad, sino que también promueven medidas de seguridad en las organizaciones que manejan y manipulan información sensible.

En definitiva, el no proteger la privacidad o la intimidad de las personas naturales y jurídicas es una total vulneración a los derechos de los mismos, para esto es necesario la aplicación de medidas de seguridad, cifrado de datos, transparencia en las políticas de privacidad, la protección tanto a los usuarios y sus contraseñas; por ello las empresas deben implementar medidas de seguridad desarrolladas que sean óptimas para la protección de la información tanto de la empresa como para el usuario, previniendo de esa forma los ataques cibernéticos con la finalidad de minimizar riesgos y maximizar seguridad en las redes.

Adicional, es necesario que los gobiernos adopten medidas preventivas para combatir los delitos cibernéticos y salvaguardar la privacidad de todo individuo y/o empresa privada o pública. Una medida a aplicar es la concientización sobre los riesgos

digitales, la educación a la ciudadanía sobre prácticas de seguridad en la Web, así como la promoción de la responsabilidad digital, que en conjunto son una serie de componentes fundamentales para combatir esta problemática.

El ciberdelito y su interacción con la inteligencia artificial

El ciberdelito se ha convertido en una problemática generalizada en los últimos años, que afecta tanto a personas naturales y jurídicas tanto del sector privado y público, es así como la continua evolución tecnológica lamentablemente es aprovechada por este tipo de personas o grupos organizados que se dedican a la ciberdelincuencia utilizando sistemas o plataformas digitales para cometer actividades ilícitas.

Como lo manifiesta (Bartolomé & Monteiro, 2021, pág. 70), la capacidad de las autoridades para combatir amenazas digitales se ha visto comprometida por el crecimiento exponencial de las actividades relacionadas con los ciberdelitos lo cual ha traspasado las fronteras tradicionales, aún más con la llegada de la pandemia (año 2020) a causa del COVID 19, se intensificó la vulnerabilidad del ciberespacio por el giro que tomó la vida laboral de muchas personas y empresas que optaron la digitalización como mecanismo para la generación de recursos; no obstante, esto originó la aparición masiva de ataques, tales como el phishing en donde los ciberdelincuentes se aprovecharon del miedo y la incertidumbre para engañar a las personas de manera fraudulenta extrayéndose su información confidencial.

Así también (Salvador, 2022, pág. 45) añade, se evidenció el aumento significativo de los ataques de ransomware o secuestro de datos, dirigidos a empresas y organizaciones quienes debido a la transición al trabajo remoto no contaban con sistemas de seguridad robustos y muchas de éstas fueron presas fáciles para los ciberdelincuentes.

Por consiguiente, a partir de la pandemia del COVID 19 se notaron cambios significativos en todo el mundo, en donde la mejor alternativa fue el adoptar la virtualidad en la vida cotidiana de las personas y empresas, hecho que fue aprovechado por los ciberdelincuentes, quienes utilizan herramientas tecnológicas cada vez más sofisticadas, incluso implementando la IA, con el propósito de que sus delitos sean más eficientes y anónimas, que por lo general quedan en la impunidad por la utilización de herramientas

y mecanismos tecnológicos que permiten cada vez ser menos localizados gracias al uso de la calidad tecnológica que adoptan para cometer los ciberdelitos.

De acuerdo con (Ospina & Sanabria, 2020, pág. 208) entre las técnicas de ciberdelincuencia más destacables se encuentran las que emplean inteligencia artificial para lanzar ataques de phishing o suplantación de identidad, fraude en línea, ataque a plataformas sofisticadas; la manera de operar está ligada al comportamiento de los mensajes y correos electrónicos, los ciberdelincuentes desarrollan algoritmos de aprendizaje automático que pueden optimizar la orientación de los correos electrónicos.

Finaliza (Ospina & Sanabria, 2020, pág. 208) puntualizando respecto a, los ciberdelincuentes elaboran mensajes que sean a la vez convincentes y engañosos, ajustándolos en consecuencia a la mente del destinatario, lo que puede llevar a su exposición o disposición para hacer clic en enlaces dañinos o revelar datos confidenciales.

Mientras que, (Morán, 2021, pág. 291) indica, los ataques de ingeniería social respaldados por inteligencia artificial han ido en aumento, al utilizar modelos de lenguaje avanzados, los generadores de texto han podido crear correos electrónicos y contenido en línea que imitan el tipo de discurso utilizado por empresas legítimas, lo que dificulta que los usuarios o los sistemas los detecten.

Por otro lado, (Chávez, Malpartida, Villacorta, & Orellano, 2021, pág. 28) la detección e identificación mejoradas de malware (programas maliciosos) han sido posible asociar gracias al uso de IA, el uso de algoritmos de aprendizaje automático para eludir las defensas convencionales ha permitido a los ciberdelincuentes atacar debilidades específicas del sistema y de la red, esto es particularmente eficaz contra atacantes sofisticados, es decir se trata de la creación de malware que puede sufrir cambios en su comportamiento con el tiempo, dificultando su detección por parte de las soluciones de seguridad convencionales.

Así también, (Chávez, Malpartida, Villacorta, & Orellano, 2021, pág. 29) la IA ha contribuido a la evolución de los ataques de ransomware o códigos maliciosos utilizados por parte de los ciberdelincuentes, los cuales son manipulados para mejorar la efectividad y sofisticación de sus ataques, lo que se consigue con este tipo de actividades

es que los atracadores identifiquen de manera más fácil los sistemas informáticos vulnerables es decir aquellos que no cuentan con ciberseguridad de calidad, lo cual agiliza el robo de información, datos y en muchos casos ejecutan la sustracción de dinero.

Adicional, (Chávez, Malpartida, Villacorta, & Orellano, 2021, pág. 29) la IA por medio de ransomware y la utilización de algoritmos lo que se consigue es la obtención de información de sus víctimas tales como nombres, dirección de correos, información bancaria entre otros, con la recopilación de esta información los ciberdelincuentes analizan y personalizan los ataques por esta vía según la situación financiera de la víctima.

Como lo indica, (Banafa, 2018), la automatización de ataques es una tendencia que está siendo utilizada con mayor frecuencia por los sistemas de IA, los ciberdelincuentes se han vuelto expertos en ejecutar ataques por la web identificando y explotando automáticamente las vulnerabilidades de las plataformas informáticas, dichos ataques son cada vez más rápidos y frecuentes, lo que hace que dificulta a las organizaciones afectadas.

Determina (Banafa, 2018) respecto a, estas amenazas que se han vuelto más difíciles de detectar y mitigar por la utilización de la IA tomando en consideración que la tecnología está en constante evolución, muchas son las formas que se utilizan como algoritmos y lenguajes con IA, tales como el aprendizaje automático en las soluciones de ciberseguridad, para identificar comportamientos maliciosos y prevenir ataques en tiempo real, como parte de su plan defensivo.

Tal como lo manifiesta, (Comisión Económica para América Latina y el Caribe, 2020, pág. 4) la confianza en los canales de comunicación digitales se está viendo afectada por el aumento de los ataques de phishing y las técnicas de ingeniería social respaldadas por inteligencia artificial, estos ataques sofisticados crean una sensación de desconfianza y paranoia en la sociedad, lo que dificulta diferenciar entre información legítima e intenciones maliciosas.

La disminución de la participación en línea y la mayor cautela en la comunicación digital pueden provocar un cambio en la dinámica social y la forma en que las personas

interactúan en línea, además, las repercusiones económicas y operativas de los ataques de ransomware dirigidos por IA están directamente vinculadas a las comunidades empresariales, las cuales sufren ataques financieros que afectan en gran medida al desarrollo de las empresas ocasionando perdidas e incluso el cierres de empresas y por ende afectando el empleo de sus colaboradores.

Por otro lado, (Comisión Económica para América Latina y el Caribe, 2020, pág. 6) señala que, las implicaciones sociológicas de la IA se pueden ver en la automatización de los ataques, lo que puede llevar a una mayor sensación de que las personas son vulnerables y carecen de control sobre cotidianidad laboral o financiera, esto puede causar ansiedad y miedo en la sociedad, causando un impacto significativo en la salud mental y emocional de las personas, provocando un mayor estrés y preocupación sociológica.

En definitiva, el control y la regulación a nivel gubernamental son urgentes y necesarios para combatir la amenaza del ciberdelito impulsado por la IA, puesto que se enfrenta a un delincuente sin rostro, por así decirlo. Por ende, los gobiernos deben implementar políticas públicas y entidades especializadas que promuevan la ciberseguridad en donde se establezcan estándares efectivos de protección de datos y privacidad, así como para combatir actos causados por la ciberdelincuencia.

A nivel mundial se percibe la problemática como una guerra invisible para la ciudadanía puesto que las organizaciones internacionales y gobiernos, se enfrentan a una lucha constante contra el ciberdelito, los cuales incluso como ya se ha demostrado en la investigación bibliográfica del presente estudio, no sólo ejecutan los ataques de la forma tradicional, sino que en la actualidad incluso utilizan herramientas tecnológicas sofisticadas que incluyen el manejo de IA; por tanto se requiere el trabajo de estrategias innovadoras tanto a nivel nacional e internacional acompañada de marcos legales y acciones gubernamentales para eliminar este tipo de amenazas.

Para (Pons, 2017, pág. 81) el paso inicial es mejorar el sistema legal mejorando las capacidades de los organismos encargados de hacer cumplir las leyes y normativas, proporcionando los recursos y la formación necesarios para investigar y combatir eficazmente los delitos cibernéticos, para esto se requiere mejorar la detección y

prevención de ciberataques desarrollando herramientas y técnicas forenses digitales en colaboración con el sector privado y el gobierno.

De igual manera, (Pons, 2017, pág. 82), el ciberdelito influenciado por la inteligencia artificial exige modificaciones en las leyes las cuales deben de ser más estrictas, esto incluye la definición explícita de delitos como el uso de algoritmos maliciosos, la manipulación de sistemas automatizados y la creación de malware altamente avanzado, de ahí la necesidad de que la mala utilización de este tipo de herramientas en delitos cibernéticos debería estar regulada por las legislaciones de cada país, creando un marco legal capaz de combatir este tipo de problemáticas.

Así también, (Juca, 2023, pág. 327) indica, los gobiernos deben mejorar su capacidad para investigar y procesar de manera efectiva los delitos cibernéticos, el contar con herramientas forenses digitales de calidad que a la vez les permita extraer información que sirva como pruebas para que los procesados sean judicializados en base a la ley, de ahí importancia que las personas y empresas quienes son víctimas de los ataques cibernéticos alerten de manera inmediata a las autoridades y estas trabajen de manera conjunta con el propósito de desmantelar este tipo de organizaciones que operan causando varios perjuicios a la sociedad en general.

De todo lo anteriormente señalado por los distintos autores, nace la importancia respecto a la responsabilidad innata y cuidado que tanto las personas y empresas adopten buenas prácticas en la protección de datos e información bajo la implementación de sistemas robustos de ciberseguridad, es esencial contar con tecnología avanzadas que permita identificar de manera inmediata posibles amenazas.

Por otro lado, la aplicación periódica de auditorías de seguridad son esenciales para mitigar posibles ataques cibernéticos mediante la identificación y corrección de posibles fallas en los sistemas se puede evitar que estos sean alterados, a través de estas auditorías se garantiza que los sistemas estén actualizados, configurados adecuadamente y cumplan con estándares de seguridad, con el propósito de minimizar el riesgo de ciberataques, esto se considera una medida preventiva y efectiva si son efectuadas con regularidad.

Como lo señala, (Maino, 2022, pág. 8) tanto los sectores público y privado deben trabajar juntos para lograr resultados satisfactorios, mediante el intercambio de información sobre posibles amenazas cibernéticas, lo que conlleva a soluciones conjuntas, una de estas medidas puede ser por medio de la implementación de capacitaciones sobre ciberseguridad tanto a personas y empresas para prevenir y a su vez protegerse contra las técnicas empleadas por los ciberdelincuentes, así también, la definición de normas y acuerdos internacionales promueven la cooperación en la investigación de los procesos aportando de manera activa en la coordinación de esfuerzos y el intercambio de información entre países.

En conclusión, las acciones preventivas como el uso de sistemas de seguridad desarrollados, la educación sobre ciberseguridad y la implementación de políticas de acceso seguro hacen que los sistemas, datos e información sean menos vulnerables a los ataques por ende la importancia de adoptar este tipo de medidas, por otro lado, la definición e implementación de medidas legales a nivel nacional e internacional por medio de leyes, normativas o tratados aportan a la criminalización de la ciberdelincuencia y contribuye con un marco legal claro y coherente que faculta a las autoridades a combatir de manera eficaz contra los delincuentes cibernéticos, estas medidas lo que pretenden es promover un entorno digital más seguro y confiable para la sociedad en general.

Análisis de las normativas legales

El Convenio de Budapest sobre ciberdelincuencia, fue creado con la intención de abordar los problemas emergentes del delito cibernético, en el año 2001 fue adoptado como un tratado internacional, este es el primer tratado internacional, tiene como objetivo crear estándares comunes para combatir el delito cibernético, un aspecto importante de este Convenio es su cobertura integral de diversas cuestiones relacionadas con el delito cibernético, este acuerdo incluye delitos relacionados con el uso no autorizado de equipos informáticos, la destrucción o corrupción de datos asociados con el sistema informático, el material ilegal en línea como la pornografía infantil. (Consejo de Europa, 2001).

Fundamentalmente dicho convenio proporciona disposiciones específicas para prevenir y perseguir los delitos cibernéticos, así como para facilitar la colaboración internacional en su investigación, proporciona instrucciones para la implementación de leyes nacionales que penalizan la actividad cibernética ilegal y fomenta la coordinación de las leyes, una de las características clave del Convenio es que hace hincapié en la cooperación transfronteriza, al enfatizar la escala global del cibercrimen, pues tiene como objetivo promover una colaboración más estrecha entre los Estados miembros, creando protocolos para detener a ciberdelincuentes, proporcionar pruebas electrónicas y colaboración en las investigaciones. (Consejo de Europa, 2001).

En definitiva, a lo largo de los años, el Convenio de Budapest ha sido ratificado por muchos países de todo el mundo como una herramienta base para el manejo de los delitos a causa de la rápida proliferación de los casos de ciberdelincuencia, este acuerdo sigue siendo una referencia importante en el campo de la ciberseguridad y la lucha contra el ciberdelito, proporcionando directrices y mecanismos legales para la cooperación internacional, este tratado no solo es adoptado por países de Europa, su impacto es significativo ya que impacta la forma en que los países manejan las cuestiones legales relacionadas con las actividades delictivas en línea y fomenta la seguridad del ciberespacio en todo el mundo.

Por otro lado, la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional (UNTOC), esta norma internacional fue diseñada para abordar diferentes tipos de crimen organizado, a pesar de la falta de un protocolo exclusivo para combatir el delito cibernético dentro de la convención, se encuentra un marco integral y su énfasis en la colaboración internacional pueden usarse como guía para abordar los problemas actuales. (Naciones Unidas, 2004).

Debido a su alcance global, el delito cibernético ha generado la necesidad de estrategias coordinadas a nivel mundial en relación con el crimen organizado, la UNTOC sirve como base para la cooperación global en la prevención, enjuiciamiento y castigo del delito cibernético, así como los principios de extradición, intercambio de información y asistencia jurídica mutua de la convención son esenciales para abordar los aspectos transfronterizos de los delitos cibernéticos (Naciones Unidas, 2004).

Además, la normativa señalada en el párrafo anterior, también llamada Convenio de Palermo aborda la cuestión del blanqueo de dinero, actividad delictiva vinculada al ciberdelito. La convención contra el lavado de dinero resulta útil para hacer frente a grupos criminales internacionales involucrados en actividades cibernéticas ilícitas, ya que buscan explotar las ganancias financieras de sus actividades. La rápida evolución del delito cibernético ha llevado a los Estados miembros y a la comunidad mundial a reconocer la importancia de adoptar medidas más específicas para combatir este tipo de actividades delictivas y su propósito principal es combatir el cibercrimen. (Naciones Unidas, 2004).

Adicional, en base a lo señalado por el Foro Global sobre Ciberseguridad (GFC) de la ONU su rol principal es combatir la lucha contra el cibercrimen mediante una plataforma internacional para el debate, la colaboración y el intercambio de mejores prácticas en ciberseguridad. Aunque no es un acuerdo vinculante, su metodología es importante en la gestión de la problemática asociada con el cibercrimen, como resultado de la creciente amenaza del delito cibernético, este foro destaca la naturaleza global de los sistemas digitales y la importancia de abordar colectivamente los desafíos de la ciberseguridad. (Global Cybersecurity Forum, 2024).

Sin embargo, el GFC es una plataforma que promueve el intercambio de ideas sobre políticas y estrategias de ciberseguridad, el cual tiene como objetivo originar la conciencia compartida sobre las amenazas cibernéticas y desarrollar estrategias efectivas y coordinadas para combatir el delito cibernético a través de conferencias, mesas redondas y eventos; en sí el foro es una herramienta de gran ayuda para que gobiernos, empresas y otras partes interesadas colaboren y compartan información y al mismo tiempo para combatir las amenazas cibernéticas. Su función como centro de discusión, colaboración e intercambio de información es esencial para el avance de la ciberseguridad global y a la vez es un aporte para interactuar con la sociedad en general (Global Cybersecurity Forum, 2024).

Al efecto, la Constitución de la República del Ecuador de 2008, establece principios generales y derechos constitucionales y no aborda de manera específica sobre el crimen cibernético, no obstante, este tipo de delitos vulnera algunos derechos de las

personas, quienes en esencia son afectadas en su privacidad, seguridad, la libertad de expresión, que es el resultado de una sociedad que se ha vuelto más dependiente de la tecnología, y es ahí que los ciberdelincuentes encuentran nuevas formas de vulnerar los derechos anteriormente mencionados.

En base a lo establecido en la Constitución 2008, que otorga a sus ciudadanos el derecho a la privacidad, el derecho a la protección de datos de carácter personal, así como el derecho a la inviolabilidad y al secreto de la correspondencia física y virtual estos están determinados en su artículo 66, por otro lado, de acuerdo con lo establecido en el artículo 3, en donde es deber del Estado el garantizar la seguridad integral (Ecuador, Asamblea Constituyente, 2008).

No obstante, a pesar de que existen derechos y deberes estipulados en la Constitución de Ecuador de 2008, como la privacidad, la protección de datos y la seguridad integral, estos son vulnerados cuando se ejecutan actos ilícitos como el robo de identidad o ataques cibernéticos que conducen a la vulneración de estos derechos; el defender la libertad de información en línea y salvaguardar los datos mediante la ciberseguridad es fundamental para prevenir estos actos, tomando en cuenta la particularidad de que el Estado ecuatoriano es el encargado principal de garantizar los derechos de los ciudadanos.

Por otro lado, de acuerdo con el artículo 19 de la Constitución 2008, el Estado está obligado a controlar la información, que incluye el uso del lenguaje o elementos ofensivos para salvaguardar la reputación y el honor de la población, en base a lo expuesto por esta disposición puede relacionarse con casos de ciberdelitos que involucran la difamación, calumnia o ataques a la reputación en línea, es así que la difusión de este tipo de contenido puede tener graves consecuencias para la víctima, incluyendo daños emocionales y sociales, de ahí la importancia que las personas hagan prevalecer sus derechos para que el Estado implemente medidas de control y prevención, protegiendo así los derechos de las personas naturales y jurídicas.

Así también, los delitos informáticos en el Ecuador están regulados por el Código Orgánico Integral Penal, de aquí en adelante COIP, figura legal que describe los delitos y sanciones penales como, por ejemplo, el acceso no autorizado a sistemas informáticos,

ataques cibernéticos, acoso digital entre otros, en tal virtud este ordenamiento legal señala:

La vulneración de la intimidad es un delito tipificado en el artículo 178 del COIP, cometido por un sujeto activo y se sanciona con hasta 3 años de prisión, mientras que, si comete fraude mediante el uso de dispositivos electrónicos para alterar, modificar, clonar o duplicar los dispositivos originales del cajero automático, se enfrenta a entre cinco y siete años de prisión (Ecuador, Asamblea Nacional, 2014).

De igual forma, el COIP en el artículo 190, estipula:

> La persona que utilice fraudulentamente un sistema informático o redes electrónicas y de telecomunicaciones para facilitar la apropiación de un bien ajeno o que procure la transferencia no consentida de bienes, valores o derechos en perjuicio de esta o de una tercera, en beneficio suyo o de otra persona alterando, manipulando o modificando el funcionamiento de redes electrónicas, programas, sistemas informáticos, telemáticos y equipos terminales de telecomunicaciones, será sancionada con pena privativa de libertad de uno a tres años. La misma sanción se impondrá si la infracción se comete con inutilización de sistemas de alarma o guarda, descubrimiento o descifrado de claves secretas o encriptadas, utilización de tarjetas magnéticas o perforadas, utilización de controles o instrumentos de apertura a distancia, o violación de seguridades electrónicas, informáticas u otras semejantes (Ecuador, Asamblea Nacional, 2014).

Por otro lado, el artículo 231 del COIP, impone sanciones a quienes modifiquen, manipulen o alteren programas de orden informático, sistemas telemáticos para obtener activos de otros para obtener ganancias financieras, así como cualquiera que proporcione detalles financieros para recibir activos mediante transferencias electrónicas también enfrentará consecuencias. La duración de la pena de prisión en ambos casos oscila entre tres y cinco años, lo que se busca con esta normativa es prevenir a los ciudadanos sobre este tipo de delitos y que conozcan que estos actos se encuentran regulados y que son sancionados y castigados con todo el rigor de la ley, así también, se busca salvaguardar la seguridad financiera y personal tanto de los ciudadanos como de las entidades (Ecuador, Asamblea Nacional, 2014).

En cambio, el artículo 232, en resumen destaca que, las personas declaradas culpables de destruir, dañar, alterar o manipular datos informáticos y sistemas

telemáticos o de telecomunicaciones se enfrentan a penas de prisión de tres a cinco años, también quienes desarrollan, publican o emplean software malicioso con el mismo objetivo se enfrentan a consecuencias penales, se estima una pena de entre cinco a siete años de prisión si la infracción se refiere a bienes informáticos vinculados con servicios públicos o seguridad ciudadana. Lo que se pretende con la aplicación de este código es disuadir la manipulación indebida de los sistemas tecnológicos contribuyendo así a la seguridad de la información digital de las personas y empresas.

El artículo 233 del COIP, establece:

> La persona que destruya o inutilice información clasificada de conformidad con la ley, será sancionada con pena privativa de libertad de cinco a siete años. La o el servidor público que, utilizando cualquier medio electrónico o informático, obtenga este tipo de información, será sancionado con pena privativa de libertad de tres a cinco años. (Ecuador, Asamblea Nacional, 2014).

Por consiguiente, el artículo 234 del COIP, indica:

> Acceso no consentido a un sistema informático, telemático o de telecomunicaciones.- La persona que sin autorización acceda en todo o en parte a un sistema informático o sistema telemático o de telecomunicaciones o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho, para explotar ilegítimamente el acceso logrado, modificar un portal web, desviar o redireccionar de tráfico de datos o voz u ofrecer servicios que estos sistemas proveen a terceros, sin pagarlos a los proveedores de servicios legítimos, será sancionada con la pena privativa de la libertad de tres a cinco años (Ecuador, Asamblea Nacional, 2014).

En definitiva, como se puede evidenciar el Estado ecuatoriano por medio del COIP se ha esforzado por incorporar dentro de su normativa las distintas normas y formas de delitos penales que pueden cometerse a través de medios electrónicos, informáticos y demás relacionados con estos, de ahí la importancia que los ecuatorianos tengan el conocimiento necesario que dichas prácticas ilegales están tipificadas con el propósito que sean denunciadas y atendidas por las entidades que corresponden y no queden en la impunidad. A continuación, se detalla un cuadro comparativo relacionando a los diferentes tipos de delitos informáticos que existen en Europa y América con los delitos informáticos establecidos en el COIP:

Tabla 2. Derecho comparado del delito informático

Derecho comparado del delito informático	
Tipos Penales en Europa y América	**Tipos penales en el COIP, Ecuador**
Delitos contra los sistemas informáticos: Acceso indebido Sabotaje informático Espionaje Informático Falsificación de documentos Distribución de virus	Art. 190.- Apropiación fraudulenta por medios electrónicos Art. 232.- Ataque a la integridad de sistemas informáticos Art. 234.- Acceso no consentido a un sistema informático, telemático o de telecomunicaciones.
Delitos contra la propiedad: Hurto, fraude Obtención indebida de bienes y servicios Manejo fraudulento de tarjetas inteligentes o instrumentos análogos Apropiación de tarjetas inteligentes o instrumentos análogos Provisión indebida de bienes o servicios	Art. 191.- Reprogramación o modificación de información de equipos terminales móviles. Art. 234.1.- Falsificación informática
Delitos contra la privacidad de las personas y de las comunicaciones: Violación de la privacidad de la data o información de carácter personal Violación de la privacidad de las comunicaciones Revelación indebida de data o información de carácter personal Calumnia, injuria, intimidad.	Art. 178.- Violación a la intimidad Art. 229.- Revelación ilegal de base de datos Art. 230.- Interceptación ilegal de datos Art. 233.- Delitos contra la información pública reservada legalmente
Delitos contra menores (niños, niñas y adolescentes): Difusión o exhibición de material pornográfico	Art. 103.- Pornografía con utilización de niñas, niños o adolescentes

Exhibición pornográfica de niños o adolescentes.	Art. 104.- Comercialización de pornografía con utilización de niñas, niños o adolescentes
Delitos contra el orden económico y patrimonio: Apropiación de propiedad intelectual Oferta engañosa	Art. 212.- Suplantación de identidad Art. 231.- Transferencia electrónica de activo patrimonial Art. 238.- Transporte y comercialización ilícitos y tráfico de bienes del patrimonio cultural Art. 239.- Falsificación o adulteración de bienes del patrimonio cultural Art. 240.- Sustracción de bienes del patrimonio cultural

Fuente: (Vega, 2022) (Ecuador, Asamblea Nacional, 2014)

En general se comprende que el ciberdelito es una problemática relevante que aún no ha transformado a la sociedad ecuatoriana, sin embargo, puede hacerlo ya que este tipo de delitos generan desafíos complejos que afectan la seguridad, la privacidad y la estabilidad económica. Por ende, este tipo de amenaza digital que actúa bajo el anonimato requiere no sólo capacidades técnicas y de seguridad, sino también políticas públicas y atención inmediata de parte del Estado ecuatoriano para prevenir cualquiera de los delitos tipificados en el COIP, para así llegar a una eliminación completa de estos.

Asimismo, es importante la divulgación de la existencia de estos delitos a la sociedad en general a través de campañas publicitarias, puesto que una sociedad informada y preparada estaría en alerta, lo cual ayudaría directamente a la prevención de los ciberdelitos, y de paso alivianaría la carga procesal de la Fiscalía, Policía Nacional y Unidades Judiciales.

Este tipo de actos delictivos desde el ámbito social impacta de manera significativa, ya que involucran desde la pérdida de información personal, el robo de identidad, la suplantación de identidad y el fraude financiero, todos estos comprometiendo la privacidad y a su vez causando intimidación e intranquilidad a la ciudadanía. Por otro lado, en los entornos empresariales que sufren ciberataques, dan

lugar al robo de propiedad intelectual causando interrupciones operativas, así como daños a la reputación.

Jurisprudencia

A partir del año 2021, entró en vigor la Ley Orgánica de Protección de Datos Personales (LOPDP) en Ecuador, ordenamiento jurídico que se catapultó debido a la sentencia No. 456-20-JP/21 de la Corte Constitucional del Ecuador, por lo que es bastante pertinente mencionar que la litis que se conformó debido al “sexting” entre dos estudiantes de colegio, puesto que una estudiante recibió y reenvió las fotografías íntimas de su compañera de clases.

La causa permitió conocer el fenómeno del sexting en los adolescentes dentro del ámbito educativo y las consecuencias que generó la intervención de las autoridades educativas del plantel, y el golpe psicológico y emocional que le produjo a la víctima que sus fotos íntimas estén en su entorno educativo. El desenlace de la litis determinó faltas graves por parte de la institución educativa que no supo afrontar ni escuchar a la víctima ni a la estudiante que compartió las fotos de la víctima, ambas terminaron por separarse de la institución educativa, por lo que de manera taxativa la Corte Constitucional evidenció las faltas al código de convivencia y evidentemente sanciona al Colegio por haber vulnerado el debido proceso. (Ecuador, Corte Constitucional, 2021)

Es así como, se demuestra la importancia de normativas legales acuciosas, perspicaces y eficaces para combatir el ciberdelito, sin que existan antinomias, ni lagunas jurídicas. Es fundamental que los diferentes ordenamientos jurídicos establezcan de manera clara los diferentes tipos de delitos informáticos, con el fin de que las autoridades y las instituciones correspondientes lleven a cabo investigaciones y procedimientos efectivos para evitar la impunidad de los actos ilícitos cometidos por ciberdelincuentes ya que en la actualidad sigue siendo un campo dinámico y en evolución constante por el uso de la IA, de ahí la necesidad de que la Asamblea Nacional debe revisar y modificar las normativas para manejar los riesgos emergentes y ofrecer soluciones eficientes en el campo jurídico.

El hecho de que se hayan establecido leyes, regulaciones y que las sanciones se apliquen claramente no significa que se ha producido una disminución del delito

cibernético, al contrario, ha aumentado en Ecuador, los más frecuentes están dados por la violación de la privacidad y el fraude. Los delitos cibernéticos también incluyen el robo de identidad, la falsificación, el uso de documentos falsos, el robo electrónico con fines fraudulentos y el acceso no autorizado a computadoras que resulta en daños a los activos de los usuarios de distintas plataformas y terminan siendo víctimas estancadas en el sistema judicial.

Las medidas efectivas para combatir el cibercrimen no implican únicamente la implementación de leyes y regulaciones, debe transformarse en un trabajo en conjunto de individuos, empresas, el Estado y la cooperación internacional. Respecto a los principios de legalidad, proporcionalidad, transparencia, seguridad y responsabilidad, siempre deben ser respetados por el Estado al momento de recopilar y procesar masivamente los datos personales de sus ciudadanos.

Una medida clave a adoptar es la inversión en educación tecnológica y concientización, es esencial para combatir esta problemática, puesto que el conocimiento insuficiente sobre los delitos cibernéticos con la falta de ciberseguridad son la causa fundamental de su ocurrencia. El conocimiento va de la mano con la educación tanto para las personas como para las distintas organizaciones, por ello son necesarias las campañas educativas públicas, la capacitación en ciberseguridad en entornos académicos y corporativos, para lograr la promoción de una cultura de ciberseguridad.

Por lo tanto, el Estado debe priorizar la implementación eficiente de la ciberseguridad, la cooperación entre las autoridades y las entidades competentes en conocer la litis para el seguimiento y la identificación de los ciberdelincuentes, de esa forma resolviendo eficazmente y receptivamente al delito cibernético, sobre todo garantizando que los profesionales de la seguridad cibernética y las instituciones del Estado tengan recursos adecuados para responder de manera efectiva a la ciberdelincuencia.

Como último punto, pero no menos importante es de urgencia y necesidad que las familias ecuatorianas protejan a los niños, niñas y adolescentes puesto que la red es tan amplia e infinita, por lo cual deben restringir su uso y promover el uso adecuado de la tecnología puesto que ya estamos hablando de generaciones que se criaron

prácticamente con el celular en la mano y esto produce cambios significativos en la crianza, por ende tanto padres como madres de familia deben estar atentos a cualquier mala práctica o amenaza que se pueda inmiscuir en la vida de los menores.

CONCLUSIONES

Primeramente, de acuerdo con las bases teóricas consultadas en referencia al ciberdelito existe una gran cantidad de información, fuentes que sin duda aportaron al desarrollo del presente estudio, dichas referencias bibliográficas fueron tomadas tanto de libros, ordenamientos jurídicos vigentes, jurisprudencia, revistas científicas de carácter legal, así como de sitios web los cuales otorgaron conocimientos sólidos y significativos para la comprensión, análisis y desarrollo de este.

En segundo lugar, es importante entender que a medida que la tecnología ha tenido avances significativos, este se ha vuelto un medio para cometer delitos, puesto que en la actualidad, los robos, fraudes son efectuados vía internet, incluso con el manejo de IA, la cual es utilizada por los ciberdelincuentes quienes están a la vanguardia tecnológica, ya que este tipo de herramientas les facilita para cometer de manera efectiva sus delitos; no obstante tanto las personas como empresas se ven obligadas a adoptar medidas de ciberseguridad para aplacar los ciberataques que en muchas ocasiones lo que causan son grandes pérdidas económicas.

En definitiva, es importante que tanto los organismos internacionales y nacionales por medio de los gobiernos estén en la constante búsqueda de crear, modificar y/o ajustar las diferentes normativas legales, a fin de contar con herramientas sancionatorias que permitan tanto a las personas, así como a fiscales, jueces y abogados contar con los suficientes elementos legales para abatir este tipo de crímenes. De la misma forma, es deber del Estado, educar a sus ciudadanos sobre medidas preventivas, así como, dotar de suficiente información para que procedan a denunciar cuando sean víctimas para que las autoridades efectúen las investigaciones pertinentes y actúen acorde a sus funciones.

RECOMENDACIONES

Una vez culminado el presente estudio, se recomienda que el sistema judicial ecuatoriano adopte políticas públicas para el cumplimiento de lo determinado por la Constitución, así como lo establecido en el COIP a fin de garantizar los derechos de las personas naturales y jurídicas. Además, se debe fomentar la educación continua en jueces, fiscales e incluso del personal judicial a cargo de lo concerniente a la materia de ciberseguridad, con la finalidad de manejar eficazmente los casos relacionados con la informática y a su vez garantizar que los procesos penales sean mucho más efectivos, transparentes y menos burocráticos, obviamente salvaguardando siempre los derechos constitucionales.

Por otro lado, se recomienda tanto para las personas naturales y jurídicas que tengan acceso a plataformas, sistemas, redes sociales, sitios webs, ejecuten controles de seguridad de manera continua, esto puede evitar el robo o suplantación de identidad, y para el caso de sistemas informáticos más sofisticados se recomienda la implementación de medidas como controles más extremos a los usuarios que manipulan los sistemas, así como mantener actualizado el software, utilizar antivirus, establecer contraseñas seguras, también realizar copias de seguridad y limitar el acceso a datos confidenciales, realizar auditorías periódicas a la red y actualizar regularmente las políticas de ciberseguridad.

Es fundamental desde la perspectiva socioeconómica que la Banca y la Policía Nacional trabajen en conjunto con la finalidad de que puedan manejar la problemática de los ciberdelitos, que en la actualidad tiene mayor efectividad debido al apoyo de la IA, y desde una visión más humana es imperioso contar con un sistema educativo en pro de valores para que el uso de la tecnología no tenga un efecto negativo en la sociedad, como se pudo evidenciar en el caso No. 456-20-JP/21.

BIBLIOGRAFÍA

Acurio, S. (08 de agosto de 2015). *Derecho penal informatico*. Recuperado el 08 de enero de 2024, de https://www.academia.edu/19803737/Derecho_Penal_Inform%C3%A1tico

Banafa, A. (27 de marzo de 2018). *Inteligencia Artificial en ciberseguridad: retos*. Recuperado el 15 de enero de 2024, de https://www.bbvaopenmind.com/tecnologia/inteligencia-artificial/inteligencia-artificial-en-ciberseguridad-retos/

Bartolomé, M., & Monteiro, A. (1 de abril de 2021). El ciberespacio, durante y después de la pandemia del Covid 19. *Revista Academia de Guerra del Ejército Ecuatoriano, 14*(1), 67-76. Recuperado el 13 de enero de 2024, de https://journal.espe.edu.ec/ojs/index.php/Academia-de-guerra/article/view/VOL14ART6/pdf

Boden, M. (2017). *Inteligencia artificial.* Madrid : Turner Publicaciones . Recuperado el 15 de Diciembre de 2023, de https://play.google.com/books/reader?id=LCnYDwAAQBAJ&pg=GBS.PP1.w.2.0.1&hl=es

Chávez, J., Malpartida, D., Villacorta, A., & Orellano, J. (diciembre de 2021). La influencia de la automatización inteligente en la detección del cibercrimen. *Boletín de Coyuntura Universidad Técnica de Ambato, 31*, 26-33. Recuperado el 14 de enero de 2024, de https://revistas.uta.edu.ec/erevista/index.php/bcoyu/article/view/1462

Comisión Económica para América Latina y el Caribe. (2020). *La ciberseguridad en tiempos del Covid 19 y el transito a la ciberinmudidad*. Recuperado el 15 de enero de 2024, de https://repositorio.cepal.org/server/api/core/bitstreams/6727e17b-6ebc-4544-b8cf-5f859a45fa28/content

Consejo de Europa. (23 de noviembre de 2001). *Convenio sobre la Ciberdelicuencia*. Recuperado el 19 de enero de 2024, de https://www.oas.org/juridico/english/cyb_pry_convenio.pdf

Cusson, M. (2020). *La Criminología.* París: Hachette.

Ecuador, Asamblea Constituyente. (2008). *Constitución de la República del Ecuador.* Quito: Registro Oficial N3- 449, 20 de octubre de 2008. Ultima modificacion: 25-ene-2021. Recuperado el 18 de enero de 2024, de https://www.ambiente.gob.ec/wp-content/uploads/downloads/2018/09/Constitucion-de-la-Republica-del-Ecuador.pdf

Ecuador, Asamblea Nacional. (2014). *Código Orgánico Integral Penal.* Quito: Registro Oficial N° 180 del 10 de febrero de 2014. Recuperado el 22 de enero de 2024, de https://www.defensa.gob.ec/wp-content/uploads/downloads/2021/03/COIP_act_feb-2021.pdf

Ecuador, Asamblea Nacional. (2015). *Código Orgánico General de Procesos.* Quito: Registro Oficial S. 506 del 22 de mayo de 2015. Última Reforma 05 ene 2024.

Ecuador, Corte Constitucional. (10 de Noviembre de 2021). *Sentencia No. 456-20-JP/21.* Recuperado el 5 de Marzo de 2024, de http://esacc.corteconstitucional.gob.ec/storage/api/v1/10_DWL_FL/e2NhcnBldGE6J3RyYW1pdGUnLCB1dWlkOic2NTc4YWZiYi00ZTZhLTRjMzQtYTkyNC05MzYxYzNmOTE5YjEucGRmJ30=

Global Cybersecurity Forum. (2024). *Una plataforma global para la colaboración en el ciberespacio*. Recuperado el 19 de enero de 2024, de https://globalcybersecurityforum.com/

Jiménez, J. (2022). *Ciberdelicuencia: Evolución y relación con la actual situación de pandemia, nuevas modalidades y nuevas problemáticas*. Recuperado el 09 de enero de 2024, de Universidad de Salamanca:

https://gredos.usal.es/bitstream/handle/10366/150144/TG_Jim%C3%A9nezRozas_Ciberdelincuencia.pdf?sequence=1&isAllowed=y

Juca, F. (01 de septiembre de 2023). Ciberdelitos en Ecuador y su impacto social;panorama actual y futuras perspectivas. *Revista científica Portal de la Ciencia, 4*(2), 325-337. Recuperado el 13 de enero de 2024, de https://institutojubones.edu.ec/ojs/index.php/portal/article/view/394/693

Larrotta, R. (14 de Agosto de 2023). *Evolución y tendencias de ciberdelito en EE. UU. reveladas en el Informe del IC3 del FBI - 2022*. Recuperado el 09 de enero de 2024, de https://es.linkedin.com/pulse/evoluci%C3%B3n-y-tendencias-de-ciberdelito-en-ee-uu-reveladas-el-informe

Maino, V. (2022). *Estrategia Nacional de Ciberseguridad del Ecuador*. Recuperado el 18 de enero de 2024, de https://asobanca.org.ec/wp-content/uploads/2022/08/ESTRATEGIA-NACIONAL-DE-CIBERSEGURIDAD-DEL-ECUADOR-2022481.pdf

Martínez, J. (2016). El derecho a la intimidadde la configuración inicial a los últimos desarrollos de la jurisprudencia constitucional. *Universidad de la Rioja, 32*, 409-430. Recuperado el 13 de enero de 2024, de https://dialnet.unirioja.es/servlet/articulo?codigo=5712518

Mayer, L. (2018). Elementos criminológicos para el análisis jurídico-penal de los delitos informáticos. *Lus et Praxis, 24*(1), 159-206. Recuperado el 12 de enero de 2024, de https://www.scielo.cl/pdf/iusetp/v24n1/0718-0012-iusetp-24-01-00159.pdf

Meléndez, J. (25 de julio de 2018). *Delitos informáticos y ciberdelitos*. Recuperado el 08 de enero de 2024, de https://derechoecuador.com/delitos-informaticos-o-ciberdelitos/

Morán, A. (diciembe de 2021). Responsabilidad penal de la inteligencia artificial IA, ¿la proxima frontera? *Ius. Revista del Instituto de Ciencia Juríricas de Puebla, México, 15*(48), 289-323. Recuperado el 14 de enero de 2024, de https://www.scielo.org.mx/pdf/rius/v15n48/1870-2147-rius-15-48-289.pdf

Naciones Unidas. (2004). *Convención de las Naciones Unidas contra la delincuencia organizada transnaciona y sus protocolos*. Recuperado el 19 de enero de 2024, de https://www.unodc.org/documents/treaties/UNTOC/Publications/TOC%20Convention/TOCebook-s.pd

Narváez Montenegro, B. D., & Recalde Machado, G. E. (15 de julio de 2018). El delito informático en América. *Debate Jurídico Ecuador, 1*(1), 3-14. Recuperado el 14 de enero de 2024, de https://revista.uniandes.edu.ec/ojs/index.php/DJE/article/download/1206/602

Ospina, M., & Sanabria, P. (26 de noviembre de 2020). Desafíos nacionales frente a la ciberseguridad en el escenario global: un análisis para Colombia. *Revista Criminalidad, 62*(2), 199-217. Recuperado el 15 de enero de 2024, de http://www.scielo.org.co/pdf/crim/v62n2/1794-3108-crim-62-02-199.pdf

Palladino Pellón & Asociados. (2016). *Definición de delito*. Recuperado el 13 de enero de 2024, de https://www.palladinopellonabogados.com/definicion-de-delito/

Parlamento Europeo. (26 de marzo de 2021). *¿Qué es la inteligencia artificial y comó se usa?* Recuperado el 10 de enero de 2024, de https://www.europarl.europa.eu/news/es/headlines/society/20200827STO85804/que-es-la-inteligencia-artificial-y-como-se-usa

Pons, V. (26 de abril de 2017). Internet, la nueva era del delito: ciberdelito, ciberterrorismo, legislación y ciberseguridad. *Urvio, Revista Latinoamericana de Estudios de Seguridad, 20*, 80-93. Recuperado el 18 de enero de 2024, de https://revistas.flacsoandes.edu.ec/urvio/article/view/2563/2108

Rodríguez, I. (16 de Junio de 2023). *La inteligencia artificial y el cibercrimen*. Recuperado el 12 de enero de 2024, de https://www.auditool.org/blog/auditoria-de-ti/la-inteligencia-artificial-y-el-cibercrimen

Saltos, M., Robalino, J., & Pazmiño, L. (2021). Análisis conceptual del delito informático en Ecuador. *Revista Conrado, 17*(78), 343-351. Recuperado el 12 de enero de 2024, de http://scielo.sld.cu/pdf/rc/v17n78/1990-8644-rc-17-78-343.pdf

Salvador, W. (2022). Derecho a la intimidad y la ciberdelincuencia. Efectos sociales y económicosenvíctimas ecuatorianas. *Revista Mundo Financiero, 3*(9), 41-55. Recuperado el 13 de enero de 2024, de https://mundofinanciero.indecsar.org/revista/index.php/munfin/article/view/74/79

Torra, V. (2019). *¿Que es la inteligencia artificial?* Recuperado el 11 de enero de 2024, de Universidad de Catalunya: https://openaccess.uoc.edu/bitstream/10609/148039/3/QueEsLaInteligenciaArtificial.pdf

Vega, J. (2022). *Ciberdelitos.* Lima: Lustitia.