UNIVERSIDAD NACIONAL "SANTIAGO ANTÚNEZ DE MAYOLO"

ESCUELA DE POSTGRADO

TEORÍA DE LA IMPUTACIÓN OBJETIVA Y AUTORÍA MEDIATA DEL PROGRAMADOR DE INTELIGENCIA ARTIFICIAL PARA FINES DELICTIVOS EN EL PERÚ

Tesis para optar el grado de Doctor
en Derecho y Ciencias Políticas

RONALD REGAN LÓPEZ JULCA

Asesor: **Dr. JOSE ANTONIO BECERRA RUIZ**

Huaraz - Ancash - Perú

2023

Registro Nº : **TE113**

UNIVERSIDAD NACIONAL
"SANTIAGO ANTUNEZ DE MAYOLO"
ESCUELA DE POSTGRADO

ACTA DE SUSTENTACION DE TESIS

Los miembros del Jurado de Sustentación de Tesis Doctoral, que suscriben, reunidos en acto público en el Auditorio de la Escuela de Postgrado, de la Universidad Nacional "Santiago Antúnez de Mayolo" para calificar la Tesis presentada por el:

Maestro : **LÓPEZ JULCA RONALD REGAN**

Título : ***TEORÍA DE LA IMPUTACIÓN OBJETIVA Y AUTORÍA MEDIATA DEL PROGRAMADOR DE INTELIGENCIA ARTIFICIAL PARA FINES DELICTIVOS EN EL PERÚ.***

Después de haber escuchado la sustentación, las respuestas a las preguntas y observaciones finales, lo declaramos:

APTO, con el calificativo de Dieciocho (18)

De conformidad con el Reglamento General a la Escuela de Postgrado y Reglamento de Normas y Procedimientos para optar los Grados Académicos de Maestro y Doctor, queda en condición de ser aprobado por el Consejo de la Escuela de Postgrado y recibir el Grado Académico de Doctor en **DERECHO Y CIENCIAS POLÍTICAS,** a otorgarse por el Honorable Consejo Universitario de la UNASAM.

Huaraz, 19 de setiembre del 2023

Dr. Luis Wilfredo Robles Trejo
PRESIDENTE

Dr. Elmer Robles Blacido
SECRETARIO

Ph.D. Félix Claudio Julca Guerrero
VOCAL

Dr. José Antonio Becerra Ruíz
Asesor

Anexo de la R.C.U N° 126 -2022 -UNASAM

ANEXO 1

INFORME DE SIMILITUD.

El que suscribe (asesor) del trabajo de investigación titulado:

TEORÍA DE LA IMPUTACIÓN OBJETIVA Y AUTORÍA MEDIATA DEL PROGRAMADOR DE INTELIGENCIA ARTIFICIAL PARA FINES DELICTIVOS EN EL PERÚ

Presentado por: RONALD REGAN LÓPEZ JULCA

con DNI N°: 41715034

para optar el Grado de Doctor en :

Derecho y Ciencias Políticas

Informo que el documento del trabajo anteriormente indicado ha sido sometido a revisión, mediante la plataforma de evaluación de similitud, conforme al Artículo 11 ° del presente reglamento y de la evaluación de originalidad se tiene un porcentaje de : ...14%.... de similitud.

Evaluación y acciones del reporte de similitud para trabajos de investigación, tesis posgrado, textos, libros, revistas, artículos científicos, material de enseñanza y otros (Art. 11, inc 2 y 3)

Porcentaje	Evaluación y acciones	Seleccione donde corresponda
Del 1 al 20%	Esta dentro del rango aceptable de similitud y podrá pasar al siguiente paso según sea el caso.	◉
Del 21 al 30%	Devolver al autor para las correcciones y se presente nuevamente el trabajo en evaluación.	○
Mayores al 31%	El responsable de la revisión del documento emite un informe al inmediato jerárquico, quien a su vez eleva el informe a la autoridad académica para que tome las acciones correspondientes; sin perjuicio de las sanciones administrativas que corres andan de acuerdo a Ley.	○

Por tanto, en mi condición de **Asesor responsable**, firmo el presente informe en señal de conformidad y adjunto la primera hoja del reporte del software anti-plagio.

Huaraz,

25/10/2023

FIRMA

Apellidos y Nombres: Becerra Ruiz, José Antonio

DNI N°: 31673886

Se adjunta:

I. Reporte completo Generado por la plataforma de evaluación de similitud

NOMBRE DEL TRABAJO

TEORÍA DE LA IMPUTACIÓN OBJETIVA Y AUTORÍA MEDIATA DEL PROGRAMADOR DE INTELIGENCIA ARTIFICIAL PARA F

AUTOR

RONALD REGAN LOPEZ JULCA

RECUENTO DE PALABRAS

34164 Words

RECUENTO DE CARACTERES

202410 Characters

RECUENTO DE PÁGINAS

157 Pages

TAMAÑO DEL ARCHIVO

328.5KB

FECHA DE ENTREGA

Oct 25, 2023 4:59 PM GMT-5

FECHA DEL INFORME

Oct 25, 2023 5:01 PM GMT-5

14% de similitud general

El total combinado de todas las coincidencias, incluidas las fuentes superpuestas, para cada base d

- 11% Base de datos de Internet
- Base de datos de Crossref
- 10% Base de datos de trabajos entregados
- 2% Base de datos de publicaciones
- Base de datos de contenido publicado de Crossr

Excluir del Reporte de Similitud

- Material bibliográfico
- Material citado
- Material citado
- Coincidencia baja (menos de 8 palabras)

MIEMBROS DEL JURADO

Doctor Luis Wilfredo Robles Trejo — Presidente

Doctor Elmer Robles Blacido — Secretario

Ph. D Félix Claudio Julca Guerrero — Vocal

ASESOR

Doctor José Antonio Becerra Ruiz

Este trabajo está dedicado a Dios, fuente inagotable de sabiduría y fortaleza, sin quien nada de esto sería posible.

A mis queridos padres Macario y Esperanza, quienes han sido mi roca en los momentos más difíciles. Sin su amor, apoyo y sacrificio incondicional, esta tesis no habría sido posible. Gracias por ser mi inspiración y por dedicar su tiempo y esfuerzo en mi formación académica y personal.

A mi amada esposa Liz Quispe, mi compañera de vida y cómplice en cada logro. Tu paciencia, comprensión y motivación han sido fundamentales para alcanzar este objetivo. Gracias por compartir conmigo cada paso en este camino.

A mis adorables hijas Yaretzy y Ketzaly, quienes son mi mayor motivación y razón de ser. Espero que esta tesis les sirva de ejemplo de que con esfuerzo y disciplina se pueden alcanzar las metas que nos proponemos.

Con todo mi amor y gratitud, dedico este logro a mi familia, quienes han sido mi mayor apoyo y fortaleza en esta etapa de mi vida.

INDICE

Resumen

Esta tesis doctoral tuvo como propósito determinar los alcances de la imputación objetiva de la autoría mediata del programador de inteligencia artificial con fines delictivos en el Perú. Para lo cual se ejecutó una investigación de tipo teórico – dogmática, no experimental de corte transversal, a nivel explicativo, el mismo que se desarrolló bajo un enfoque cualitativo.

Los resultados que registraron fueron tanto a nivel dogmático y normativo, donde se mostró la existencia de vacío normativos para determinar la aplicación de la teoría de la imputación objetiva en los supuestos criminalidad con inteligencia, arribándose a la siguiente concluyente la adaptación de la teoría de la imputación objetiva para hacer frente a nuevos supuestos de criminalidad mediante inteligencia artificial.

Palabras clave: Inteligencia Artificial, Derecho Penal, Imputación Objetiva Autoría Mediata, Programadores.

Abstract

The purpose of this doctoral thesis was to determine the scope of the objective imputation of the indirect authorship of the artificial intelligence programmer for criminal purposes in Peru. For which a theoretical-dogmatic, non-experimental, cross-sectional investigation was carried out at an explanatory level, which was developed under a qualitative approach.

The results they recorded were both at a dogmatic and normative level, where the existence of a regulatory vacuum was shown to determine the application of the theory of objective imputation in the alleged criminality with intelligence, arriving at the following conclusive adaptation of the theory of objective imputation to confront new cases of criminality through artificial intelligence.

Keywords: Artificial Intelligence, Criminal Law, Objective Imputation, Indirect Authorship, Programmers.

INTRODUCCIÓN

La tesis se enfoca en los desafíos jurídicos planteados por la inteligencia artificial en el derecho penal, centrándose en la autoría mediata de los programadores de inteligencia artificial en actividades delictivas. A medida que la inteligencia artificial se incorpora en la vida cotidiana, los algoritmos avanzados y autónomos pueden potencialmente facilitar el delito y desafiar las convenciones legales tradicionales. Nuestro análisis examina el impacto de estos vacíos normativos y busca determinar la imputación objetiva del programador en casos de uso criminal de inteligencia artificial. La investigación propone la adaptación de la dogmática penal para enfrentar estos retos legales de la era digital.

En el Capítulo I, se desarrolla el planteamiento del problema sobre la inteligencia artificial y su influencia en la teoría de la imputación jurídica, concretamente en la actuación del programador y el usuario, estableciendo los propósitos, límites y justificaciones al estudio.

En el Capítulo II, desarrolla la parte del marco teórico encontramos diversos estudios doctorales que recogen la sintonía de la inteligencia artificial frente al derecho, luego se desarrolla las bases de la filosofía del paradigma sociocrítico, la epistemología que cuestiona la cientificidad del derecho como conocimiento, la epistemología jurídica que se enfoca en el conocimiento jurídico complejo y bajo interdisciplinariedad. También encontramos las bases teorías de la imputación objetiva, la autoría penal y el estado actual de la inteligencia artificial, concluyendo el planteamiento de la hipótesis y su categorización para el estudio.

En el Capítulo III, se desarrolla la parte de la metodología del estudio se trazó la línea de lo cualitativo, estudio jurídico filosófico, bajo nivel descriptivo

jurídico de la teoría de la imputación objetiva en contextos de inteligencia artificial, así como también se precisó que no es experimental de orden transversal, se precisó el enfoque y métodos generales como particulares en donde destaca la dogmática jurídica.

En el Capítulo IV, se desarrolla la parte de los resultados se estableció doctrinalmente el desarrollo de la filosofía y epistemología general como jurídica en los contextos del avance de la inteligencia artificial, también se trató la criminalidad con inteligencia artificial y sus modelos de imputación y se precisó los avances normativos sobre el tratamiento de la inteligencia artificial en el derecho internacional como interno y los casos emblemáticos del uso de inteligencia artificial.

En el Capítulo V, se desarrolla la parte de discusión, nuevamente recordamos la formulación de la hipótesis para luego proseguir con su contrastación en base a argumentos de orden doctrinal, normativo y de casos emblemáticos.

En las conclusiones se resalta la teoría de la imputación objetiva que propone un marco para evaluar la responsabilidad penal ante la IA, enfrentando desafíos y la complejidad sobre la atribución de responsabilidad entre programador, usuario y máquina. La inteligencia artificial desafía las normas tradicionales de autoría penal, requiriendo un nuevo marco jurídico y ético que equilibre la responsabilidad con la autonomía de la inteligencia artificial, adaptando el derecho penal a la era digital.

En las recomendaciones se sugiere la creación de un marco jurídico y ético específico para la inteligencia artificial, considerando los retos de la imputación objetiva, como la atribución de responsabilidad entre programador, usuario y

máquina. Este marco debe reflejar la rapidez con que la inteligencia artificial está transformando la sociedad y economía. Adicionalmente, se propone un análisis interdisciplinario que integre filosofía, epistemología, ciencias sociales y tecnología para un entendimiento profundo de la intersección entre inteligencia artificial y derecho penal.

El tesista.

Capítulo I

PROBLEMA DE INVESTIGACIÓN

1.1 Planteamiento y formulación del problema

1.1.1 Planteamiento del problema.

a) El Diagnóstico del problema

La inteligencia artificial es considerada como una disciplina autónoma, que no solo tiene desarrollo en el ámbito informático, sino también filosófico, conductual, legal, psicológico, pedagógico, neuronal, etc. Las implicancias de la inteligencia artificial en el derecho, ha tenido diversas afectaciones a los artistas como se puede observar en los derechos intelectuales o de creación obtenida por la inteligencia digital, en el diagnóstico estadístico de la conducta criminal, en las mejoras en la gestión de datos de la administración pública y entre otras ventajas sobre el derecho aplicado.

Las nuevas tecnologías han aportado diversas alteraciones, adaptaciones a las relaciones personales, al contexto social, revolucionando a la educación, renovando el mundo empresarial y el entendimiento de la naturaleza del ser humano. Una de estas tecnologías lo constituye la inteligencia artificial que bajo sus diversos enfoques buscan aproximarse a la razón y comportamiento humano; es decir busca aproximarse a la condición humana, generando nuevas categorías como inteligencias autónomas que pueden tener curso de acción independiente, situación que puede generar diversas implicancias jurídicas.

La inteligencia artificial se viene incorporando en la vida diaria. Teniendo en cuenta a Amigone et al. (2018) la inteligencia artificial ha sobrepasado el ámbito informático para su interrelación con lo económico y social, pues encuentra

presente en todo el ámbito de la vida moderna. De acuerdo con García (2019) el diseño de los sistemas de inteligencia artificial tiene connotaciones éticas, pues se les otorga complejos algoritmos para que puedan tomar decisiones tales como la conducción de vehículos autónomamente. Como lo hace notar Barrios et al. (2020) los programadores de algoritmos de la inteligencia artificial no solamente generan exclusiones y vulnerabilidades a la sociedad, aumentan la discriminación, la ignorancia y atentados a los derechos humanos de los ciudadanos. En consecuencia, la inteligencia artificial trae consigo eficiencia y desarrollo a la sociedad, pero a su vez problemas y vulnerabilidades que deben afrontarse mediante nuevas formas de control o adaptación de controles ya conocidos.

El derecho penal y procesal penal no se encuentra ajeno a los cambios producidos por la inteligencia artificial. De acuerdo con Hernández (2019) reconoce el financiamiento público y privado en pro de la inteligencia artificial, pero siempre bajo el dominio humano, pues puede obtener autonomía de decisión. Según Romeo (2018) en el caso Estado de Winconsin vs. Loomis, la Corte Suprema de dicho Estado se pronunció sobre la constitucionalidad del uso de algoritmos de inteligencia artificial para fundamentar un fallo judicial. Teniendo en cuenta a Morales (2021) menciona que se tiene que replantear la teoría y responsabilidad penal conforme a los avances de la inteligencia artificial. Es así, que la inteligencia artificial se convierte en una herramienta eficaz para ayudar a la indagación del delito mediante el procesamiento de información que puede ser relevante para las investigaciones y también para agilizar las decisiones en el proceso penal.

Es así, que dentro del derecho penal se puede apreciar que la utilización de la inteligencia virtual para fines delictivos, en donde se abre la cuestión

problemática la relación entre el programador (persona natural) y la inteligencia autónoma (agente inteligente). La razón es que la inteligencia artificial desarrolla curso de acción separado e independiente al programador; por lo que, dogmáticamente se viene discutiendo el reconocimiento de personalidad a la inteligencia artificial para otorgarle su condición de sujeto de derecho al igual que los fundamentos para otorgar derechos a la persona jurídica bajo la teoría de la ficción legal.

La incorporación de la tecnología viene modificando diversos contextos no solo fácticos sino también dogmáticos, normativos como jurisprudenciales en las ciencias penales. Corresponde analizar el vacío jurídico que se genera para la teoría de la imputación objetiva del programador como autor mediato mediante la utilización de la inteligencia autónoma (agente inteligente). Esta situación más concretamente se podría dar cuando el programador de inteligencia artificial programa un dron o robot sin control humano para que sea agente autónomo, con curso de acción independiente y así realizar daños o eventos delictivos que se realizan después de la programación y se prolongan en el tiempo y generan problemas de imputación, pues dicho agente se encuentra en la condición de seguir aprendiendo y desarrollando acciones más allá de los algoritmos programados gracias al autoaprendizaje que poseen.

En la era de la digitalización, la inteligencia artificial se ha convertido en una herramienta poderosa y omnipresente. Con base en Morales (2021) la inteligencia artificial para algunos se concentra en congeniar con la inteligencia humana y para otro sector en mejorar la inteligencia humana en labores que demandarían mucho tiempo, trayendo eficiencia y resultados.

Los innumerables beneficios de la Inteligencia Artificial también han dado lugar a la aparición de nuevos delitos y la transformación de delitos tradicionales, por lo que surge la necesidad de abordar la responsabilidad penal de los programadores, las empresas y los usuarios. Los sistemas jurídicos de derecho penal tradicional y ciberdelitos parecen insuficientes para enfrentar estos desafíos, los principios tradicionales de imputación y autoría, basados en la intervención directa o indirecta de un individuo en la comisión de un delito. Es así, corresponde comprender los alcances la imputación objetiva y la autoría mediata aplicadas al programador de Inteligencia Artificial para poder afrontar la presencia de este tecnología divergente y exponencial en nuestra sociedad.

b) Pronóstico positivo y negativo del problema

La inteligencia artificial frente al entendimiento de la razón humana resulta comparable y en otros supuestos no resulta comparable, por el grado de profundidad o labores que realizan. Dicho en las palabras de Barrios et al. (2020) lo humano se somete a nuevos retos con la inteligencia artificial en donde se deben discutir los derechos de naturaleza digital y los tecnoderechos cuyas respuestas se generan de la convivencia con dichas tecnologías. La inteligencia artificial al ser producto del ingenio humano también puede ser utilizada para conducta delictivas que, al no cubrirse mediante regulaciones en los sistemas jurídicos o el cuestionamiento de teorías penales existentes, pueden generar impunidad en el uso de esta tecnología. En consecuencia, resulta importante explorar sus efectos negativos.

El pronóstico negativo que se puede apreciar, es que bajo el criterio conservador de la teoría de la imputación objetiva se podría imputar al programador de la generación del riesgo desaprobado jurídicamente al construir una serie de

algoritmos para fines delictuales, quedando cercenada todo análisis amplio a los procesos disruptivos de la tecnología sobre el ser humano y la sociedad, pues también se debe observar que la inteligencia artificial puede llevar adelante actos daños y delictivos autónomos con curso independiente gracias a su aprendizaje autónomo, que no se vienen evaluando bajo la teoría de la imputación objetiva.

En otras palabras, se está dejando de adaptar las teorías penales a la disrupción o incorporación accidental de la tecnología al derecho penal, más concretamente al análisis de la autoría mediata establecida entre programador (Autor mediato) y la inteligencia artificial (ejecutor material) y como dicha unidad se prolonga en el tiempo, en consideración a que el agente inteligente lleva curso de acción independiente.

c) Control de efectos negativos del pronóstico

Para el control de los efectos negativos generados por la evaluación de la teoría de la imputación objetiva del programador de inteligencia artificial para el supuesto de autor mediato, se hace necesario llevar adelante la corrección de dichos vacíos mediante perspectivas a favor del ser humano y así como la adaptación de la dogmática penal.

Teniendo en cuenta a Barrios et al. (2020) la tecnología de la inteligencia artificial debe generar la mejora del humano y bajo la perspectiva transhumanista variará el concepto, conciencia, naturaleza del ser humano (p. 98). En este sentido, para la solución del problema de la inteligencia artificial en el contexto del programador (autor mediato) con el agente inteligente (ejecutor material), corresponde realizar la adaptación de la teoría de la imputación objetiva para un mayor acercamiento de la disrupción digital de estos avances tecnológicos.

Es por lo señalado, que si no se aborda adecuadamente esta problemática es probable que el número de delitos relacionados con la inteligencia artificial aumenten se pueda apreciar márgenes de la impunidad y se puede evidenciar inseguridad; es así que la ausencia de la teoría jurídica penal sólido para analizar el uso de la Inteligencia Artificial podría llevar a la comisión de delitos cada vez más sofisticados y difíciles de rastrear.

1.1.2 Formulación del problema.

a) Problema general

¿Cuáles son los alcances de la imputación objetiva de la autoría mediata del programador de inteligencia artificial con fines delictivos en el Perú?

b) Problemas específicos

¿Cuáles son las consecuencias jurídicas de los vacíos normativos en la imputación objetiva de la autoría mediata del programador de inteligencia artificial con fines delictivos en el Perú?

¿Cómo se superará los vacíos normativos en la imputación objetiva de la autoría mediata del programador de inteligencia artificial con fines delictivos en el Perú?

1.2 Objetivos

1.2.1 Objetivo general.

Determinar los alcances de la imputación objetiva de la autoría mediata del programador de inteligencia artificial con fines delictivos en el Perú.

1.2.2 Objetivos específicos.

Establecer las consecuencias jurídicas de los vacíos normativos en la imputación objetiva de la autoría mediata del programador de inteligencia artificial con fines delictivos en el Perú.

Exponer cómo se superará los vacíos normativos en la imputación objetiva de la autoría mediata del programador de inteligencia artificial con fines delictivos en el Perú.

1.3 Justificación

1.3.1 Justificación filosófica

La arista sobre la justificación filosófica del estudio resulta ser novedosa, pues poco se ha reflexionado sobre inteligencia artificial. La razón filosófica dentro de la ciencia jurídica también resulta ser novedosa por la disrupción digital de la inteligencia artificial y su crecimiento exponencial en la vida diaria. Como plantea Marquisio (2015) encontramos al positivismo, tradicional, constitucional, crítico y normativista, siendo el positivismo crítico que es alejado de la ideología, prescripción y descripción del discurso jurídico. Como plantea Morales (2023) el paradigma en el derecho se viabiliza mediante la argumentación evitando el reduccionismo del fenómeno jurídico, precisando que las fuentes del derecho no se concentran solo en la moral sino en lo social, valorativo, histórico e institucional.

En definitiva, las posturas con respecto a análisis crítico de la realidad jurídica se encuentran distribuidas en posturas post positivistas fundamentadas en teorías críticas, las mismas que tiene claras diferencias en las fuentes sociales, la unidad del sistema, la descripción o prescripción del discurso jurídico, entre otras. La teoría de la imputación objetiva como teoría moderna que regula la intervención

del derecho penal bajo la perspectiva de una sociedad de riesgo o potencialidad de peligro para deslindar entre las conductas con relevancia jurídica. Esta teoría merece ser analizada dentro del contexto de la sociedad de conocimiento e información con los avances de la inteligencia artificial y sus repercusiones en la naturaleza del ser humano.

1.3.2 Justificación epistemológica

El sustento epistemológico del estudio resulta innovador por la confluencia de diversas ciencias para abarcar a la inteligencia artificial. La epistemología, como lo hace notar Padrón (2007) es sinónimo de gnoseología o conocimiento general para el mundo anglosajón, para nuestro entorno es conocimiento científico con exclusión de los demás conocimientos, con las denominaciones de filosofía de la ciencia, teoría de la ciencia, "teoría de la investigación científica. De acuerdo con Cabrera-Ramírez & Cepeda-Retana (2022) la epistemológica legitima el conocimiento científico mediante la búsqueda de objetividad y elementos indispensables para la cientificidad.

Es así, que el estudio se justifica desde la epistemología de la teoría de la ciencia y se aleja de las reflexiones filosóficas de la ciencia, para poder buscar los elementos científicos del derecho penal y la tecnología, aspectos que se centran concretamente en el análisis de la teoría de la imputación objetiva dentro del derecho penal y la inteligencia artificial dentro del ámbito de la sociedad del conocimiento y la información, nuevos escenarios que vienen reformulando al ser humano y la sociedad tecnológica.

La epistemología del derecho debate como necesario el cuestionamiento de la cientificidad del derecho, situación que también abarca el abordaje de la

inteligencia artificial dentro del fenómeno jurídico. Desde la posición de Salamanca (2015) el conocimiento jurídico evaluado epistemológicamente cuenta con dos paradigmas epistemológicos jurídicos, uno denominado escepticismo, que deniega la categoría científica del derecho y el otro, que enarbola la cientificidad del conocimiento jurídico. Según Mendez et al. (2022) la epistemología jurídica se concentra en los sistemas, modelos teóricos y otros en la práctica institucional del derecho, en el constructivismo jurídico se concentra en la cientificidad del derecho y el objeto de verdad de la ciencia jurídica.

Es así, que bajo este aspecto consideramos al derecho como ciencia social que regula la conducta relevante bajo aspectos finalidades valorativas para garantizar la convivencia social, pues en nuestro estudio nos concentraremos en el derecho penal que regula las conductas bajo la última ratio y dentro de las garantías de la teoría de la imputación objetiva en los supuestos de la autoría concurrentes entre el programador y la inteligencia artificial autónoma dentro del contexto de una sociedad de la información, comunicación y tecnología, es decir bajo este análisis comparativo podrá llevarnos a establecer comparaciones multidisciplinarias e interdisciplinarias entre el derecho y la tecnología.

1.3.3 Justificación teórica

El sustento teórico del estudio fue bajo la línea del análisis de la teoría de la imputación objetiva y la autoría del derecho penal se encuentra fundamentada en el funcionalismo penal que se bifurca en el funcionalismo teleológico y normativo. Como expresa Garcete (2021) el funcionalismo teológico el derecho penal es subsidiario y de última ratio mientras que el funcionalismo normativo es de primera ratio y se edifica en la defensa y conservación de la norma penal. Mientras que la

razón teórica de la investigación se ubicó en el aspecto de en avance tecnológico de la inteligencia artificial como parte de la sociedad tecnológica, de conocimiento y de información. Como plantean Pérez et al. (2018) esta sociedad se relaciona con la tecnología y comunicaciones como nuevas realidades de aprendizaje, mientras que otra precisa que es reduccionista en el uso de la tecnología y otra postura como medio de comunicación.

Es así, que teóricamente nos fundamentamos en postura que la sociedad del conocimiento e información es reduccionista respecto a que los procesos sociales se vienen estableciendo mediante la tecnología y así generan nuevos escenarios problemáticos como la inteligencia artificial, que debería asumir de manera equilibrada entre un funcionalismo teológico o normativo.

1.3.4 Justificación metodológica

La razón metodológica del estudio, se bifurca entre los estudios jurídicos penales y la tecnología de la inteligencia artificial. Como plantea Paoli (2019) lo multidisciplinario es participación comunitaria de disciplinas sin dejar el objeto ni método, lo interdisciplinario es integración teórica, del objeto y método para otorgar otra perspectiva de estudio que puede llegar a su plenitud a lo que se denomina transdisciplinario. Como plantea Caceres (2023) reconoce que el tratamiento de la inteligencia artificial en el derecho evoca a lo interdisciplinario o transdiciplinario, entre lo teórico y práctico.

En consecuencia, la teoría jurídica no solo debe quedarse en un trabajo de razonamiento sobre sí misma, sino que también debe implicar otros conocimientos que complementan, amplían el conocimiento jurídico como el caso de la

inteligencia artificial que tiene implicancias con la informática, estadística, matemáticas, psicología, sociología y otras ramas científicas.

A nivel metodológico el presente estudio es cualitativo, dogmático-jurídico y bibliográfico documental. La teoría de la imputación objetiva y de la autoría penal se analizará conforme a la dogmática penal vigente dentro del contexto del funcionalismo penal normativo.

La inteligencia artificial se analizará bajo la teoría de la sociedad del conocimiento e información. Ambos análisis se concentrarán en un tratamiento adaptativo de la tecnología de inteligencia artificial a la teoría y dogmática jurídica penal, mediante el tratamiento multidisciplinario y tratando de llegar a establecer lo interdisciplinario entre el derecho y la tecnología.

1.3.5 Justificación social

El estudio se justifica en los alcances de la sociedad del conocimiento y la información que tiene como herramienta principal la tecnología que pone disposición el conocimiento, comunicación, desarrollo e investigación para reformular los paradigmas de la naturaleza humana, las relaciones sociales y la sociedad actual.

Es así, que la presencia de la inteligencia artificial en la vida cotidiana no solo mejor la convivencia humana mediante eficiencia y eficacia en los procesos productivos con en la vida cotidiana, sino también que puede generar actos dañosos y delictivos que deberán ser analizados bajo la teoría de la imputación objetiva en el supuesto de la autoría penal que se genera entre el programador y el agente inteligente autónomo con curso de acción independiente.

1.3.6 Justificación jurídico-legal

La presente investigación se justifica de manera jurídica-penal mediante la Constitución Política del Estado que garantiza la investigación científica en la educación universitaria (primer párrafo del art. 18°). En este mismo sentido también se fundamenta en el derecho constitucional de la Autonomía Universitaria en donde se ha establecido el régimen y líneas de investigación (último párrafo del art. 18°).

En el ámbito de la Universidad, este estudio se justifica en la Ley Universitaria – Ley 30220, pues en el primer párrafo del art. 1, establece como fundamento la investigación, en el principio espíritu crítico y de investigación regulada en el numeral 5.6 del art. 5 de dicha Ley. Además, en el Estatuto de la Unasam, aprobado con Resolución N° 001-AE-UNASAM-2015, el mismo que en su numeral 9.5 del art. 9 establece como fin de la UNASAM la investigación científica, tecnológica y humanística y demás reglamentos de Grados y Títulos emitidos dentro de su autonomía normativa como académica.

1.3.7 Justificación práctica

La teoría de la imputación objetiva dentro del derecho penal, sirve para establecer el funcionamiento y roles de la sociedad de riesgo, pero no todos los contextos de la sociedad son iguales, pues en el contexto premunido de tecnología, como en el caso de inteligencia artificial, es donde se podrá establecer diversos alcances para analizar o cuestionar los alcances de esta teoría penal frente a los supuestos del programador y agente inteligente como autor mediato y ejecutor material.

1.4 Delimitación

1.4.1 Delimitación teórica

La imputación objetiva como teoría se delimitará en la dogmática-jurídica de la teoría de la imputación jurídica y su adaptación al fenómeno de la inteligencia artificial, doctrina que se viene aplicando a la luz de la jurisprudencia nacional como extranjera para poder establecer sus diversas categorías como subcategorías materia de estudio.

La inteligencia artificial teóricamente se delimitará en los aspectos delictivos de dicha tecnología registrados dentro de la teoría europea como en Estados Unidos, para poder establecer la imputación objetiva del programador frene al agente inteligente.

1.4.2 Delimitación temporal

El estudio se delimitó durante el año 2022-2023.

1.4.3 Delimitación social

La sociedad peruana no se encuentra exentas de formar parte de la sociedad del conocimiento e información y la imputación objetiva por motivos de la globalización también tendrá sus afectaciones en los fenómenos delictuales que utilizan inteligencia artificial.

Capítulo II

MARCO TEÓRICO

2.1 Antecedentes de la investigación

2.1.1 Antecedentes internacionales

Meza (2020) la indagación científica de su tesis doctoral tuvo como propósito determinar los alcances de los elementos de la imputación objetiva en el supuesto de la omisión de actuaciones administrativas que desembocan en responsabilidad extracontractual estatal. La hipótesis estableció que el funcionalismo puede construir dogmáticamente fundamentos para el derecho administrativo más concretamente en los actos, funciones y servicios estatales que ante la omisión pueden generar responsabilidad civil extracontractual estatal. La metodología es cualitativa y mediante la técnica documental enfocada en la dogmática jurídica de la imputación objetiva y la responsabilidad estatal. Las conclusiones establecen que la teoría de la imputación objetiva es apropiada para determinar alejarse de la causalidad y de la justicia retributiva de la justicia administrativa por omisión administrativa estableciendo criterios concretos para establecer la responsabilidad administrativa del Estado en materia extracontractual.

Zornoza (2020) en la tesis de doctorado en derecho tuvo como propósito analizar el manejo autónomo de vehículos, sin intervención humana, frente a su impacto en los accidentes de tránsito, la responsabilidad civil y los seguros. La hipótesis establece que para la determinación de la responsabilidad civil por producto defectuoso en el supuesto de conducción no tripulada (autónomo) tanto en España como en Italia no necesitan muchos ajustes, recayendo dicha responsabilidad sobre el fabricante, inclusive por productos defectuosos. La

metodología del estudio fue cualitativa, investigación jurídica en el ámbito dogmático y normativo comparativo entre el sistema jurídico español e italiano, mediante la técnica documental-bibliográfica. Las conclusiones precisan que los vehículos autónomos mediante inteligencia artificial si bien es cierto a nivel internacional no se reconoce de manera expresa su responsabilidad por la falta de control humano o su posterior retorno de control; es así que la legislación española como italiana no regulaban los niveles de automatización que ayudan a establecer la responsabilidad civil por productos defectuosos, en donde el fabricante, el operador y conductor de respaldo son responsables de la creación del peligro.

Terrones (2021) en su tesis doctoral tuvo como propósito el análisis reflexivo de la inteligencia artificial responsable dentro del contexto histórico y revolucionario de la tecnología y el transhumanismo. La hipótesis se centraliza en el planteamiento de criterios, habilidades filosóficas y cívicas para afrontar responsablemente el tránsito de la inteligencia artificial con el transhumanismo. La metodología fue cualitativa, bajo un ámbito multidisciplinario con la ética, filosofía, política y el derecho para establecer la responsabilidad frente a la tecnología de la inteligencia artificial. La técnica fue documental – bibliográficas respecto las ciencias descritas de manera multidisciplinaria. Las conclusiones establecen que el ser humano como creador de la inteligencia artificial no puede desconocer en dichos avances su condición y naturaleza humana frente a los intereses empresariales, siendo los límites la administración adecuada, el servicio al ser humano y la regulación éticos y jurídicos.

Suárez (2020) en su tesis doctoral concentra su propósito en el estudio de la función jurisdicción y la labor del Juez con el apoyo de inteligencia artificial como

procesos de modernización de la administración de justicia con el uso de tecnologías móviles por los usuarios o litigantes en España y la Unión Europea. La hipótesis establece que en el marco de implementación de la justicia digital mediante inteligencia artificial se debe establecer un marco de carácter ético y jurídico que apoye la gestión y adapte al derecho administrativo y procesal que tenga relación con este tipo de tecnología. La metodología es cualitativa, estudio jurídico dogmático, normativo y jurisprudencial en el ámbito de España y la Unión Europea. Mediante la técnica documental – bibliográfica. Las conclusiones precisan que las formas alternativas de solución de conflictos y servicio de justicia usan inteligencia artificial y tecnología móvil para mejorar la prestación, eliminando la burocracia que se puede advertir de los derechos administrativos y procesales aplicables a la justicia, así mismo se puede modernizar y mejorar la celeridad, pero no reemplazar las labores jurisdiccionales.

2.1.2 Antecedentes nacionales

Ayasta (2021) en su tesis doctoral formula que el propósito del estudio fue determinar si la gestión y distribución de energía mejora con la automatización de la inteligencia artificial aplicada a estos procesos. La hipótesis establece que la inteligencia artificial se integra con la gestión, distribución, comunicación de los sistemas informáticos para la distribución de energía. La metodología es una investigación aplicada, descriptiva correlacional, la técnica fue el cuestionario y guía de observación en trabajadores del grupo empresarial Distriluz durante los años 2014-2018. Las conclusiones establecieron relación entre los sistemas informáticos y empresariales mediante inteligencia artificial que se garantizó en la gestión de la distribución de la energía eléctrica.

Solís (2019) en su tesis doctoral indica que el propósito del estudio se centró en el impacto de la tecnología de la inteligencia artificial sobre los entornos y construcción de las aplicaciones móviles. La hipótesis precisa que la elaboración de aplicaciones móviles mejora con la inteligencia artificial mediante moldeamientos de predicciones y reglas de dicha tecnología. La metodología fue aplicada bajo el enfoque de corte cuantitativo, mediante el modelamiento de inteligencia artificial para móviles con 75 usuarios de Lima metropolitana y 05 expertos. Las conclusiones establecen que las técnicas de inteligencia artificial (redes neuronales) fortalecen significativamente la construcción de aplicaciones móviles a satisfacción de los usuarios.

Carretero (2018) en su tesis doctoral establece que el propósito del estudio es la determinación de exoneraciones de responsabilidad de índole penal en los supuestos de accidentes de tránsito conforme a los alcances de la teoría de la imputación objetiva. La hipótesis establece que se podrá descongestionar la carga procesal por delitos referentes a accidentes de tránsito mediante la utilización de la imputación objetiva. La metodología del estudio es cualitativa, a nivel jurídico empírico-jurídico, la técnica mediante cuestionario aplicado a jueces, fiscales y abogados en materia penal. Las conclusiones establecieron que la mayoría de los afectos tiene en cuenta en los delitos de accidentes de tránsito la autopuesta en peligro del conductor como de afectado, así como el riesgo desaprobado jurídicamente por parte del conductor.

2.1.3 Antecedentes locales

En la búsqueda de antecedentes locales de los repositorios de Alicia - Concytec y así como en los repositorios locales de la Universidad Santiago Antúnez

de Mayo y la Universidad César Vallejo, fue un resultado negativo, pues en la búsqueda de tesis de doctorado no se encuentran tesis sobre imputación objetiva o inteligencia artificial.

2.2 Bases filosóficas y epistemológicas

2.2.1 Bases filosóficas

Las bases filosóficas de la investigación científica se centran en los paradigmas o bloques filosóficos para otorgar una perspectiva para orientar, programar y ejecutar el estudio.

La imputación objetiva como teoría penal también trata de superar la visión causalista o de equivalencia de condiciones para establecer responsabilidad penal en una sociedad moderna; es decir trata de actuar con justicia y racionalidad conforme al entendimiento de la asignación de roles sociales de los ciudadanos bajo determinados contextos.

Por su parte, el tratamiento de la inteligencia artificial dentro de la filosofía encuentra posturas que la califican como deshumanizante. Teniendo en cuenta a Barrios et al. (2020) precisa que bajo el trans y post humanismo la inteligencia artificial y sus múltiples aplicaciones trae consigo la reconfiguración de la sociedad como de la cultura, así como naturaleza y comprensión humana. Desde la posición de Rodríguez (2022) el ser humano es la representación que él mismo realiza durante la historia y avance de la sociedad, siendo la inteligencia artificial una nueva forma de humanización o desarrollo posthumano. En definitiva, es apropiado analizar estos nuevos escenarios dejados por la inteligencia artificial, bajo el paradigma el socio-critico, pues estas tecnologías vienen erosionando los cimientos de la sociedad como de entendimiento del ser humano en sociedad.

La investigación se fundamenta en la postura positivista enfocada en el tratamiento normativo como estático del derecho, de los discursos prescriptivos como descriptivos del derecho, para poder construir un derecho más justo y conforme a la sociedad moderna. Es así, que se funda este estudio en la postura filosófica positivista crítica, postura que a criterio de Marquisio (2015) se encuentra muy marcado con las críticas constantes a la ideología, prescripción y descripción del discurso jurídico, siendo ello diferente a los post positivismos constitucionalismos y normativista. Según Garrido (2022) la neurociencia aplicada a la computación se enfoca replicar el cerebro humano en cada uno de sus procesos como visión autómata del hombre su ser.

En consecuencia, el positivismo adaptado para este estudio es el crítico, el mismo que tiene como base el alejamiento de tendencias positivistas jurídicas que entendía al sistema jurídico como único y perfecto y al discurso jurídico como acabado sin aceptar las indeterminaciones del lenguaje jurídico, dejando al criterio del operador jurídico la determinación del lenguaje jurídico sin razones, ni argumentación o estructuras de razonamiento para imputar efectos jurídicos a las diversas relaciones sociales. Es así, que bajo estos fundamentos se puede llevar adelante el cuestionamiento o adaptación de la teoría de la imputación objetiva del derecho penal frente al fenómeno de la inteligencia artificial con fines delictivos.

2.2.2 Bases epistemológicas

Desde la perspectiva de Hashimoto, (2010) es importante dentro de una adecuada metodología de la investigación partir de las bases corrientes o paradigmas que ayuden a llevar adelante la investigación, siendo los paradigmas el idealista, materialista o socio-critico. Con base en Escuela (2019) el idealismo es

inevitable a la razón humana, se concentra el sujeto y el objeto para que sean interpretados bajo el espíritu, descartando cuestiones característica del objeto. Según Gonzales (2018) el paradigma materialista es la realidad que se construye por procesos ajenos al sujeto, lo objetos de conocimiento otorgan posibilidades teóricas para su estudio. Como hace notar Rodríguez (2022) lo sociocrítico se fundamenta en la autonomía, reflexión y transformación de la ideología, el sistema social para buscar su transformación mediante el pensamiento crítico.

Es así que cada paradigma se distingue conforme a sus perspectivas e investigación que se afronte; es así que para el estudio de la teoría de la imputación objetiva y la inteligencia artificial tienen como fundamentos la criticidad de la sociedad y su adaptación a los nuevos cambios.

El paradigma socio-crítico resulta ser el que actualmente debe enfocar la investigación científica. Teniendo en cuenta a Loza et al. (2020) es la acción del investigador bajo autocrítica y transformación de la realidad, siendo necesario las propuestas de solución en esa conjugación entre teoría y práctica, en del derecho por ejemplo puede tener una crítica emancipadora de relaciones o grupos. Como afirma Bibiana et al. (2023) la acción del paradigma sociocrítico es la solución a los problemas para modificar la realidad o formas de reforma.

En consecuencia, el análisis sociocrítico del estudio se debe enfocar sobre la realidad de la inteligencia artificial y las transformaciones positivas como negativas que viene generando en el derecho, concretamente en la atribución de responsabilidad penal.

El paradigma sociocrítico ayuda a la comprensión de la inteligencia artificial dentro de las transformaciones que realiza a la sociedad. Desde la posición de Loza

et al. (2020) este paradigma trata de superar el conservadurismo de lo idealista y el reduccionismo del positivismo u objetivismo, para aportar una visión teórica y práctica de las ciencias sociales. A juicio de Bibiana et al. (2023) el paradigma sociocrítico que se caracteriza por lo dialéctico, apuesta en el sujeto social otorga la solución a la complejidad encontrada en la realidad.

En consecuencia, este paradigma es donde se puede encontrar a la sociedad del conocimiento e información que viene aportando la tecnología de la inteligencia artificial y también a la imputación objetiva que sirve para establecer a una sociedad de riesgo en donde debe delimitarse apropiadamente la responsabilidad penal.

La epistemología ha tenido diversas tendencias al momento de enfocarse en la ciencia como en la filosofía y la metodología de la investigación científica. Es así, que en este estudio partimos de la postura mayoritaria latinoamericana como teoría de la ciencia. Es en este sentido, que advierte Padrón (2007) es sinónimo de gnoseología o conocimiento general para el mundo anglosajón, para nuestro entorno es conocimiento científico con exclusión de los demás conocimientos, con las denominaciones de "filosofía de la ciencia", "teoría de la ciencia", "teoría de la investigación científica". Desde la posición de Gadea et al. (2019) la epistemología se encarga de cuestionar o derribar modelos de orden teóricos, lógicos, informacionales, entre otros, aspirando esta disciplina a abarcar el conocimiento complejo. En resumen, la epistemología general frente al derecho siempre encuentra cuestionamiento de los componentes y elementos como ciencia social y del mismo modo con la tecnología se podrá criticar sus acercamientos e interrelación las ciencias sociales, naturales o exactas.

En las bases de la epistemología del derecho surge el problema de su cientificidad como elemento indispensable para poder elaborar cualquier estudio o investigación. Como expresa Salamanca (2015) epistemológicamente el conocimiento jurídico es escepticismo o no científico y por otro lado, es aceptable su cientificidad. Es así, que partimos de la base que el derecho es ciencia, es una ciencia social que regula la conducta relevante bajo aspectos finalidades valorativas para garantizar la convivencia social. Como hace notar Caceres (2023) la epistemología del derecho se enfoca en la construcción de modelos epistémicos para que el profesional del derecho pueda establecer la verdad de las premisas relevantes que se encuentran en el discusión. Empleando las palabras de Paoli (2019) lo multidisciplinario es participación comunitaria de disciplinas sin dejar el objeto ni método, lo interdisciplinario es integración teórica, del objeto y método para otorgar otra perspectiva de estudio que puede llegar a su plenitud a lo que se denomina transdisciplinario.

En consecuencia, el otro escenario sobre las bases epistemológicas del derecho lo resulta ser su autosuficiencia o comunicación interna como externa con otras ciencias, en consideración a que el lenguaje jurídico resulta ser indeterminado, por lo que se plantean escenarios como la multidisciplinariedad, interdisciplinariedad y transdisciplinariedad del derecho.

En nuestro estudio nos concentraremos en el derecho penal que regula las conductas bajo la última ratio y dentro de las garantías de la teoría de la imputación objetiva en los supuestos de la autoría concurrentes entre el programador y la inteligencia artificial autónoma dentro del contexto de una sociedad de la información, comunicación y tecnología. Es decir, bajo este análisis comparativo

podrá llevarnos a establecer comparaciones multidisciplinarias e interdisciplinarias entre el derecho y la tecnología.

2.3 Bases teóricas

2.3.1 Teoría de la imputación objetiva

La teoría de la imputación es la más aceptable en el ámbito del derecho penal. Tal como lo hace notar Allué (2017) es necesario excluir la imprevisibilidad del azar, corregir la causalidad verificando el riesgo no permitido que con la imputación subjetiva deben evaluar la voluntariedad y la lesión o puesta en peligro de bien jurídico. De acuerdo con Gimbernat (2020) la causalidad es elemento necesario para la evaluación de imputación objetiva en consideración a la puesta en riesgo o peligro. En definitiva, constituye la superación de la causalidad aplicada mecánicamente para otorgar el análisis de la creación de riesgo para deslindar la imputación de responsabilidad penal sobre la acción y el resultado.

La imputación objetiva se desarrolla por varías teorías, entre las que destacan las propuestas por Roxin y Jakobs.

Roxin, en su abordaje de la imputación objetiva, enfatiza la importancia de distinguir entre la relación causal y la atribución de responsabilidad penal. Postula que no toda acción causalmente relacionada con un resultado debe ser imputada al autor desde el prisma penal. La centralidad de su teoría radica en la creación de un riesgo jurídicamente relevante y la realización de este riesgo en el resultado concreto. Roxin insta a considerar las normas y roles sociales, lo que enriquece la comprensión de la imputabilidad en un contexto social dinámico.

Contrariamente, Jakobs propone una visión normativa del Derecho Penal, argumentando que este sirve para estabilizar las expectativas normativas en la

sociedad. Su enfoque se aleja del análisis individualizado de Roxin, para posicionar al Derecho Penal como un mecanismo de comunicación que perpetúa el orden social. La teoría de Jakobs, por lo tanto, se centra más en la función social del Derecho Penal que en la evaluación de la acción y el resultado en sí.

Ambas teorías, aunque divergentes, contribuyen significativamente a la riqueza conceptual del Derecho Penal. Mientras Roxin proporciona un marco analítico robusto para evaluar la imputabilidad en casos concretos, Jakobs eleva la discusión a un plano normativo-social, explorando la función del Derecho Penal en la preservación del orden social. Estas perspectivas, aunque pueden parecer en contraposición, en realidad pueden ser vistas como complementarias, ofreciendo una visión holística de la imputación objetiva.

2.3.1.1 Imputación objetiva de la conducta

2.3.1.1.1 Riego permitido

La imputación objetiva de la conducta se necesita delimitar la conducta, mediante la configuración del riesgo permitido. De acuerdo con Paz-López (2018) la sociedad es denominada de riesgo, bajo los esquemas tecnológicos, económicos, sociales modernos que de cierta manera soportan diversas modalidades de riesgos que permiten estos riesgos para llevar adelante una vida en la sociedad. Según Coca (2019) existen negocios de alto riesgo que son roles de los administradores societarios que deben ser analizados las disposiciones internas como por los operadores de justicia. Como hace notar Vallejo-Jiménez (2017) que en el caso de la profesión médica también con el riesgo permitido se enfoca en las prácticas y actividades médicas estandarizadas que no afecten al paciente en situaciones concretas. Desde el punto de vista de Villavicencio (2007) que el riesgo debe ser

típico, relevante, no permitido (permitido es socialmente aceptado), no todo riesgo es relevante penalmente, pues pueden ser tolerables, se encuentra regulado (lex artis) y genera exoneración de responsabilidad penal.

En consecuencia, tan arraigado los riesgos en la sociedad, que podemos evidenciar su manejo a nivel empresarial, en donde no solo se habla de riesgos de las inversiones sino de su nivel y magnitud conforme a los intereses que se juegan.

2.3.1.1.2 Disminución del riesgo

Este elemento es necesario para establecer la disminución del riesgo que se ha creado. Como plantea Alcocer (2015) la regla de disminución en el riesgo es evaluando al creador de riesgo que busca modificar los eventos causales o la provocación de daños con la finalidad de conservar el bien jurídico, situación que genera exclusión de imputación objetiva. Como lo hace notar Villavicencio (2007) esta disminución genera exoneración de responsabilidad, por cuando el sujeto pasivo optimizando su acción, durante el curso causal, disminuye o evita el daño para la mejor protección del bien jurídico. En así, que dentro de la imputación objetiva se evalúan la creación del riesgo como autor y como contribuyó a disminuir dicho foco de peligro.

2.3.1.1.3 Riesgo insignificante

Este otro elemento de la imputación objetiva es el riesgo insignificante. A juicio de Alcocer (2015) el riesgo debe ser significativo o relevante, si no está no se consideraba dentro de la generación de riesgo para una imputación objetiva por la falta de lesividad trascendente del bien jurídico. Dicho en palabras de Villavicencio (2007) precisa que es insignificante socialmente porque falta relevancia con el bien jurídico o concretamente con el tipo penal, no procede exoneración penal, lo que

procede es que por motivo de falta de afectación del bien jurídico es falta relevancia penal. En consecuencia, para la imputación objetiva se tiene que evaluar que la creación de riesgo tiene que tener condición de relevancia que se considera en base a como resulta afectado el bien jurídico protegido.

2.3.1.1.4 Principio de confianza

Este es otra parte integrante de la imputación objetiva resulta ser el principio de confianza. Desde la perspectiva de Alcocer (2015) la sociedad se encuentra regulada por roles, funciones y trabajo entrelazados, cada uno debe controlar sus acciones, es por eso que el principio de confianza en la creencia social que otro actúa conforme a su función, rol o trabajo. Según Villavicencio (2007) que se trata que el sujeto actúa confiado en que otros actuarán dentro del riesgo permitido conforme a la división de trabajo dentro de la sociedad. Los componentes que fundamentan el principio de confianza, como hace notar Alcocer (2015) son la garantía del sentido de la norma, la debida ponderación de intereses en juego y preocupación de la propia conducta.

En consecuencia, la garantía del sentido de la norma es la orientación o guía que tienen los ciudadanos sobre sus funciones y roles en la sociedad para su actuación, así como considerar otro criterio para considerar el principio de confianza resulta ser la ponderación de los intereses que obedece a los roles y trabajo encomendado a los integrantes de la sociedad que son necesarios para el avance y desarrollo que son soportados y ponderados frente a la creación de algunos riesgos tolerables, así como la preocupación de la propia conducta frente a la conducta de los demás es importante para establecer el principio de confianza.

2.3.1.1.5 Prohibición de regreso

Esta categoría ayuda a establecer razonadamente la imputación objetiva. Desde el punto de vista de Alcocer (2015) es delimitar entre conductas insignificantes y posteriores conductas delictuales objetivamente reprochables, evitando responsabilidad sin deslinde adecuado de la conducta neutral previa, por ejemplo del profesional o técnico que entrega su trabajo o producto para luego un tercero aprovecharlo delictualmente. De acuerdo con Villavicencio (2007) el análisis de la conducta imprudente y la posterior conducta dolosa, es el análisis que se centra de la conducta neutral con la participación con la conducta posterior dolosa. Desde la posición de Gimbernat (2020) el análisis parte de tener una primera acción del autor para luego verificar la intervención de tercero en el resultado, no pudiendo asumir el resultado el autor. En consecuencia, la imputación objetiva ante la prohibición de regreso evalúa la neutralidad del actor frente a la actuación de otro que aprovecha de dicha neutralidad para encausar la creación del riesgo.

2.3.1.1.6 Ámbito de responsabilidad de la víctima.

Es relevante la delimitación de los ámbitos de actuación del agresor como de la víctima. En la opinión de Alcocer (2015) es necesario determinar las conductas típicas con la conducta de la víctima o de un tercero con relación al resultado, es decir también resulta coherente realizar la imputación a la víctima de su conducta desplegada. Con base en Villavicencio (2007) que se trata una forma de exclusión de responsabilidad penal por actuación de la víctima, por autopuesta en peligro o que es determinante la intervención del tercero para el resultado. Es así, que una interesante herramienta de la imputación objetiva resulta ser la delimitación de las

conductas de la víctima como del agresor para poder evaluar como se les atribuye la creación del riesgo.

2.3.1.2 Imputación objetiva de resultado.

La imputación objetiva de resultado es la superación de las otras teorías penales de imputación. Tal como lo hace notar Allué (2017) el análisis para la imputación del responsable, que es posible ante la superación de las teorías de la equivalencia de condiciones, causalidad adecuada y relevancia. Según Contreras (2019) el resultado es imputable al accionar del sujeto en la creación del riesgo desaprobado. En consecuencia, la imputación objetiva de resultado, se concentra en la actuación riesgosa del sujeto y como contribuyó al resultado.

2.3.1.2.1 Relación de riesgo.

En este apartado se valora la relación entre acción y resultado. Dicho con palabras de Allué (2017) trata de la acción riesgosa jurídicamente y desaprobada que se establece en el resultado. Desde el punto de vista de Villavicencio (2007) es la atribución objetiva entre la acción y el resultado que se mide con la magnitud del riesgo prohibido. En definitiva, la vinculación que se encuentra entre la acción y el resultado resulta indispensable para la imputación objetiva para poder atribuir responsabilidad.

2.3.1.2.2 Nexos causales desviados.

Los nexos causales desviados para deslindar la imputación. Como expresa Villavicencio (2007) se trata de verificar si la conducta riesgo creada se encuentra dentro de los márgenes de imputación entre la acción y los resultados obtenidos. Como plantea Kaufmann (2020) se debe evaluar que es decisiva la acción dolosa de creación del peligro para determinar los resultados atribuibles al sujeto. En

consecuencia, la evaluación de la vinculación de la acción riesgosa y el resultado debe tener en consideración que puede existir desviación del nexo causal antes de imputar penalmente.

2.3.1.2.3 Interrupción del nexo causal

La interrupción del nexo causal necesaria para deslindar la imputación. Empleando las palabras de Villavicencio (2007) constituye la alteración de la causalidad que modifica o anticipe el resultado como sería el caso de la intervención de un tercero. Según Panisello (2022) la interrupción del nexo causal es por intervención del tercero o de la víctima en la construcción del riesgo desaprobado. En definitiva, la adecuada imputación objetiva debe tener en cuentan la secuencia causal entre la acción y el resultado en la creación del resultado y que se encuentre libre de interrupción por tercera persona o por la propia víctima, para que sea atribuible al autor.

2.3.2 Autoría penal

La autoría penal representa un pilar fundamental en el edificio del derecho penal, dado que es a través de la determinación de la autoría que se asignan responsabilidades y se imponen las sanciones correspondientes a los perpetradores de actos delictivos. La evolución del pensamiento jurídico ha propiciado la emergencia de diversas teorías que buscan elucidar con precisión quién debe ser considerado autor de un delito y en qué medida. Esta reflexión se sumerge en el análisis de las teorías más prominentes que han tratado de desentrañar la autoría en el ámbito penal.

La Teoría clásica o formal, por ejemplo, emerge como una postura que sitúa como autor del delito a aquel que ejecuta de manera directa la acción típica y

antijurídica descrita por la ley penal. Esta perspectiva se aferra a una comprensión literal y directa de la autoría, centrando su análisis en la ejecución material del hecho delictivo. Sin embargo, esta teoría se muestra insuficiente al relegar a los demás participantes a una categoría inferior como cómplices o instigadores, sin reconocer que en ocasiones, la influencia de estos puede ser determinante en la consumación del delito.

En contraposición, la teoría del dominio del hecho, propone una visión más amplia y flexible de la autoría. Bajo esta lente, el autor es concebido como aquel que ostenta el control final sobre la realización del delito, siendo capaz de decidir sobre la ejecución del hecho y determinar su consumación o cesación. Esta teoría abre la puerta a una interpretación más inclusiva de la autoría, abarcando no solo a quien ejecuta el delito, sino también a quienes, desde una posición de poder o influencia, organizan, instigan o contribuyen de manera significativa al hecho delictivo.

Extendiendo la lógica del dominio sobre el hecho, la teoría del dominio de la organización, se aplica principalmente en escenarios donde existen estructuras organizativas que facilitan la perpetración de delitos. Aquí, el autor es concebido como aquel que, al controlar la organización, detenta el dominio sobre los actos delictivos que de ella se derivan. Esta teoría refleja una comprensión profunda de la autoría en contextos complejos y organizados, que a menudo escapan al análisis simplista de la teoría clásica.

en una línea similar, la teoría del dominio del hecho en virtud de aparatos organizados de poder se centra en estructuras organizativas complejas, designando como autor a quien, mediante una organización, tiene el dominio sobre la comisión

del delito. Esta perspectiva refleja una evolución en la comprensión de la autoría, adaptándose a las realidades de un mundo cada vez más interconectado y organizado.

Por otro lado, la teoría de la participación se enfoca en discernir entre autores y partícipes, estableciendo diferentes grados de responsabilidad penal. Los partícipes son aquellos que contribuyen al delito pero sin ejecutar la acción delictiva directamente. Esta teoría refleja una comprensión matizada de la autoría, reconociendo diversos grados de participación y responsabilidad en la comisión del delito.

la teoría del autor medio, en cambio, propone una comprensión de la autoría que incluye a aquel que realiza la acción delictiva por medio de otra persona que actúa como instrumento. Esta perspectiva amplía la noción de autoría, reconociendo la posibilidad de ejercer control sobre el delito a través de terceros.

Finalmente, la teoría de la culpabilidad se distancia de las anteriores al centrar su análisis en la culpabilidad del individuo respecto al delito cometido, independientemente de si realizó la acción delictiva directamente o a través de terceros. Esta teoría desplaza el foco desde la acción hacia la culpabilidad, ofreciendo una lente diferente para analizar la autoría.

Las teorías de la autoría penal ofrecen diversas perspectivas que reflejan la evolución del pensamiento jurídico en torno a la determinación de la responsabilidad en el ámbito penal. Desde la rigidez de la teoría clásica hasta la flexibilidad y profundidad de las teorías del dominio del hecho y de la organización, estas propuestas proporcionan herramientas analíticas esenciales para desentrañar la autoría en un mundo jurídico cada vez más complejo y dinámico. También, estas

teorías poseen una relevancia singular en el estudio de la interacción entre la inteligencia artificial y el derecho penal, especialmente en lo que respecta a la autoría y responsabilidad en casos de delitos cometidos con la asistencia o mediante el uso de tecnologías avanzadas.

2.3.2.1 Concepto

La autoría penal es un elemento principal del derecho penal para poder establecer la responsabilidad penal. Como lo hace notar Arenas (2017) en términos generales constituye autor aquel a quien le recae imputación subjetiva como objetiva. De acuerdo con Corcino (2017) menciona que la determinación de autor, parte de teoría unitaria por el aporte causalista del autor y la teoría diferenciadora extensivo como restrictivo entre autoría y participación.

Con relación a la autoría penal con la participación criminal. A criterio de Arenas (2017) la participación criminal de manera amplia es la intervención del autor, cómplice e instigadores, mientras en que el sentido restringido cuando es ajeno o accesorio a la acción criminal de otro (autor). Así mismo la concepción de autor tiene mucho que ver con la pluralidad de intervinientes en el hecho criminal, pues Corcino (2017) precisa que la concepción de autor como interviniente no genera problemas, sino que el problema es cuando existe varios participantes para administrar la reprochabilidad penal.

2.3.2.2 Tipos de autoría penal

2.3.2.2.1 Autoría directa

El concepto de autor directo. Como plantea Corcino (2017) no solamente lo constituye la ejecución de la acción típica, sino bajo la imputación objetiva se debe sopesar el injusto para determinar la autoría.

2.3.2.2.2 Autoría mediata.

En lo que se refiere a este tipo de autoría mediata. Desde la perspectiva de Pineda (2017) se trata del autor detrás de la ejecución que tiene decisión de corte autónomo frente al ejecutor material del hecho. Según Aboso (2017) la autoría mediata se basa en la instrumentalización de otra persona aprovechando el error o justificadamente por control directo o por organización. En consecuencia, se puede establecer a la autoría mediata como una manera de instrumentalizar la acción delictual por otro.

2.3.2.2.3 Coautoría.

La coautoría conceptualmente. Dicho en palabras de Arenas (2017) la intervención plural, común que realizan la acción típica. Como lo hace notar Corcino (2017) es la decisión y materialización conjunta ejecutiva de la acción contenida en el verbo rector del tipo penal. Es así, que la coautoría, es la ejecución conjunta bajo una decisión común para materializar el delito.

2.3.3 Inteligencia artificial

2.3.3.1 Concepto

La aproximación al concepto de inteligencia artificial. Teniendo en cuenta a Navas (2017) que refiere que es la emulación de la razón o conducta humana, también precisa que se trata de ciencia, ingeniería e informática dedicada a dicha emulación y hasta la confección de artefactos bajo dicha finalidad. Con base a Rouhiainen (2018) las máquinas puedan reproducir la inteligencia humana, solo en el análisis de la información, si no en la toma de decisiones, siendo inteligencia artificia la que tendría ventaja y eficiencia en estas labores. A juicio de Rusell & Norvig (2016) la inteligencia artificial se define entre la conducta (acción) y la

racionalidad asemejada con la naturaleza humana. Desde el punto de vista de Coloma et al. (2020) el agente inteligente debe causar cambios a su entorno y así como comunicarse con otros agentes inteligentes. De acuerdo con Morales (2021) en estos últimos años la inteligencia artificial débil o especifica ha dado mejoras como asistentes de voz que toman decisiones que pronostican superar la inteligencia y habilidades humanas. En definitiva, la tecnología que trae la inteligencia artificial superaciones a la inteligencia, conducta, pensamientos humanos para mejorar procesos y otorgar eficiencia.

La inteligencia artificial viene modificando la realidad. Desde la posición de Navas (2017) se trabaja en el ámbito de emulación de la inteligencia humana y el comportamiento inteligente y que se relaciona con la filosofía y demás ciencias en donde resalta la matemática y la estadística. Desde el punto de vista de García (2019) la inteligencia artificial es otorgar a las máquinas mediante la computación otorgar capacidad cognoscitiva humana. Como lo hace notar Barrios et al., (2020) la inteligencia artificial fuerte es analítica o cognitiva, humana con emociones y decisiones humanizadas con la adquisición de inteligencia social. En consecuencia, dotar a los algoritmos definiciones cercanas y superiores a la inteligencia artificial van a mejorar las condiciones actuales de la sociedad.

2.3.3.2 Enfoques

2.3.3.2.1 Comportamiento humano: Enfoque de la prueba de Turing.

La interpretación y evaluación de que se entiende por inteligencia de las máquinas o programas, paso por su primera etapa en los años 50, bajo la prueba de Turing en donde se diseñó una evaluación en donde un humano evalúe una máquina, siendo el humano el que desconoce que evalúa a una máquina. Desde la posición

de Rusell & Norvig (2016) nace como un test para delimitar a la inteligencia artificial, en donde se evalúa el nivel de procesamiento de lenguaje y conocimiento, así como el razonamiento y aprendizaje automático.

2.3.3.2.2 Pensar como humano: El enfoque del modelo cognitivo.

En este enfoque se trata de establecer como deberían pensar las máquinas. Rusell & Norvig (2016) en este enfoque trata de involucrarse en la mente, pensamiento y las experiencias psicológicas que también son parte del proceso del razonamiento humano y la interdisciplinariedad para el estudio de la inteligencia artificial.

2.3.3.2.3 El pensamiento racional: El enfoque de las leyes del pensamiento.

Este enfoque se centra en lo lógico. Como lo hace notar Rusell & Norvig, (2016) en este enfoque se tiene en cuenta la lógica y sus leyes para establecer el modelo de inteligencia artificial, presentando inconvenientes en la solución práctica de problemas con relación a las coordenadas lógicas preestablecidas.

2.3.3.2.4 Actuar en forma racional: El enfoque del agente racional.

Los avances actuales se centran en los paradigmas de racionalidad. Como plantea Leyva et al. (2018) la inteligencia artificial tiene como concepto aceptable a "agente racional" que va más allá de profundidad y complejidad de la inteligencia humana. Como afirma Rusell & Norvig (2016) la inteligencia artificial trata del agente que actúa de manera autónoma en un entorno, es adaptable, con la condición de tomar decisiones, por lo que las inferencias lógicas no necesariamente son eficientes o llevan a racionalidad. En esta línea de avance tecnológico, según Coloma et al. (2020) la investigación de la inteligencia se encamina en los agentes múltiples o bajo sistemas de comunicación, interacción y cooperación.

2.3.3.3 Aplicaciones de la inteligencia artificial

La aplicación de la inteligencia artificial en las labores de la sociedad moderna. Dicho en palabras de Rouhiainen (2018) el manejo de imágenes y objetos, es mejorado datos y algoritmos en el ámbito empresarial, también la predicción, manejo de redes sociales y defensa frente a amenazas cibernéticas.

2.3.3.3.1 Planificación autónoma

En las múltiples aplicaciones de la inteligencia artificial, también podemos encontrar su utilidad en el mundo empresarial. Teniendo en cuenta a García (2019) la gestión, organización y planificación que se lleva adelante previa programación en forma autónoma. A juicio de Coloma et al. (2020) esta planificación también puede apreciarse de la actuación del agente inteligente en una entorno como su interacción con otros agentes, situaciones que crean comunicación, organización y planificación.

2.3.3.3.2 Juegos

La inteligencia artificial aplicada a los juegos. Empleando las palabras de Amigone et al. (2018) se puede establecer que el agente puede llevar adelante jugadas automáticas demostrando espontaneidad y adaptabilidad para emerger nuevos escenarios. Desde el punto de vista de Bustamante et al. (2020) la inteligencia artificial mejora los procesos de resultados de los juegos lógicos, como el caso del sudoku que con la sola toma de una fotografía se puede otorgar el resultado o una aproximación. Como lo hace notar Borromeo et al. (2019) los juegos de estrategias con inteligencia artificial se enfocan en aprender de la información que va registrando el usuario mediante su interacción y aprende y se adapta otorgando experiencias desafiantes al usuario.

2.3.3.3.3 Control autónomo

La diferencia de otros programas o software, la inteligencia artificial se caracteriza por su autonomía. Como afirma Coloma et al. (2020) se caracteriza por su autonomía, recreatividad, proactividad, habilidad social, cooperación, razonamiento, adaptación e integridad. En relación con la autonomía de las máquinas frente a un operador, desde la posición de Leyva et al. (2018) el aprendizaje autónomo que se vienen enfrentando a problemas como los algoritmos, el razonamiento y red neuronal. Dicho en palabras de Coloma et al. (2020) el aprendizaje autónomo y adaptable es producto de la tecnología compleja y la provisión de inteligencia de resolución de problemas compleja.

2.3.3.3.4 Diagnosis

El procesamiento de datos mediante el análisis y síntesis para luego encontrar los motivos o causas de lo estudiado es un atributo de la inteligencia humana. Pero cuando la información son mega datos o datos complejos que si bien es cierto se pueden procesar, es así que recurrimos a los medios informáticos, resaltando la inteligencia artificial para dicho mega procesamiento en periodos cortos y de manera efectiva.

El diagnóstico médico mediante inteligencia artificial. Teniendo en cuenta a González et al. (2018) constituyen las mejores técnicas las redes neuronales artificiales (base de datos y proceso de respuesta complejo), razonamiento de casos (atendiendo a la variedad de casos y su registro) y las redes bayesianas (probabilidad).

2.3.3.3.5 Planificación logística

La complejidad de las labores de la industria y la empresa en sus procesos productivos también se han valido de la inteligencia artificial para mejorar la eficiencia y eficacia de sus procesos. Como lo hace notar Coloma et al. (2020) la inteligencia artificial domina los procesos industriales o de fabricación mediante una planificación, inclusive en las etapas críticas como complejas, hasta mediante la reconfiguración de los procesos, valiéndose de la información de la web.

2.3.3.3.6 Robótica

Uno de los avances en la tecnología son los autómatas o robots que pueden gobernarse. Dicho con palabras de Hernández (2019) el robot no es persona natural o jurídica, no es animal o cosa, pero contiene movimiento, autonomía e inteligencia. Empleando las palabras de Salazar (2018) desde las civilizaciones antiguas se procuró máquinas que imiten figuras y movimientos humanos mediante autonomía, siendo en la etapa industrial en donde se dio la complejidad y eficiencia para garantizar el trabajo. Desde el punto de vista de Rodas (2021) la inteligencia artificial combinada con la robótica puede generar apoyo a la industria, trabajo pesado como doméstico.

2.3.3.3.7 Procesamiento de lenguaje y resolución de problemas

La inteligencia artificial también es útil para favorecer el diálogo y comunicación. Citando a Leyva et al. (2018) encontramos a los Chat Bots y los denominados agente u operadores virtuales, que representan la interacción comunicativa con los usuarios para desarrollar tareas ordinaria y cotidianas. Desde el punto de vista de Coloma et al. (2020) el agente inteligente se enfoca en la resolución de la problemática, en especial en el ámbito de la industria, en donde se

refleja la competencia empresarial en la fabricación, producción y planificación altamente compleja.

2.3.3.4 Usos de la inteligencia artificial para la criminalidad

La inteligencia humana considerada compleja y múltiple tiende a la criminalidad, situación a la que no podría escapar la inteligencia artificial. Desde la posición de García (2019) la autonomía de la inteligencia artificial no es estricta, pues se programan para realizar y hasta superar las acciones racionales humanas, recayendo la responsabilidad en el diseñador y programado que le otorgan curso de acción.

2.3.3.4.1 Nivel Alto.

A. Suplantación de la identidad en audio y video.

Los derechos de la personalidad expresados en la imagen y la voz que dentro del ámbito virtual fácilmente pueden ser alterados por otros usuarios de la web, así como por la inteligencia artificial. Como lo hace notar Villota (2019) los avances de la inteligencia en el tratamiento de los datos, imagen, texto y video para fines delictivos puede modificar la identidad en línea y la percepción u opinión de los usuarios mediante bot. Como plantea Barrios et al. (2020) la intimidad y las emociones pueden ser amenazadas por la imitación de las personas en sus apariencias y voz mediante inteligencia artificial.

B. Vehículos sin conductor como armas.

La inteligencia artificial favorece la conducción de vehículos armados y no armados. Como afirma Villota (2019) la delincuencia se valdría de inteligencia artificial mediante armas de categoría letal con autonomía para asesinatos a

distancia de la escena del crimen, de la víctima o cualquier situación que pueda comprometer su identidad, generando zozobra postdelictual.

C. *Phishing*[1] personalizado.

Phishing personalizado es un ciberdelito facilitado por inteligencia artificial. Como plantea Avila & Torres (2021) la obtención de datos confidenciales tales como contraseñas, tarjetas bancarias, mediante el engaño y suplantación. Empleando las palabras de Villota (2019) phishing consiste en sustraer información contra cualquier víctima mediante engaño bajo fachadas de la red confiables mediante correo como chat o comunicaciones inmediatas, siendo el *spear phishing* en contra de una víctima puntual o determinada.

D. Interrumpir los sistemas controlados por inteligencia artificial

La actividad delictual utilizando inteligencia artificial también puede atentar contra la misma inteligencia artificial. Desde la posición de Barrios et al. (2020) es alterar los datos de entrenamiento de la inteligencia artificial para modificar los resultados del sistema. Como expresa Villota (2019) dentro de estos ataques están el envenenamiento de los datos de un servidor del Estado o entidad financiera para

[1] El "phishing" es una forma común de ciberdelito que involucra el engaño para obtener información confidencial de una persona. Los ciberdelincuentes que practican el phishing se hacen pasar por una entidad confiable para engañar a las personas y que estas proporcionen datos personales, como contraseñas, números de tarjetas de crédito, números de seguro social y otra información que pueda ser utilizada para el robo de identidad.

Este engaño suele realizarse a través de correo electrónico, donde el estafador envía un mensaje que parece provenir de una fuente legítima, como un banco o un sitio de redes sociales. El correo electrónico contiene un enlace que lleva a un sitio web falso que imita al sitio real, donde se le pide al usuario que introduzca su información personal. También existen otros tipos de phishing, como el "spear phishing" (dirigido a individuos o empresas específicas) y el "smishing" (donde se utilizan mensajes de texto en lugar de correos electrónicos).

La mejor defensa contra el phishing es la conciencia y la educación. Es importante ser escéptico respecto a los correos electrónicos que piden información personal, incluso si parecen provenir de una fuente confiable. También es útil mantener el software de seguridad actualizado y utilizar la autenticación de dos factores cuando sea posible.

manipular datos de usuarios o clientes, pudiendo traer problemas económicos como de reputación.

E.- Noticias falsas creadas por inteligencia artificial

La inteligencia artificial puede generar noticias que no coinciden con la realidad. De acuerdo con Barrios et al. (2020) los algoritmos de la inteligencia artificial predicen el comportamiento de los usuarios en las redes generando control y pérdida de libre albedrío mediante la configuración de lo político, lo psicológico y lo digital. Es así que se puede direccionar las opiniones y pareceres de los usuarios, pues como plantea Villota (2019) la inteligencia artificial recolecta y modifica texto, imágenes y audio generando engaños que generan *fake news*[2] que pueden influenciar sobre la comunicación y opinión de las personas. En consecuencia, las noticias falsas pueden afectar gravemente la credibilidad e identidad digital de los diversos usuarios de la web; sin embargo, su creación y proliferación que es conforme a las tendencias y gustos procesados por la inteligencia artificial.

[2] "Fake news" o noticias falsas, es una frase que se utiliza para describir una forma de desinformación o propaganda que se presenta como una noticia auténtica. A menudo, las noticias falsas se crean y difunden con la intención de engañar, para ganar beneficios económicos o influir en las opiniones o comportamientos políticos. Las noticias falsas pueden contener elementos que son totalmente falsos, o pueden distorsionar hechos reales mediante la omisión de detalles cruciales, la presentación de información fuera de contexto o la inclusión de opiniones como si fueran hechos.

Con la proliferación de las redes sociales y otros medios digitales, las noticias falsas pueden difundirse rápidamente y llegar a un público amplio. Esto ha llevado a una creciente preocupación sobre el impacto de las noticias falsas en la política, la salud pública y otros aspectos importantes de la sociedad. Para luchar contra las noticias falsas, es importante aprender a reconocerlas y verificar la información antes de compartirla. Algunas estrategias incluyen revisar las fuentes de información, verificar los hechos con múltiples fuentes y ser escéptico ante las noticias que parecen diseñadas para provocar una fuerte respuesta emocional.

2.3.3.4.2 Nivel Medio

A. Robots militares

La inteligencia artificial incrementa el movimiento sin control de los robots destinados para todo uso. Teniendo en cuenta a Villota (2019) la robótica ha incorporado lenguaje humano y así como complejos proceso de reconocimiento de las imágenes, de los textos y de la acústica, que se utilizan para el hogar, industria, la salud, entre otras actividades letales y deshumanizantes.

B. Aceite de serpiente

La inteligencia artificial también se encuentra encaminada a la predicción del comportamiento de las personas, pero estas labores que en muchas oportunidades no tienen explicación científica, se le denomina "aceite de serpiente". Como lo hace notar Romeo (2018) menciona que mediante el complejo manejo de algoritmos por la inteligencia artificial alimentada con los datos de actuaciones y personalidad de los criminales, se podrá pronosticar su futuro comportamiento como herramienta para decisiones judiciales en relación con la libertad.

C. Ciberataques basados en el aprendizaje.

Para establecer los alcances del ciberataque, debemos tener en cuenta diversas aristas informáticas para delimitar dicha acción criminal digital mediante inteligencia artificial. Según Avila & Torres (2021) el riesgo es el análisis de vulnerabilidad, amenaza es la determinación de potencialidad de daño o pérdida y la vulnerabilidad es la debilidad del sistema informático, siendo el ciberataque el daño, alteración o modificación del sistema digital. En consideración a que también la inteligencia artificial se puede utilizar para el ataque virtual. Desde la perspectiva de Villota (2019) si bien es cierto la inteligencia artificial se alimenta de datos para

desarrollar eficazmente sus labores, pero estos datos pueden ser envenenados (en el entrenamiento y aprendizaje) para que se cometan error en sus acciones y resultados. Como lo hace notar Avila & Torres (2021) el aprendizaje autónomo es una rama de la inteligencia artificial en donde mediante el análisis de los datos que se obtienen durante el entrenamiento va generando patrones y predicciones.

D. Drones de ataque autónomo

Los drones también facilitan su funcionamiento sin control por la inteligencia artificial. Como expresa Martín (2017) el uso de robots o máquinas autónomas o no tripuladas no es un tema nuevo, sino data de más de 20 años que se han encontrado a disposición de labores de seguridad, tácticas, armas y destrucción masiva. Citando a Villota (2019) los drones es un fenómeno del internet de las cosas que se viene incrementando en su producción y utilización. En relación con los actos delictivos cometidos por dron, desde la posición de Marín (2018) los drones han mejorado las tecnologías, comunicación y navegación han permitido el empleo en contrabando, drogas y terrorismo.

E. Engañar al reconocimiento facial.

El reconocimiento facial con inteligencia artificial es sencilla y manipulable para actividades ilícitas. A decir de Villota (2019) el ejemplo de drones o vehículo de vuelo no tripulados que aprovechando la tecnología facial puedan matar personas seleccionándolas entre la multitud.

F. Bombardeo de mercado

La facilidad como la inteligencia artificial puede recoger y gestionar la información de los gustos, preferencias y en general de nuestras tendencias y comunicaciones públicas puede generar una serie de problemas y manipulaciones.

Según Villota (2019) el usuario se crea confianza y autoestima por los mensajes y anuncios generados y bombardeados por la inteligencia artificial, en donde como el síndrome de Estocolmo en la red las víctimas confían en su agresor virtual.

2.3.3.4.3 Nivel bajo

A. Explotación de sesgos

Los sesgos en los cuales recae la inteligencia artificial, tratan del procesamiento estadístico o pronóstico algoritmo sin valoración del contexto o entorno. Empleando las palabras de Faliero (2021) constituye el uso de los algoritmos que se involucran en la psicología de las personas y otorgan resultados con tendencia estadística alejados de contextos de sensibilidad humana, por lo que corresponde otorgarle límites como la ética, la privacidad y seguridad.

B. *Bots*[3] antirrobo

Los *bots* se pueden potenciar para inteligencia artificial. Según Villota, (2019) son programas autónomos que realizan tareas determinadas, capaces de generar citas, correos, llamadas y chats extensos y naturales con cualquier persona.

C. Evadir la detección de inteligencia artificial.

[3] Los bots, abreviatura de robots, son programas de software diseñados para realizar tareas automatizadas. Estas tareas pueden ser simples y monótonas, como indexar contenido web para los motores de búsqueda, o complejas, como analizar datos a gran escala para obtener información útil.

Existen diferentes tipos de bots con diferentes funciones: Chatbots: Estos bots interactúan con los usuarios a través de interfaces de chat. Pueden proporcionar asistencia al cliente, responder a preguntas frecuentes, hacer recomendaciones y mucho más. Web Crawlers: Estos bots, utilizados por los motores de búsqueda, exploran Internet para indexar y clasificar contenido web. Social Media Bots: Pueden publicar automáticamente contenido, interactuar con usuarios, o incluso influir en el discurso en las redes sociales. Algunos bots de redes sociales son benignos, pero otros pueden ser utilizados para la desinformación o el spam. Trading Bots: Utilizados en el mundo financiero, estos bots pueden realizar transacciones basadas en algoritmos y patrones de mercado. Game Bots: Estos bots pueden jugar juegos, a menudo a velocidades y niveles de habilidad que los humanos no pueden igualar. Pueden ser usados para pruebas o para hacer trampa.

Los bots pueden ser muy útiles, pero también pueden ser mal utilizados para actividades perjudiciales, como el spam, la difusión de noticias falsas, y los ataques de denegación de servicio. Como tal, es importante utilizar y interactuar con los bots de manera responsable y ética.

La misma inteligencia artificial también puede servir para contrarrestar la vigilancia o detección de otras herramientas de inteligencia artificial. Desde la posición de Rondo (2020) se ha mejorado la detección en el análisis de los videos con el aprendizaje automático de la inteligencia digital, mejorando los procesos de atención humana, pero que necesitan del juicio humano y seguridad de los datos. En consecuencia, la inteligencia artificial aplicada a la seguridad e identificación de imágenes y patrones en los videos, pueden servir para poder identificar semejanzas e igualdades o encontrar patrones en dichos datos multimedia, análisis que sin duda son mejores a la labor humana; sin embargo, al confundirse o alterarse los datos con que son entrenados con la realidad, estos pueden generar problemas con el análisis y resultados de la detección.

D. Reseñas falsas creadas por inteligencia artificial

La inteligencia artificial es capaz de reseñas, opiniones, opinar en las redes sociales, así como otorgar valoraciones para crear tendencias de gustos y compras para servicios o productos en línea. Teniendo en cuenta a Barrios et al. (2020) la falsedad se puede ser desde los perfiles hasta las publicaciones en la red, como la construcción de personalidades y escenarios falsos.

E. Asecho asistido por inteligencia artificial

El asecho de las personas se materializa mediante los seguimientos de personas en sus ámbitos públicos y privados. Como plantea Barrios et al. (2020) se ha facilitado la invasión de la privacidad y el acopio de datos mediante el control de la vida personal y sus alrededores, ello bajo los alcances de la seguridad implementada por el gobierno y empresas privadas.

F. Falsificación

La inteligencia artificial bajo su condición de autónomo en su acción y aprendizaje, tiene la potencialidad de creación. Como afirma Villota (2019) la creación de perfiles sociales con fotografías falsas para el engaño de solteros, o mediante comunicaciones para facilitar el acceso a información privada, falsificaciones que serán profundas y aproximadas a la realidad por el uso de inteligencia artificial.

2.4 Definición de términos

Astroturfing: Es una estrategia de relaciones públicas en la que se finge el apoyo popular a una persona, grupo, producto o idea. El nombre proviene de "AstroTurf", una marca de césped artificial, como una analogía a "grassroots" o movimientos populares auténticos.

Bots: Según Túñez-López et al. (2018) es la automatización de actividades como la redacción o la ubicación y distribución de información mediante este tipo de algoritmos de inteligencia artificial. Los bots, una abreviatura de "robots", son programas de software automatizados que realizan tareas en Internet. A menudo, estas tareas son repetitivas y se llevarían demasiado tiempo para que una persona las complete. Los bots son capaces de realizar estas tareas a una velocidad y eficiencia mucho mayores.

Deepfake: Deepfake es una técnica de inteligencia artificial que se utiliza para crear o alterar contenido audiovisual. El término "deepfake" es una combinación de "deep learning" (aprendizaje profundo) y "fake" (falso), y hace referencia a la manera en que estas técnicas usan redes neuronales profundas para producir representaciones que pueden ser muy difíciles de distinguir de la realidad.

Dron: El dron como mecanismo electrónico no tripulado. Dicho en las palabras de Martín (2017) es un sistema aéreo no tripulado, pero con control humano o con autonomía programada o la combinación de ambos.

Imputación objetiva: La imputación objetiva en el derecho penal es la que constituye en la actualidad la forma más racional de atribución de responsabilidad penal. Empleando las palabras de Cancio (2020) puede entenderse como política criminal para poder delimitar la nebulosa legislación con la vulneración del bien jurídico, así como para evitar la mera aplicación de la causalidad mediante el análisis del riesgo jurídicamente desaprobado.

Inteligencia artificial: La inteligencia artificial es el desarrollo más logrado de la informática. Según Barrios et al. (2020) el término es polisémica vinculada con big data, robots y algoritmos, es multidisciplinario, que permite la creación de programas y máquinas que tienen curso de acción y decisión autónomo en un entorno determinado.

Phishing: Villota (2019) menciona que phishing consiste en sustraer información contra cualquier víctima mediante engaño bajo fachadas de la red confiables mediante correo como chat o comunicaciones inmediatas, siendo el spear phishing en contra de una víctima puntual o determinada (p. 161).

Proxy: En términos de redes informáticas, un "proxy" es un servidor que actúa como un intermediario entre un usuario y otros servidores en la red. El usuario se conecta al proxy, y el proxy se conecta al servidor al que el usuario quiere acceder.

Robot: El robot como mecanismo complejo informático y físico para facilitar acciones y actividades. Como señala Martín (2017) la máquina que ejecuta

acciones mediante control humano o control de ordenador o la combinación de ambos.

Spoofing: El "spoofing" es una táctica que se utiliza en la ciberseguridad para disfrazar la comunicación proveniente de una fuente desconocida como si fuera de una fuente conocida y confiable. La idea es engañar al receptor haciéndole creer que la comunicación es legítima.

2.5 Hipótesis

2.5.1 Hipótesis general

Los alcances de la imputación objetiva de la autoría mediata de programador de inteligencia artificial con fines delictivos en el Perú, devienen en vacíos jurídicos para establecer la imputación objetiva del autor mediato programador y la inteligencia artificial como ejecutor material del hecho delictivo.

2.5.2 Hipótesis específicas

Las consecuencias jurídicas de los vacíos jurídicos en la imputación objetiva de la autoría mediata del programador de inteligencia artificial con fines delictivos en el Perú, es la falta imputación de acción y resultado la impunidad pese a la puesta en peligro o daños de bienes jurídicos.

Se superará los vacíos normativos en la imputación objetiva de la autoría mediata del programador de inteligencia artificial con fines delictivos en el Perú, mediante la adaptación de la imputación objetiva a los supuestos criminalidad mediante inteligencia artificial.

2.6 Categorías

2.6.1 Identificación de categorías.

Categoría 1: Imputación Objetiva

Categoría 2: Autoría Penal

Categoría 3: inteligencia artificial

2.6.2 Operacionalización de categorías

Categoría 1 – Imputación Objetiva			
Definición Conceptual	**Definición Operacional**	**Dimensiones**	**Indicadores**
Esta teoría se enfoca según Allué (2017) en excluir la imprevisibilidad del azar, corrige a la causalidad verificando el riesgo no permitido que con la imputación subjetiva deben evaluar la voluntariedad y la lesión o puesta en peligro de bien jurídico.	La imputación objetiva, desde la posición de Cancio (2020) puede entenderse como política criminal para poder delimitar la nebulosa legislación con la vulneración del bien jurídico, así como para evitar la mera aplicación de la causalidad mediante el análisis del riesgo jurídicamente desaprobado.	Tipos	• Imputación objetiva de la Conducta • Imputación objetiva del resultado
Categoría 2 – Autoría Penal			
Definición Conceptual	**Definición Operacional**	**Dimensiones**	**Indicadores**
La autoría penal es un elemento principal del derecho penal para poder establecer la responsabilidad penal. Teniendo en cuenta a Arenas (2017) en términos generales constituye autor aquel a quien le recae imputación subjetiva como objetiva. Para la delimitación del concepto de autor, Corcino (2017) menciona que la determinación de autor, parte de teoría unitaria por el aporte causalista del autor y la teoría diferenciadora extensivo como restrictivo entre autoría y participación.	Con relación a la autoría penal con la participación criminal, según Arenas (2017) la participación criminal de manera amplia es la intervención del autor, cómplice e instigadores, mientras en que el sentido restringido cuando es ajeno o accesorio a la acción criminal de otro (autor). Así mismo la concepción de autor tiene mucho que ver con la pluralidad de intervinientes en el hecho criminal, pues Corcino (2017) precisa que la concepción de autor como interviniente no genera problemas, sino que el problema es cuando existe varios participantes para administrar la reprochabilidad penal.	Tipos	• Autoría directa • Autoría mediata • Coautoría
Categoría 2 – inteligencia artificial			
Definición Conceptual	**Definición Operacional**	**Dimensiones**	**Indicadores**

Teniendo en cuenta a Navas (2017) que refiere que es la emulación de la razón o conducta humana, también precisa que se trata de ciencia, ingeniería e informática dedicada a dicha emulación y hasta la confección de artefactos bajo dicha finalidad.	Barrios et al. (2020) precisa que como versión débil es marco de administración de datos y desarrollo de algoritmos que llevan a resultados, como versión fuerte estudia la conciencia, autonomía y sensibilidad (pág. 85).	Enfoque	• Comportamiento humano: Enfoque de la prueba de Turing. • Pensar como humanos: El enfoque del modelo cognitivo. • El pensamiento racional: El enfoque de las leyes del pensamiento. • Actuar en forma racional: El enfoque del agente racional.
		Aplicaciones	• Planificación autónoma • Juegos • Control autónomo • Diagnosis • Planificación logística • Robótica Procesamiento de lenguaje y resolución de problemas.
		Criminalidad	• Nivel alto • Nivel medio • Nivel Bajo

Capítulo III

METODOLOGÍA

3.1. Tipo de investigación

Los tipos de investigación se centra en una investigación básica que bajo el ámbito jurídico se desarrolla como una investigación teoría dogmática. Como lo hace notar Sánchez (2011) esta investigación no se puede encontrar un diseño o hipótesis pero sí el esclarecimiento cuestionamiento a los conceptos predeterminados del derecho en determinados contextos. En este sentido se partió de la teoría de la imputación objetiva aplicable al fenómeno de la inteligencia artificial, en donde se trabajan con principios, reglas, sistemas y teorías que afronta la criminalidad mediante inteligencia artificial.

El estudio es explicativo. El abordaje de las investigaciones desde la perspectiva del nivel de profundidad se centra basándonos en estudios exploratorios, descriptivos, explicativos y correlacionales. Este estudio es de nivel explicativo, según Guevara et al. (2020) se centra en la inferencia de lo estudiado, el investigador no tiene control de las variables, solamente se limita a la recolección de los datos y como método resalta la observación y explicación del fenómeno.

3.1.1 Método de investigación.

3.1.1.1 Métodos de investigación científica.

A.- Métodos generales de investigación científica.

a. Método deductivo.

El método deductivo es indispensable para llevar adelante el estudio. Como lo hace notar Abreu (2015) el estudio de los casos particulares que derivan o parten de las proposiciones o leyes científicas generales previamente definidas.

b. Método inductivo.

De acuerdo con Abreu (2015) el estudio de las características comunes de la realidad para construir una propuesta o ley científica general. Dicho en palabras de Martinez (2007) la inducción puede ser completa, incompleta, coexistencia y causal.

c. Método analítico.

El método analítico es el más completo por que engloba diversas acciones en la investigación. Empleando las palabras de Lopera (2010) es el estudio que insiste en la descomposición de los elementos constitutivos. El proceso analítico se basa en las acciones de entender, en la crítica, en contrastar y en incorporar.

B.- Métodos específicos de investigación científica.

En estos métodos planteamos métodos que tienen que ver con la naturaleza de la investigación, es así, que serán métodos no experimentales, tales como:

a. Método de modelación teórico.

El estudio necesita siempre del cotejo teórico para determinar sus alcances y delimitaciones. Desde la perspectiva de Reyes & Bringas (2006) la modelación teórica es una construcción teórica del objeto estudiado (ideal o real), sobre sus

propiedades elementos, relaciones; se fundamenta en los principios de consistencia lógica, analogía, enfoque sistémico y simplicidad del diseño.

b. Método dialéctico.

La dialéctica siempre se hace necesario para entender el movimiento y cambio en el objeto de estudio. Con base en Reyes & Bringas (2006) el método dialéctico es el procesamiento de la realidad física y mental. Este método dialéctico paso del mundo idealista al materialista, siendo las categorías dialécticas tesis, antítesis, síntesis, polarización y coexistencia de opuestos.

c. Método hermenéutico.

El método hermenéutico necesario para descifrar el contenido y alcances de los contenidos. Como afirma Arráez et al. (2006) es el arte de la interpretación por la comprensión del texto. Los textos son semánticos, ideológicos, culturales, entre otros. En las ciencias naturales se interpreta desde el objeto, mientras en las ciencias sociales se interpreta desde el sujeto.

d. Método exegético

El método exegético en la investigación jurídica es un enfoque tradicional centrado en la interpretación textual de las fuentes del derecho, tales como leyes, normas y otros documentos legales. Este método prioriza la literalidad del texto normativo, buscando entender las palabras y frases en su significado más directo y explícito. Sin embargo, va más allá de una simple lectura literal al considerar también el contexto normativo en el que se inscribe la ley. Esto implica tener en cuenta no solo la ley misma, sino también su relación con otras leyes, precedentes y, en última instancia, con la Constitución del país en cuestión.

3.1.1.2 Métodos de investigación jurídica.

A.- Método Jurídico-dogmático

Bernasconi (2007) estudia el derecho positivo vigente, su sistematización, establece las construcciones conceptuales tales como principios, mediante la abstracción de las normas y la recopilación de teorías de las instituciones jurídicas.

B.- Método de argumentación jurídica

Linares (2001) precisa que la teoría de la argumentación jurídica estándar se centra en la racionalidad, en los contextos de descubrimiento y justificación, las justificaciones interna y externa, así como la corrección de la decisión. Meza, (2006) precisa que argumentar en primer nivel el establecimiento a nivel legislativo, en segundo en la aplicación de las normas en especial en casos difíciles, en el tercer nivel en la sistematización racional de la dogmática jurídica.

3.2 Diseño de investigación

Este estudio es no experimental y transversal. Como plantea Hernández et al. (2003) desde el punto de vista de la ciencia, el diseño general es un diseño "no experimental", así como también precisa que, dentro del diseño no experimental, encontramos al estudio transeccional o transversal por cuanto el estudio comprende su accionar en periodo preestablecido.

3.3 Población y muestra

3.3.1. Universo, población y muestra

El establecimiento de universo, población y muestras se concentra en el número de personas representativas. En la investigación realizada no se puede determinar dicha secuencia en consideración a que se trata de objetos de estudio tales como la teoría de materia penal tales como la imputación objetiva y la autoría

y en otro extremo se encuentra la inteligencia artificial. Es así, que no se podrá establecer o determinar muestras para estudio.

3.3.1 Plan de recolección de la información y/o diseño estadístico.

Para la recolección de la información para la investigación se emplearon las siguientes estrategias:

- Búsqueda sistemática en bases de datos académicas, utilizando palabras clave relacionadas con el problema de investigación.

- Análisis de las listas de referencias de estudios relevantes para identificar más fuentes.

- Rastreo de citas a través de Google Scholar para encontrar trabajos derivados.

- Consulta a expertos en el tema de investigación para identificar literatura gris relevante.

- Monitoreo de revistas especializadas en el campo de estudio para detectar los últimos avances.

Criterios de inclusión:

- Literatura directamente enfocada en aspectos centrales de la investigación

- Teorías, conceptos y modelos ampliamente discutidos y citados sobre el tema.

- Trabajos considerados fundamentales o clásicos en el campo de estudio.

- Fuentes actualizadas.

3.4. Técnicas e instrumentos de recolección de la información

En términos generales los documentos son una fuente relevante de información para la realización de la tesis. Es más Hernández & Mendoza (2018)

resalta permite estudiar el lenguaje escrito y gráfico, no es invasivo y puede ser consultado en cualquier momento. En forma más específica respecto a las fuentes documentales de naturaleza jurídica Botero (2003) la técnica documental jurídica se fundamenta en las fuentes bibliográficas y la recopilación de los documentos legales, no se centra en el texto sino en el archivo que configura los rastros históricos jurídicos del derecho práctico.

La indagación y recolección de datos son esenciales en cualquier proceso investigativo, ya que proporcionan el sustento empírico para la construcción de argumentos y análisis. En el campo del derecho, la educación y en diversas disciplinas, la técnica documental y el análisis de contenido se presentan como instrumentos valiosos para la recolección y análisis de información. Este ensayo explora estas dos técnicas, sus aplicaciones y relevancia en la investigación.

La técnica documental, también conocida como fichaje, es un método sistemático empleado para el registro y recolección de información a partir de diversas fuentes, ya sean bibliográficas, hemerográficas o virtuales. Robles (2014) destaca el uso de fichas textuales, de resumen y de comentario como instrumentos clave en esta técnica. Las fichas textuales permiten registrar información específica tal como se presenta en la fuente original, facilitando la retención y referencia de datos exactos. Por otro lado, las fichas de resumen proporcionan una destilación de la información, ofreciendo una comprensión condensada de los contenidos, mientras que las fichas de comentario invitan a la reflexión y análisis crítico de la información recopilada. La técnica de fichaje no solo favorece la organización y sistematización de la información, sino que también promueve una interacción

reflexiva y crítica con los datos, lo cual es esencial para una comprensión profunda y la construcción de argumentos robustos.

Por otro lado, la técnica de análisis de contenido se enfoca en el examen sistemático y objetivo de documentos y textos, permitiendo la extracción de temas, patrones y tendencias dentro del material analizado. En el contexto jurídico, esta técnica es particularmente útil para el estudio de jurisprudencia, donde es crucial entender los criterios y fundamentos jurisprudenciales que subyacen a las decisiones legales. La ficha de análisis de contenido, como menciona Robles, se emplea para recoger los criterios y fundamentos jurisprudenciales, proporcionando un marco estructurado para desglosar y analizar la información contenida en los documentos legales. Esta técnica permite una exploración profunda de los textos, facilitando la identificación de argumentos, principios y razonamientos legales que son esenciales para la interpretación y comprensión de las decisiones judiciales.

Estas dos técnicas, aunque distintas en su enfoque, son complementarias en el proceso investigativo. Mientras la técnica documental proporciona una base sólida para la recolección y organización de información, el análisis de contenido ofrece una ruta metodológica para explorar y entender el contenido de los documentos. Ambas técnicas son indispensables en la investigación jurídica, permitiendo no solo la recolección de datos, sino también la construcción y fundamentación de argumentos legales. Además, facilitan la interacción crítica y analítica con las fuentes, promoviendo una comprensión más profunda y enriquecedora de los temas investigados.

En un mundo jurídico cada vez más complejo y dinámico, donde la interacción entre la ley, la sociedad y la tecnología plantea nuevos desafíos y

preguntas, la técnica documental y el análisis de contenido se presentan como herramientas esenciales para navegar en la maraña de información y jurisprudencia disponible. A través de estas técnicas, los investigadores, juristas y educadores pueden adentrarse en el análisis de las normas, decisiones y argumentos legales, construyendo una comprensión más profunda a la realidad jurídica.

3.5 Plan de procesamiento y análisis de datos

La metodología de investigación es un elemento crucial en cualquier proyecto investigativo, ya que proporciona el marco y las herramientas necesarias para la recolección, análisis e interpretación de datos. Hernández & Mendoza (2018) delinean un proceso general para la gestión y análisis de datos cualitativos que se detalla a continuación:

Recolección de datos:

El primer paso en cualquier investigación es la recolección de datos. En el contexto cualitativo, esto puede implicar entrevistas, grupos focales, observaciones o análisis documental. La calidad de los datos recopilados es fundamental, ya que estos constituyen la base sobre la cual se edificarán las interpretaciones y conclusiones.

Revisión de datos:

Una vez recopilados, es esencial revisar los datos para asegurar su relevancia, exactitud y completitud. Esta revisión permite identificar posibles lagunas o inconsistencias que podrían requerir una recolección adicional de datos.

Organización de datos:

Los datos cualitativos pueden ser vastos y variados, lo que hace crucial su organización para facilitar el análisis. Esto puede implicar la clasificación de los datos en categorías, temas o grupos relevantes.

Preparación de datos:

La preparación de los datos incluye todas las acciones necesarias para que los datos estén listos para el análisis. Esto puede incluir la transcripción de entrevistas, la digitalización de notas de campo, o la creación de una base de datos cualitativos.

Definición de unidad de análisis:

La unidad de análisis es el "quién" o "qué" que está siendo estudiado. Definir la unidad de análisis es crucial para establecer el enfoque y el alcance del análisis.

Codificación:

La codificación es un proceso central en el análisis cualitativo. Implica asignar etiquetas o códigos a segmentos de datos para identificar temas, conceptos o categorías. La codificación facilita el análisis posterior y la comparación de datos.

Generación de hipótesis:

A partir de la codificación y el análisis inicial, se pueden generar hipótesis. Estas hipótesis representan interpretaciones tentativas o proposiciones que serán evaluadas a través del análisis.

Evaluación:

Finalmente, la evaluación implica la verificación y validación de las hipótesis generadas. Esto puede incluir la revisión por pares, la triangulación de datos o la validación con participantes.

Este proceso descrito por Hernández & Mendoza (2018) proporciona una estructura ordenada y sistemática para la gestión y análisis de datos cualitativos. Cada etapa del proceso es crucial y contribuye al desarrollo de una investigación rigurosa y bien fundamentada. Además, este proceso puede ser iterativo, permitiendo a los investigadores revisitar y ajustar etapas anteriores en función de los hallazgos emergentes. En un ámbito como el jurídico, donde la interpretación y el análisis minucioso son esenciales, adoptar un enfoque metodológico robusto como el propuesto por Hernández & Mendoza puede contribuir significativamente a la calidad y rigor de la investigación.

Capitulo IV

RESULTADOS Y DISCUSIÓN

4.1 Presentación de Resultados

4.1.1 Resultados de orden doctrinal

4.1.1.1 La inteligencia artificial en la filosofía

Las bases filosóficas de la investigación científica se centran en los paradigmas para orientar, programar y ejecutar el estudio. Es importante partir de los paradigmas ideológicos, como el idealista, materialista o socio-crítico, en una adecuada metodología de investigación (Hashimoto, 2010). El idealismo se enfoca en la interpretación subjetiva, mientras que el materialismo considera que la realidad se construye independientemente del sujeto (Escuela, 2019; Gonzales, 2018). El paradigma socio-crítico busca la transformación mediante el pensamiento crítico y la reflexión de la ideología y el sistema social (Rodríguez, 2022). Para el estudio de la teoría de la imputación objetiva y la inteligencia artificial, se requiere una perspectiva sociocrítica que aborde los cambios en la sociedad (Loza et al., 2020; Bibiana et al., 2023).

La inteligencia artificial y sus transformaciones en la sociedad son comprendidas a través del paradigma socio-crítico (Loza et al., 2020). Este paradigma busca superar el conservadurismo idealista y el reduccionismo del positivismo, ofreciendo una visión teórica y práctica de las ciencias sociales (Bibiana et al., 2023). Además, el paradigma socio-crítico aborda la complejidad encontrada en la realidad y se relaciona con la sociedad del conocimiento e información generada por la tecnología de la inteligencia artificial (Bibiana et al., 2023). Asimismo, la imputación objetiva como teoría penal busca superar la visión

causalista y establecer la responsabilidad penal en una sociedad moderna (Barrios et al., 2020). La inteligencia artificial, dentro del marco filosófico, plantea debates sobre su impacto en la sociedad y la comprensión humana (Barrios et al., 2020; Rodríguez, 2022). Es así, que el análisis socio-crítico es fundamental para comprender la influencia de la inteligencia artificial en la sociedad y el derecho. Estas tecnologías están transformando los fundamentos de la sociedad y la percepción del ser humano en comunidad (Bibiana et al., 2023; Barrios et al., 2020).

La inteligencia artificial ha transformado radicalmente diversos aspectos de nuestra sociedad. Desde una perspectiva sociocrítica, es crucial analizar sus implicaciones y desafíos. La sociocrítica aboga por una visión crítica y reflexiva de las ciencias sociales, superando enfoques idealistas y reduccionistas. Según esta perspectiva, la inteligencia artificial reconfigura la sociedad, la cultura y nuestra comprensión del ser humano. Surge así la necesidad de reflexionar sobre estos nuevos escenarios, pues erosionan los cimientos de nuestra sociedad. Asimismo, es fundamental considerar la imputación objetiva como teoría penal, que busca asignar responsabilidad penal en una sociedad justa y racional, superando la visión causalista. La inteligencia artificial plantea interrogantes sobre la humanización y el desarrollo posthumano. Por tanto, desde el paradigma sociocrítico, se debe analizar la interacción entre la inteligencia artificial y nuestra sociedad, teniendo en cuenta los aspectos éticos, legales y sociales involucrados. Es necesario abordar estos desafíos desde una perspectiva crítica y transformadora, promoviendo una convivencia armoniosa entre la inteligencia artificial y los valores humanos fundamentales.

La investigación se basa en posturas positivistas que buscan enfocarse normativo estático y prescriptivo del derecho, en aras de construir un sistema jurídico más justo y acorde a la sociedad moderna. Este estudio adopta una postura filosófica crítica positivista, diferenciándose así del constitucionalismo y del positivismo normativista (Marquisio, 2015). Por otro lado, la neurociencia aplicada a la computación tiene como objetivo replicar los procesos cerebrales humanos, planteando una visión automatizada del ser humano (Garrido, 2022). En consecuencia, el enfoque post-positivista crítico, que reconoce las indeterminaciones del lenguaje jurídico y cuestiona las tendencias positivistas, permite abordar la teoría de la imputación objetiva en el derecho penal frente al impacto de la inteligencia artificial en la comisión de delitos.

La investigación en el ámbito jurídico se ha alejado de tratamientos normativos estáticos y discursos meramente descriptivos, buscando construir un derecho más justo y acorde a la sociedad moderna. En este estudio, nos basamos en la postura filosófica postpositivista crítica, que se diferencia de los enfoques postpositivistas constitucionalistas y normativistas. Según Marquisio (2015), esta postura se caracteriza por cuestionar constantemente la ideología, prescripción y descripción del discurso jurídico. Además, la aplicación de la neurociencia a la computación, según Garrido (2022), se centra en replicar los procesos cerebrales humanos con una visión automatizada del ser humano. En este sentido, el postpositivismo adaptado para este estudio es el enfoque crítico, que se aparta de las tendencias positivistas jurídicas que consideraban al sistema jurídico como único y perfecto, y al discurso jurídico como definitivo, sin aceptar las indeterminaciones del lenguaje jurídico. Bajo estos fundamentos, se plantea el

cuestionamiento y la adaptación de la teoría de la imputación objetiva del derecho penal frente al fenómeno de la inteligencia artificial con fines delictivos. Es necesario analizar cómo esta nueva tecnología desafía las concepciones tradicionales del derecho y cómo se pueden imputar consecuencias jurídicas a las diversas interacciones sociales que involucran inteligencia artificial.

4.1.1.2 La inteligencia artificial en la epistemología

La epistemología abarca diversas tendencias en el estudio de la ciencia, la filosofía y la metodología de la investigación científica. En este estudio, partimos de la postura mayoritaria latinoamericana, considerándola como teoría de la ciencia (Padrón, 2007). En nuestro contexto, se refiere al conocimiento científico excluyendo otros tipos de conocimiento, y se denomina como "filosofía de la ciencia", "teoría de la ciencia" o "teoría de la investigación científica" (Padrón, 2007). Según Gadea et al. (2019), la epistemología se encarga de cuestionar y derribar modelos teóricos, lógicos e informacionales, aspirando a abarcar el conocimiento complejo. Es así, que resulta esencial la epistemología para tratar la influencia de la inteligencia artificial en el derecho.

La epistemología abarca diferentes enfoques al estudiar la ciencia, la filosofía y la metodología de la investigación científica. En este estudio, nos centraremos en la corriente mayoritaria latinoamericana de teoría de la ciencia. La epistemología se refiere al conocimiento científico y se conoce con diferentes nombres en distintos contextos, como "filosofía de la ciencia" o "teoría de la investigación científica". La epistemología tiene como objetivo cuestionar y desafiar modelos teóricos, lógicos e informacionales, aspirando a abarcar el conocimiento en su complejidad. En el ámbito del derecho, la epistemología plantea

interrogantes sobre los componentes y elementos del derecho como ciencia social. Del mismo modo, en relación con la tecnología, se analizan los acercamientos y las interrelaciones con las ciencias sociales, naturales o exactas.

En síntesis, la inteligencia artificial en la epistemología se enfrenta a interrogantes y análisis en su integración y relación con distintos campos del conocimiento. La epistemología general proporciona herramientas críticas para comprender y examinar el derecho y la tecnología, así como su interacción con otras disciplinas. Esto fomenta una perspectiva amplia y compleja que aborda los desafíos y oportunidades surgidos en este campo en constante evolución.

Las bases epistemológicas del derecho plantean el problema de su cientificidad y su relación con otras disciplinas. Según Salamanca (2015) el conocimiento jurídico puede ser considerado tanto escéptico como científico. Partimos de la premisa de que el derecho es una ciencia social que regula la conducta para garantizar la convivencia. La epistemología del derecho se enfoca en la construcción de modelos epistémicos para establecer la verdad en el debate jurídico (Cáceres, 2023). Lo multidisciplinario implica la participación de diversas disciplinas, lo interdisciplinario integra teoría, objeto y método, mientras que lo transdisciplinario otorga una perspectiva completa (Paoli, 2019). En este estudio, analizaremos el derecho penal, la teoría de la imputación objetiva y su relación con la inteligencia artificial autónoma en una sociedad tecnológica. Esto nos permitirá realizar comparaciones multidisciplinarias e interdisciplinarias entre el derecho y la tecnología.

La epistemología del derecho se enfrenta al desafío de establecer su naturaleza científica como elemento esencial para la realización de estudios e

investigaciones en este campo. Desde una perspectiva epistemológica, el conocimiento jurídico puede ser considerado tanto escéptico como científico. En este sentido, el derecho se posiciona como una ciencia social que busca regular la conducta humana en función de valores y finalidades orientadas hacia la convivencia social.

La epistemología del derecho se centra en la construcción de modelos epistémicos que permitan al profesional del derecho determinar la veracidad de las premisas relevantes que surgen en el ámbito jurídico. Este enfoque implica considerar la multidisciplinariedad, es decir, la participación de diversas disciplinas sin perder de vista el objeto y el método propios del derecho. Asimismo, se plantea la interdisciplinariedad, que implica la integración teórica, así como del objeto y el método, para brindar una perspectiva de estudio enriquecedora que trascienda los límites disciplinarios. En este sentido, se busca establecer conexiones entre el derecho y otras ciencias.

El lenguaje jurídico se caracteriza por su indeterminación, lo que plantea la necesidad de abordar el derecho desde enfoques multidisciplinarios e interdisciplinarios. Además, se hace relevante considerar la comunicación interna y externa del derecho con otras disciplinas, reconociendo su autonomía y su capacidad de relacionarse con diferentes ámbitos de conocimiento.

En este estudio, nos centraremos en el ámbito del derecho penal, específicamente en la teoría de la imputación objetiva, en relación con la inteligencia artificial autónoma y su interacción con los programadores. A través de este análisis comparativo, podremos explorar las implicaciones multidisciplinarias e interdisciplinarias que surgen de la intersección entre el derecho y la tecnología.

En definitiva, la inteligencia artificial en la epistemología del derecho plantea interrogantes sobre su carácter científico y su relación con otras disciplinas. La adopción de enfoques multidisciplinarios e interdisciplinarios en el estudio del derecho nos permitirá comprender mejor las implicaciones y las conexiones que se generan en el contexto de una sociedad en constante evolución.

4.1.1.3 La inteligencia artificial, autoría penal e imputación objetiva

La inteligencia artificial cerca de la inteligencia humana. Desde la posición de Hernández (2019) se parte de criterios biológicos de la inteligencia humana para estudiarse científicamente y con ayuda de la informática va más allá, en donde reconocimiento patrones simples y repetitivos hasta llegar a la conciencia de las maquinas. Teniendo en cuenta a Morales (2021) la inteligencia artificial se menciona los tipos de inteligencia artificial partiendo de la conducta, pensamiento y actuación racional, así como los generales (inteligencia humana completa) y específicos (actividad de inteligencia determinada).

En la dogmática penal para definir a la autoría penal tenemos al autor directo (Corcino, 2017), autor mediato e instrumental (Aboso, 2017) y coautoría (Arenas, 2017). En este sentido tendremos que aplicar dichos aspectos dogmáticos al fenómeno de la inteligencia artificial que puede contar con los siguientes sujetos: (i) programador o programadores o empresas desarrolladoras, (ii) usuario de la inteligencia artificial y (iii) la misma inteligencia artificial que puede adquirir autonomía e independencia como agente racional que decida (Leyva et al., 2018), siendo discutible a favor o en contra que pueda imputársele personería jurídica al igual que se ha generado mediante ficción a la persona jurídica.

4.1.1.4 Supuestos de criminalidad con inteligencia artificial

4.1.1.4.1 Nivel alto

4.1.1.4.1.1 Suplantación de la identidad en audio y video

Manipulación de videoconferencias: Un atacante utiliza inteligencia artificial para generar imágenes y voces falsas de un ejecutivo o líder de una empresa, infiltrándose en una reunión virtual y obteniendo acceso a información confidencial o influyendo en decisiones importantes.

Sextorsión: Un ciberdelincuente crea contenido multimedia falso, como videos o imágenes comprometedoras, utilizando la tecnología de *deepfake*[4] para simular a una persona real y chantajear a la víctima con la intención de obtener dinero o favores.

Desinformación en campañas políticas: La suplantación de la identidad de un político o líder de opinión a través de *deepfakes* puede utilizarse para difundir noticias falsas y afectar la percepción del público sobre el individuo, alterando el resultado de elecciones o generando conflictos sociales.

Fraude financiero: Un atacante emplea inteligencia artificial para imitar la voz de un empleado o cliente de una entidad financiera, solicitando transferencias

[4] "Deepfake" es una tecnología basada en la inteligencia artificial que se utiliza para crear o alterar contenido de vídeo o audio, haciendo que parezca real. Se trata esencialmente de una forma avanzada de manipulación digital. El término "deepfake" es una combinación de "deep learning" ("aprendizaje profundo") y "fake" ("falso"). "Deep learning" es una subcategoría de la inteligencia artificial y se refiere al uso de redes neuronales artificiales con varias capas (o "profundas") que aprenden y toman decisiones de forma independiente, imitando el funcionamiento del cerebro humano. La tecnología deepfake utiliza estas redes neuronales para analizar fotografías y vídeos de la cara de una persona, aprender sus características y luego usar esa información para generar nuevas imágenes o vídeos que parezcan auténticos. Aunque puede tener usos legítimos, como en la producción de películas o videojuegos, la tecnología de deepfake ha generado preocupación debido a su potencial para crear contenido engañoso o difamatorio. Por ejemplo, puede usarse para poner rostros de personas reales en situaciones que nunca ocurrieron, o para crear falsos discursos o declaraciones.

de fondos o cambios en información bancaria, lo que puede resultar en pérdidas económicas significativas.

Suplantación de identidad en atención al cliente: Un delincuente utiliza inteligencia artificial para imitar la voz y el comportamiento de un representante de atención al cliente de una empresa, contactando a clientes y obteniendo información personal y financiera sensible, lo que puede derivar en sustracción de la identidad y fraude.

4.1.1.4.1.2 Vehículos sin conductor como armas

Ataques terroristas: Un grupo terrorista podría secuestrar un vehículo autónomo, cargándolo con explosivos y programándolo para dirigirse a una ubicación concurrida, causando un gran número de víctimas y daños materiales.

Secuestros: Un delincuente podría hackear un vehículo sin conductor para tomar el control del mismo y secuestrar a sus ocupantes, exigiendo un rescate a cambio de su liberación.

Robos y hurtos en movimiento: Al utilizar vehículos autónomos para bloquear el tráfico o acercarse a vehículos blindados de transporte de valores, los delincuentes podrían llevar a cabo robos en movimiento de manera más eficiente y coordinada.

Atropellamientos masivos: Un atacante podría manipular un vehículo autónomo para que acelere y atropelle a peatones en áreas concurridas, causando múltiples víctimas y sembrando el pánico en la población.

Sabotaje a infraestructuras críticas: Un vehículo sin conductor podría ser utilizado para transportar dispositivos destructivos, como explosivos o material radiactivo, y ser dirigido hacia instalaciones críticas como centrales eléctricas,

represas o puentes, causando daños significativos y afectando el funcionamiento de la sociedad.

4.1.1.4.1.3 Phishing personalizado

Suplantación de correo electrónico: Un atacante podría utilizar la inteligencia artificial para crear correos electrónicos altamente personalizados y convincentes que imiten a una persona o entidad conocida, engañando a las víctimas para que compartan información confidencial o realicen transacciones financieras.

Estafas en redes sociales: Un delincuente podría emplear inteligencia artificial para analizar perfiles de redes sociales y crear mensajes falsos adaptados a los intereses y conexiones de una víctima, persuadiéndola para que haga clic en enlaces maliciosos o proporcione información sensible.

Ataques de *spear phishing*: La inteligencia artificial podría utilizarse para identificar objetivos específicos dentro de una organización, como ejecutivos de alto nivel, y luego personalizar mensajes de phishing para dirigirse a estos individuos, aumentando la probabilidad de éxito en el robo de información o acceso a sistemas internos.

Mensajes de texto y aplicaciones de mensajería: Un ataque de *phishing* personalizado podría llevarse a cabo a través de mensajes de texto o aplicaciones de mensajería instantánea, utilizando la inteligencia artificial para imitar el estilo de comunicación y lenguaje de personas conocidas por la víctima, con el objetivo de obtener datos personales o financieros.

Chatbots[5] maliciosos: Un cibercriminal podría utilizar *chatbots* impulsados por IA para interactuar con usuarios desprevenidos, haciéndose pasar por una entidad legítima, como un banco o una compañía de seguros, para extraer información confidencial o inducir a las víctimas a realizar acciones perjudiciales para sus intereses.

4.1.1.4.1.4 Interrumpir los sistemas controlados por inteligencia artificial

Ataques adversarios de aprendizaje automático: Un atacante podría utilizar ejemplos adversarios para engañar a un sistema de inteligencia artificial, provocando que el sistema tome decisiones erróneas o cause daños. Por ejemplo, un atacante podría manipular señales de tráfico para confundir a vehículos autónomos y causar accidentes.

Manipulación de datos de entrenamiento: Un delincuente podría comprometer el proceso de aprendizaje de un sistema de inteligencia artificial al infiltrarse en los datos de entrenamiento y agregar información incorrecta o

[5] Un chatbot es un programa informático diseñado para simular una conversación con un humano. Estos programas utilizan el procesamiento del lenguaje natural y la inteligencia artificial para entender y responder a los textos escritos por los usuarios. Existen varios tipos de chatbots, desde los más simples que siguen scripts predefinidos hasta los más avanzados que utilizan el aprendizaje automático para adaptarse y aprender de las interacciones con los usuarios. Algunos ejemplos de uso de los chatbots incluyen: Servicio al cliente: Los chatbots son a menudo utilizados por las empresas para proporcionar soporte al cliente 24/7. Pueden responder a preguntas frecuentes, guiar a los usuarios a través de procesos complicados, o ayudar a los usuarios a realizar pedidos. Interacción en redes sociales: Algunas empresas utilizan chatbots en plataformas de redes sociales para interactuar con los clientes, responder a sus preguntas, o promover productos y servicios. Asistentes personales: Los chatbots también pueden actuar como asistentes personales, ayudando a los usuarios a gestionar su calendario, enviar recordatorios, o buscar información en línea. Salud y bienestar: Algunos chatbots están diseñados para ayudar a los usuarios a gestionar su salud y bienestar, ofreciendo consejos y recordatorios. Educación: Los chatbots pueden ser utilizados como herramientas de enseñanza, proporcionando tutoría personalizada o respondiendo a preguntas sobre temas específicos.

Aunque los chatbots son herramientas poderosas y útiles, también presentan desafíos, como entender el lenguaje y las intenciones de los usuarios de manera precisa, mantener la privacidad y seguridad de los datos de los usuarios, y manejar situaciones complejas o sensibles de manera adecuada.

maliciosa. Esto podría causar un funcionamiento defectuoso del sistema o comportamientos no deseados.

Ataques de negación de servicio: Un atacante podría apuntar a sistemas de inteligencia artificial con un volumen masivo de tráfico malicioso o solicitudes, sobrecargando los recursos y provocando interrupciones en los servicios proporcionados por la inteligencia artificial.

Ataques de envenenamiento de modelo: Un ciberdelincuente podría inyectar datos manipulados en un sistema de inteligencia artificial en tiempo real, causando que el sistema aprenda y adopte comportamientos maliciosos o perjudiciales, lo que podría llevar a la propagación de información falsa o afectar a sistemas críticos.

Explotación de vulnerabilidades de software: Un atacante podría buscar y explotar vulnerabilidades en el software de un sistema de inteligencia artificial, permitiéndole tomar el control del sistema, robar datos o interrumpir las operaciones. Esto podría tener consecuencias graves, especialmente si el sistema controla infraestructuras críticas o procesos industriales.

4.1.1.4.1.5 Noticias falsas creadas por inteligencia artificial

Desinformación política: Un atacante podría usar inteligencia artificial para crear noticias falsas y difundirlas en las redes sociales, tergiversando las acciones o declaraciones de políticos y líderes, lo que podría influir en la opinión pública y afectar el resultado de elecciones o referendos.

Manipulación del mercado financiero: Un ciberdelincuente podría utilizar IA para crear y difundir noticias falsas sobre empresas o eventos económicos, lo que podría causar fluctuaciones en los precios de las acciones y permitir que el atacante se beneficie de estas manipulaciones.

Difamación de individuos o empresas: Un atacante podría usar inteligencia artificial para crear noticias falsas que difamen a individuos, como celebridades, ejecutivos de empresas o figuras públicas, dañando su reputación y posiblemente causando pérdidas económicas o legales.

Desestabilización social: Un delincuente podría utilizar inteligencia artificial para fabricar noticias falsas que fomenten el miedo, la discordia o el pánico en la sociedad, lo que podría provocar disturbios civiles, violencia o incluso conflictos entre comunidades o naciones.

Desacreditar a la ciencia y la investigación: Un atacante podría emplear inteligencia artificial para generar noticias falsas que tergiversen o desacrediten hallazgos científicos o médicos, lo que podría socavar la confianza en la ciencia y la investigación, y tener consecuencias negativas para la salud pública y la adopción de políticas basadas en la evidencia.

4.1.1.4.2 Nivel medio

4.1.1.4.2.1 Robots militares

Ataques no autorizados: Un ciberdelincuente podría piratear robots militares, como drones o vehículos terrestres no tripulados, y usarlos para llevar a cabo ataques no autorizados en objetivos civiles o militares, provocando bajas y daños materiales.

Espionaje: Un adversario podría utilizar robots militares para infiltrarse en territorio enemigo y recopilar información clasificada o sensible, lo que podría comprometer la seguridad nacional o la estrategia militar.

Manipulación de misiones: Un atacante podría interceptar las comunicaciones entre robots militares y sus operadores, alterando órdenes o

misiones para lograr objetivos diferentes a los previstos, lo que podría tener consecuencias desastrosas en el campo de batalla.

Creación de incidentes internacionales: Un delincuente podría utilizar robots militares hackeados para provocar incidentes internacionales, como violaciones no autorizadas del espacio aéreo o marítimo, lo que podría generar tensiones diplomáticas o incluso conflictos armados.

Desarrollo y proliferación de armas autónomas: Un grupo criminal o terrorista podría adquirir robots militares y modificarlos para desarrollar armas autónomas letales, lo que podría aumentar el riesgo de ataques indiscriminados y la proliferación de estas armas en manos de actores no estatales.

4.1.1.4.2.2 Aceite de serpiente

Productos de inteligencia artificial falsos: Ciberdelincuentes podrían crear y vender productos o servicios de inteligencia artificial que prometen resultados espectaculares pero que en realidad no funcionan o son de baja calidad, engañando a consumidores y empresas.

Estafas de inversión en inteligencia artificial: Delincuentes podrían promover oportunidades de inversión en compañías de inteligencia artificial inexistentes o fraudulentas, aprovechándose del interés y la confianza en el potencial de la inteligencia artificial para estafar a inversionistas desprevenidos.

Publicidad engañosa: Los estafadores podrían utilizar técnicas de inteligencia artificial para generar publicidad engañosa y manipuladora, atrayendo a consumidores a comprar productos o servicios de baja calidad o falsificados.

Desinformación en salud: Ciberdelincuentes podrían utilizar la inteligencia artificial para difundir información errónea o engañosa sobre productos de salud o

tratamientos médicos, aprovechándose de la vulnerabilidad de las personas que buscan soluciones rápidas o milagrosas a sus problemas de salud.

Falsas promesas de empleo: Los estafadores podrían utilizar sistemas de inteligencia artificial para crear ofertas de empleo falsas o fraudulentas, engañando a personas en busca de trabajo y extrayendo información personal o financiera para fines ilícitos.

4.1.1.4.2.3 Ciberataques basados en el aprendizaje

Malware adaptativo: Los ciberdelincuentes pueden utilizar algoritmos de aprendizaje automático para desarrollar malware capaz de adaptarse y evolucionar automáticamente, lo que dificulta su detección y eliminación por parte de los sistemas de seguridad.

Ataques de envenenamiento de datos: Los delincuentes pueden corromper los conjuntos de datos utilizados para entrenar sistemas de inteligencia artificial, introduciendo información errónea o maliciosa, lo que afecta negativamente el rendimiento y la precisión de los sistemas de inteligencia artificial.

Generación automática de phishing: Los ciberdelincuentes pueden utilizar algoritmos de aprendizaje automático para crear y personalizar automáticamente correos electrónicos y sitios web de phishing, aumentando la efectividad de sus estafas y la probabilidad de que las víctimas caigan en ellas.

Ataques de adversario en redes neuronales: Los atacantes pueden utilizar técnicas de aprendizaje automático para identificar y explotar debilidades en los sistemas de inteligencia artificial, generando entradas especialmente diseñadas para engañar a los sistemas de reconocimiento de imágenes, texto o voz.

Optimización de ataques: Los ciberdelincuentes pueden utilizar algoritmos de aprendizaje automático para mejorar la eficacia y el alcance de los ataques de denegación de servicio distribuido, identificando patrones en el tráfico de red y ajustando sus tácticas en tiempo real para evadir los sistemas de defensa.

4.1.1.4.2.4 Drones de ataque autónomo

Ataques a infraestructuras críticas: Drones autónomos equipados con armas o explosivos podrían ser utilizados por actores malintencionados para atacar infraestructuras críticas como centrales eléctricas, redes de comunicación o instalaciones gubernamentales.

Asesinatos selectivos: Los drones de ataque autónomo podrían ser programados para identificar y eliminar objetivos específicos, como líderes políticos, militares o empresariales, basándose en características físicas o de comportamiento.

Espionaje y vigilancia: Los drones autónomos pueden ser utilizados para espiar y recopilar información sobre objetivos, tanto en entornos militares como civiles, sin ser detectados fácilmente debido a su tamaño reducido y capacidad de vuelo silencioso.

Contrabando y tráfico de drogas: Los drones autónomos pueden ser utilizados por organizaciones criminales para transportar drogas, armas y otros bienes ilegales a través de fronteras y zonas de control sin ser detectados por las autoridades.

Despliegue de ciberarmas: Los drones de ataque autónomo podrían ser utilizados para infiltrarse en áreas protegidas y desplegar dispositivos de

ciberataque, como dispositivos de interferencia de señales o dispositivos de acceso remoto, en sistemas informáticos y de comunicaciones críticos.

4.1.1.4.2.5 Engañar al reconocimiento facial

Uso de maquillaje y accesorios: Algunas personas pueden aplicar maquillaje específico o usar accesorios, como gafas o pelucas, para alterar su apariencia y engañar a los sistemas de reconocimiento facial, dificultando su identificación.

Impresión 3D de máscaras: Se pueden crear máscaras realistas a través de la impresión 3D que imitan el rostro de otra persona, lo que permite a los delincuentes suplantar la identidad de alguien y evadir la detección.

Ataques de adversarios en las redes neuronales: Los ciberdelincuentes pueden introducir ruido o manipular imágenes digitales para confundir a los sistemas de reconocimiento facial, lo que podría resultar en identificaciones erróneas o en la incapacidad de reconocer a personas conocidas.

Uso de tecnología de camuflaje: Se pueden utilizar dispositivos y prendas de vestir con tecnología de camuflaje, como capuchas con patrones específicos o lentes reflectantes, para confundir a los sistemas de reconocimiento facial y evitar ser identificados.

Manipulación de metadatos: Los delincuentes pueden modificar los metadatos de imágenes y videos, como las fechas y horas de captura, para crear confusiones en la cronología de eventos y dificultar el rastreo de sus movimientos por parte de las autoridades que utilizan sistemas de reconocimiento facial.

4.1.1.4.2.6 Bombardeo de mercado

Manipulación de algoritmos de trading: Los delincuentes pueden utilizar inteligencia artificial para manipular algoritmos de trading en los mercados

financieros, creando fluctuaciones artificiales en los precios de acciones y otros instrumentos financieros para obtener ganancias ilícitas.

Creación de *bots* para la manipulación de opiniones: Los ciberdelincuentes pueden crear y utilizar *bots* que generen opiniones falsas o comentarios negativos sobre productos o empresas en línea, lo que puede afectar el comportamiento de los consumidores y las decisiones de inversión en el mercado.

Ataques de *spoofing*[6] y manipulación del mercado: Los delincuentes pueden utilizar la inteligencia artificial para realizar ataques de *spoofing*, colocando y retirando rápidamente órdenes de compra y venta en el mercado para crear una falsa impresión de demanda o suministro y manipular los precios.

Falsificación de datos financieros: La inteligencia artificial puede ser utilizada para crear y difundir informes financieros fraudulentos o datos manipulados, lo que puede llevar a la toma de decisiones de inversión erróneas y a la inestabilidad del mercado.

[6] El "spoofing" es una técnica utilizada en ciberseguridad donde alguien se hace pasar por otra persona, dispositivo o programa, generalmente con la intención de ganar acceso a recursos de información o para engañar a otros sistemas o usuarios. Hay varios tipos de spoofing, aquí te presento algunos: Spoofing de IP: Esto ocurre cuando un atacante falsifica la dirección IP en los paquetes de datos para que parezca que provienen de una fuente confiable. Esto puede ser utilizado para ocultar la identidad del atacante o para eludir las medidas de seguridad de una red. Spoofing de correo electrónico: En este caso, los atacantes envían correos electrónicos que parecen provenir de una dirección de correo electrónico legítima, a menudo con el objetivo de engañar al receptor para que revele información personal o financiera. Spoofing de sitio web: Aquí, un atacante crea una copia de un sitio web legítimo con el fin de engañar a los usuarios para que introduzcan información sensible, como contraseñas o números de tarjetas de crédito. Spoofing de GPS: En este tipo de ataque, las señales de GPS son manipuladas para mostrar una ubicación incorrecta. Esto puede ser utilizado para engañar a los sistemas de navegación o a otros dispositivos que dependen de la información de GPS. Spoofing de llamadas o ID de llamadas: Aquí, los atacantes pueden falsificar el número que aparece en el identificador de llamadas para que parezca que están llamando desde un número diferente.

Para protegerse contra el spoofing, es importante mantener los sistemas de seguridad actualizados, ser cauteloso al proporcionar información personal o financiera, y verificar la autenticidad de las comunicaciones y sitios web antes de interactuar con ellos.

Ataques de manipulación de noticias y desinformación: Los ciberdelincuentes pueden utilizar inteligencia artificial para generar y propagar noticias falsas o desinformación relacionada con empresas, industrias o eventos económicos, lo que puede afectar el comportamiento de los inversores y causar fluctuaciones en el mercado.

4.1.1.4.3 Nivel bajo

4.1.1.4.3.1 Explotación de sesgos

Sesgos en algoritmos de contratación: Los delincuentes pueden aprovechar los sesgos presentes en los algoritmos de contratación de personal para obtener ventajas indebidas en la selección de candidatos, lo que puede resultar en discriminación o favoritismo.

Manipulación de recomendaciones de productos: Los ciberdelincuentes pueden explotar sesgos en sistemas de recomendación de productos en línea para promocionar sus propios productos o perjudicar a sus competidores, lo que puede afectar la percepción del consumidor y las decisiones de compra.

Ataques de *astroturfing*[7]: Los delincuentes pueden utilizar cuentas falsas o bots en redes sociales para crear la ilusión de un apoyo generalizado o una opinión

[7] *Astroturfing* es una práctica de desinformación que involucra la creación de apariencia de apoyo popular espontáneo a una idea, individuo, producto o política, cuando en realidad es un movimiento patrocinado o impulsado por una organización o entidad interesada. El término proviene de la marca *AstroTurf*, que es un tipo de césped sintético diseñado para parecer césped natural, aludiendo a la idea de que el apoyo es falso (sintético) en lugar de genuino (natural). Un ejemplo de *astroturfing* podría ser una compañía que paga a personas para publicar reseñas positivas en línea de sus productos, creando la impresión de que muchos clientes satisfechos están compartiendo sus experiencias positivas, cuando en realidad es una campaña de marketing organizada. El *astroturfing* puede suceder en muchos contextos, como las redes sociales, donde se crean cuentas falsas para dar la impresión de un fuerte apoyo a una causa o idea, o en la política, donde se puede intentar influir en la opinión pública o en las decisiones políticas mediante la creación de apariencia de un amplio apoyo público. La práctica del *astroturfing* es ampliamente considerada engañosa y poco ética, y en algunos casos puede ser ilegal. También puede ser dañina, ya que puede sesgar el discurso público, influir en la toma de decisiones basada en información falsa y erosionar la confianza en las plataformas en línea.

negativa sobre un tema específico, lo que puede influir en la opinión pública y la toma de decisiones políticas.

Explotación de sesgos en sistemas de crédito y préstamos: Los ciberdelincuentes pueden aprovechar sesgos en sistemas de calificación crediticia y algoritmos de préstamos para obtener financiamiento o crédito de manera fraudulenta, lo que puede llevar a pérdidas para las instituciones financieras y afectar la estabilidad económica.

Manipulación de algoritmos de búsqueda: Los delincuentes pueden explotar sesgos en los motores de búsqueda para posicionar contenido fraudulento o malicioso en las primeras posiciones de los resultados de búsqueda, lo que puede llevar a la difusión de información errónea o engañosa y afectar la percepción y el comportamiento del usuario.

4.1.1.4.3.2 Bots antirrobo

Compra automatizada de productos limitados: Delincuentes pueden utilizar *bots* antirrobo para comprar automáticamente productos de edición limitada o de alta demanda, como zapatillas o entradas para eventos, y luego revenderlos a precios inflados en el mercado secundario.

Manipulación de subastas en línea: Los ciberdelincuentes pueden usar *bots* para monitorear y manipular subastas en línea, realizando pujas automáticas en el último momento, lo que puede resultar en un aumento artificial de los precios y perjudicar a otros participantes.

Extracción de datos en sitios web: Los delincuentes pueden usar *bots* antirrobo para extraer información valiosa de sitios web, como precios de

productos, datos de contacto o información sobre la competencia, lo que puede resultar en ventajas competitivas injustas o la violación de la privacidad del usuario.

Ataques de fuerza bruta a cuentas en línea: Los ciberdelincuentes pueden utilizar *bots* antirrobo para realizar ataques de fuerza bruta en cuentas en línea, probando miles de combinaciones de nombres de usuario y contraseñas para obtener acceso no autorizado a cuentas personales o empresariales.

Generación automática de comentarios y reseñas falsas: Los delincuentes pueden emplear *bots* antirrobo para generar y publicar automáticamente comentarios y reseñas falsas en sitios web y plataformas de comercio electrónico, lo que puede afectar la reputación de empresas y productos y confundir a los consumidores.

4.1.1.4.3.3 Evadir la detección de inteligencia artificial

Uso de *Captcha*[8] falso: Los delincuentes pueden crear Captcha falso o manipulado para engañar a los sistemas de inteligencia artificial y permitir el acceso a bots maliciosos en sitios web y foros en línea.

[8] CAPTCHA es un acrónimo que significa "Completely Automated Public Turing test to tell Computers and Humans Apart" (Prueba de Turing completamente automática para diferenciar computadoras de humanos). Es un tipo de desafío-respuesta utilizado en computación para determinar si el usuario es humano. El propósito principal de un CAPTCHA es prevenir el spam y el abuso automatizado de servicios en línea. Por ejemplo, un bot podría intentar crear miles de cuentas de correo electrónico por minuto, pero un CAPTCHA detendría este comportamiento al requerir una tarea que los humanos pueden realizar fácilmente pero que los bots no pueden. Las versiones tempranas de CAPTCHA a menudo implicaban la introducción de un conjunto de letras y números distorsionados que una computadora tendría dificultades para reconocer. Sin embargo, estos han evolucionado en el tiempo a medida que la tecnología de reconocimiento de imágenes por parte de las máquinas ha mejorado. Las formas modernas de CAPTCHA pueden implicar una variedad de tareas que requieren la interpretación de imágenes, el reconocimiento de patrones y otras tareas de toma de decisiones que actualmente son difíciles para las máquinas. Un ejemplo común es el reCAPTCHA de Google, que puede requerir que los usuarios identifiquen ciertos objetos en una serie de imágenes. A pesar de su utilidad, las críticas a CAPTCHA incluyen que pueden ser difíciles de interpretar para los humanos, particularmente para aquellos con discapacidades visuales, y que pueden representar una barrera de accesibilidad si no se implementan correctamente las alternativas accesibles.

Generación de imágenes adversarias: Los ciberdelincuentes pueden utilizar imágenes adversarias, que son imágenes especialmente diseñadas para engañar a los sistemas de inteligencia artificial, como el reconocimiento facial, lo que les permite evadir la detección y el seguimiento.

Ataques de envenenamiento de datos: Los atacantes pueden introducir datos incorrectos o maliciosos en conjuntos de datos de aprendizaje automático para confundir o comprometer el rendimiento de los sistemas de inteligencia artificial y evadir la detección.

Suplantación de cuentas legítimas: Los delincuentes pueden suplantar cuentas legítimas en redes sociales y plataformas en línea, haciéndose pasar por usuarios legítimos para evitar ser detectados por sistemas de inteligencia artificial que buscan comportamientos anómalos o maliciosos.

Uso de redes privadas virtuales (VPN) y *proxies*[9]: Los ciberdelincuentes pueden utilizar VPN y *proxies* para ocultar su ubicación y actividad en línea, lo que dificulta que los sistemas de inteligencia artificial detecten y rastreen sus acciones.

[9] Un proxy, en términos de redes informáticas, es un servidor que actúa como intermediario entre un usuario y la red de Internet. Los servidores proxy proporcionan varios niveles de funcionalidad, seguridad y privacidad, dependiendo de su configuración y uso. Tipos: Proxy de reenvío: Este es el tipo más común de proxy. Toma las solicitudes de los usuarios para acceder a información en Internet y las reenvía a los servidores correspondientes. Proxy inverso: Este tipo de proxy está generalmente más cerca del servidor web que del usuario final. Se utiliza para distribuir la carga entre una serie de servidores o para proporcionar una capa adicional de seguridad o anonimato para el servidor web. Proxy de anonimato: Estos proxies se utilizan para hacer que las actividades del usuario sean anónimas al ocultar la dirección IP del usuario. Esto puede ser útil para proteger la privacidad del usuario o para acceder a sitios que están bloqueados geográficamente. Proxy de alta anonimato (Elite): No solo oculta la dirección IP del usuario, sino que también no envía cabeceras HTTP que podrían revelar que el usuario está utilizando un proxy. Proxy de filtrado de contenido: Algunas escuelas y empresas utilizan proxies para filtrar el contenido que se puede acceder a través de su red, bloqueando sitios web específicos o tipos de contenido.

Un uso común de los servidores proxy es acceder a contenido que está geográficamente restringido. Por ejemplo, si un servicio de streaming solo está disponible en ciertos países, un usuario podría configurar un proxy para que parezca que su tráfico de Internet está originándose en uno de esos países, permitiéndole acceder al contenido. Es importante mencionar que aunque los proxies pueden proporcionar una capa adicional de seguridad y privacidad, no son infalibles y no deben ser utilizados como sustituto de las buenas prácticas de seguridad en línea.

4.1.1.4.3.4 Reseñas falsas creadas por inteligencia artificial

Generación de reseñas falsas positivas: Los delincuentes pueden utilizar la Inteligencia artificial para crear reseñas falsas positivas en línea, con el objetivo de mejorar la reputación de productos o servicios deficientes y engañar a los consumidores para que realicen compras basadas en información errónea.

Creación de reseñas falsas negativas: Los ciberdelincuentes también pueden utilizar la inteligencia artificial para generar reseñas falsas negativas en un intento de dañar la reputación de productos o servicios competidores, desviando así a los clientes hacia su propia oferta.

Manipulación de clasificaciones y puntuaciones: Mediante la generación de un gran volumen de reseñas falsas, tanto positivas como negativas, los atacantes pueden manipular las clasificaciones y puntuaciones de productos o servicios en plataformas en línea, lo que afecta la percepción y las decisiones de compra de los consumidores.

Imitación del estilo de escritura de reseñas legítimas: La inteligencia artificial puede ser utilizada para imitar el estilo de escritura de reseñas legítimas, lo que dificulta la detección de reseñas falsas por parte de sistemas de moderación y otros usuarios.

Generación automática de reseñas en múltiples plataformas: Los delincuentes pueden utilizar la inteligencia artificial para generar automáticamente reseñas falsas en una variedad de plataformas y sitios web, ampliando su impacto y dificultando la detección y eliminación de estas reseñas.

4.1.1.4.3.5 Asecho asistido por inteligencia artificial

Recopilación y análisis de información: Los acosadores pueden utilizar la inteligencia artificial para recopilar y analizar grandes cantidades de información sobre sus víctimas, incluidas las redes sociales, las interacciones en línea y la información personal, lo que les permite obtener un conocimiento detallado de sus vidas y rutinas.

Identificación de patrones y hábitos: Mediante el uso de algoritmos de aprendizaje automático, los acosadores pueden identificar patrones y hábitos de comportamiento de sus víctimas, lo que les permite predecir y anticipar sus movimientos y acciones.

Generación de perfiles falsos: La inteligencia artificial puede ser utilizada para crear perfiles falsos en redes sociales y plataformas de citas, permitiendo a los acosadores interactuar con sus víctimas de manera anónima y recopilar más información sobre ellas.

Manipulación de imágenes y videos: Los acosadores pueden utilizar la inteligencia artificial para generar imágenes y videos manipulados o *deepfakes* de sus víctimas, lo que puede ser utilizado para chantajear, intimidar o dañar la reputación de las personas.

Vigilancia en tiempo real: La inteligencia artificial puede ser utilizada para monitorear en tiempo real las actividades en línea de las víctimas, incluido el seguimiento de sus ubicaciones y la interceptación de sus comunicaciones, lo que permite a los acosadores mantener un control constante sobre sus víctimas y ajustar sus tácticas en consecuencia.

4.1.1.4.3.6 Falsificación

Falsificación de documentos: La inteligencia artificial puede ser utilizada para falsificar documentos, como identificaciones, pasaportes y certificados, mediante el uso de algoritmos de generación de imágenes y manipulación de textos, lo que facilita la creación de documentos falsos convincentes.

Falsificación de firmas: Los algoritmos de aprendizaje automático pueden ser entrenados para replicar la firma de una persona, permitiendo a los delincuentes falsificar firmas en contratos, cheques y otros documentos legales.

Falsificación de arte: La inteligencia artificial puede ser utilizada para crear obras de arte falsas que imiten el estilo de artistas famosos, lo que dificulta la detección de falsificaciones y aumenta el riesgo de fraude en el mercado del arte.

Falsificación de productos: Los delincuentes pueden utilizar la inteligencia artificial para diseñar y fabricar productos falsificados, como productos electrónicos, ropa y accesorios de marca, que son difíciles de distinguir de los originales, lo que lleva a una pérdida de ingresos para las empresas y posibles daños a los consumidores.

Falsificación de monedas y billetes: La inteligencia artificial también puede ser utilizada para crear monedas y billetes falsos de alta calidad, utilizando técnicas de impresión y grabado avanzadas, lo que puede llevar a la desestabilización de la economía y la pérdida de confianza en el sistema financiero.

4.1.1.5 Modelos de imputación en supuestos de criminalidad mediante inteligencia artificial

El criterio de atribución de responsabilidad penal frente a las acciones típicas de la inteligencia artificial no es nada pacifico. Desde la posición de Morales

(2021) se tiene que triangular entre el creador, programador o fabricante o usuario de la inteligencia artificial y la persona que no ejecuta el control debido. En consecuencia, estas dificultades de imputación pueden ser más complicada frente a la poca regulación jurídica sobre los límites y alcances de la inteligencia artificial fuerte y débil.

Para establecer la responsabilidad penal del programador de inteligencia artificial, se deben considerar diversos criterios, como el nivel de control que tenía el programador sobre la inteligencia artificial, la previsibilidad de las acciones de la inteligencia artificial y la intención del programador en la creación y uso de la inteligencia artificial.

Determinar la responsabilidad penal en casos de delitos cometidos por inteligencia artificial presenta desafíos únicos. Estos incluyen la autonomía de la inteligencia artificial, la complejidad de los sistemas de aprendizaje automático y la dificultad de rastrear la cadena de responsabilidad en la creación y uso de la inteligencia artificial.

Para abordar estos desafíos, se han propuesto diversas soluciones y enfoques jurídicos, incluida la creación de un marco legal específico para la responsabilidad penal de los programadores de inteligencia artificial, la imposición de responsabilidad civil en lugar de responsabilidad penal y la creación de entidades legales para las inteligencias artificiales que actúen de manera autónoma. Hallevy (2019) plantea tres modeles de imputación para asignar responsabilidad penal frente a la inteligencia artificial:

4.1.1.5.1 Modelo de imputación: Inteligencia artificial "inocente" o perpetración de "otro"

La inteligencia artificial solo es un instrumento. De acuerdo con Hallevy (2019) la inteligencia artificial es inocente y no tiene capacidad humanas para acciones delictivas, dejando dicha asignación al programador o usuario, en caso de la inteligencia artificial sea autónomo e independiente se le asignará responsabilidad al programador o usuario.

4.1.1.5.2 Modelo de imputación: Consecuencia probable natural

La inteligencia artificial es probable que cometa delito. De acuerdo con Hallevy (2019) los programadores o creadores realizan la construcción de la inteligencia artificial que durante su piloto o ejecución definitiva comete delitos que pueden ser facilitados por negligencia o dolo en la programación, frente a agente autónomo se le asigna responsabilidad.

4.1.1.5.3 Modelo de imputación: Responsabilidad directa

La inteligencia artificial es probable que cometan delitos. De acuerdo con Hallevy (2019) el problema es vincular el elemento interno con el externo, pues cada inteligencia artificial varía en sus sistemas cognitivo y autónomo.

4.1.2 Resultados de orden normativo

4.1.2.1 Normatividad jurídica interna

Proyecto de Ley 2775/2022 -CR promueve el uso de la inteligencia artificial en favor del desarrollo económico y social del país, es una iniciativa legislativa que busca impulsar el progreso tecnológico en nuestro país. Esta ley tiene como objetivo principal fomentar el uso de la inteligencia artificial en el marco del proceso

nacional de transformación digital, privilegiando a la persona humana y garantizando su uso ético, sostenible, transparente, replicable y responsable.

La inteligencia artificial es una tecnología que ha revolucionado la forma en que las empresas y los gobiernos operan. Su capacidad para procesar grandes cantidades de datos y tomar decisiones precisas y rápidas ha permitido mejorar la eficiencia y reducir los costos en muchos sectores. Además, su potencial para mejorar la calidad de vida de las personas es enorme.

En este sentido, el Proyecto de Ley 2775/2022 -CR establece un marco regulatorio para el uso de la inteligencia artificial en nuestro país. Este marco se basa en tres principios fundamentales: ética, transparencia y responsabilidad. La ética se refiere a garantizar que el uso de la inteligencia artificial sea compatible con los valores humanos fundamentales. La transparencia se refiere a garantizar que las decisiones tomadas por sistemas basados en inteligencia artificial sean comprensibles para los seres humanos. La responsabilidad se refiere a garantizar que los sistemas basados en inteligencia artificial sean responsables por sus acciones. Además, esta ley establece un enfoque pluralista para el desarrollo de políticas orientadas a regular el uso de la inteligencia artificial en nuestro país. Se promueve la participación de personas naturales y jurídicas, organizaciones e instituciones públicas y privadas en el debate para el desarrollo de políticas orientadas a la regulación sobre el uso de la inteligencia artificial en el país.

4.1.2.2 Derecho internacional

En relación a la criminalidad mediante inteligencia artificial, no encontramos concretamente normatividad internacional que abarque dicho

fenómeno, pero podemos encontramos avances de la Unión Europea que es más tendiente a proteger datos personales, en donde destaca:

Unión Europea: La mayoría de los países de la Unión Europea tienen sus propias estrategias nacionales para regular la Inteligencia Artificial, pero estas son en gran medida convergentes. La Unión Europea está guiada por una Estrategia Europea sobre Inteligencia Artificial, apoyada por un Grupo de Expertos de Alto Nivel en Inteligencia Artificial.

La Comisión Europea ha sido líder en la regulación de la inteligencia artificial a nivel internacional. Una de las iniciativas más destacadas en este ámbito ha sido la publicación de las Directrices éticas para una inteligencia artificial fiable (Comisión Europea, 2019). Estas directrices se centran en promover la Inteligencia Artificial confiable, la cual se define en tres componentes que deben cumplirse durante todo el ciclo de vida del sistema de inteligencia artificial:

- Debe ser legal, cumpliendo con todas las leyes y regulaciones aplicables.
- Debe ser ética, asegurando la adherencia a principios éticos y valores.
- Debe ser robusta, tanto desde una perspectiva técnica como social, ya que, incluso con buenas intenciones, los sistemas de inteligencia artificial pueden causar daño no intencional.

Cada componente es necesario, pero no suficiente para el logro de la inteligencia artificial confiable. Idealmente, los tres componentes trabajan en armonía y se superponen en su operación. Si en la práctica surgen tensiones entre estos componentes, la sociedad debe esforzarse por alinearlos.

4.1.3 Casos emblemáticos de inteligencia artificial

4.1.3.1 El caso de ChatGPT

ChatGPT es tipo de inteligencia artificial generativa de texto a texto. GPT son las siglas de "Generative Pretrained Transformer", que es un tipo de modelo de inteligencia artificial desarrollado por OpenAI. Es un ejemplo de este tipo de modelo, específicamente, la versión 3.5 y 4.0:

- Generativo: Esto significa que genera (o produce) texto. No se proporciona una lista predefinida de respuestas; en cambio, genera respuestas en función de los patrones y la información que ha aprendido durante su entrenamiento.
- Preentrenado: Antes de que se utilice para conversar o responder preguntas, se debe saber que fue "entrenado" en una enorme cantidad de texto. Esto permite entender patrones de lenguaje, gramática, hechos sobre el mundo, y más. Sin embargo, esto también significa que sólo tiene información hasta la fecha en que fue entrenada, que en este caso es septiembre de 2021.
- Transformer: Este es el nombre de la arquitectura específica de aprendizaje profundo que utiliza. Los transformers son útiles para entender el contexto a largo plazo en el texto, lo que permite generar respuestas coherentes y relevantes.

ChatGPT es un modelo de inteligencia artificial que puede generar respuestas coherentes y contextualmente relevantes a preguntas y solicitudes, basado en los patrones y la información que aprendió durante su entrenamiento. Sin embargo, este modelo viene creando dilemas como el caso de la redacción original y científica (Diaz, 2023), utilización de datos privados o sensibles sin control (Sempere & Arenas, 2023) el cuestionamiento a la educación actual y el trabajo

(Muñoz, 2023), entre otros problemas que en los próximos años se vendrán registrando.

4.1.3.2 El caso de Midjourney IA

Midjourney es un programa y servicio de inteligencia artificial generativa creado y alojado por un laboratorio independiente de investigación. Inc. Midjourney genera imágenes a partir de descripciones de lenguaje natural, llamadas "prompts", de manera similar a las herramientas de OpenAI como DALL-E y Stable Diffusion. Actualmente, se encuentra en versión beta abierta desde el 12 de julio de 2022 y es accesible a través de un bot de Discord en su servidor oficial.

Existen varios ejemplos de lo que Midjourney es capaz de generar, desde ilustraciones fotorrealistas y detalladas hasta conceptos abstractos y creativos basados en los prompts proporcionados por los usuarios. Algunos de estos ejemplos incluyen representaciones como la foto del Papa con vestimenta de cantante moderno (Zavia, 2023), el arresto de Donald Trump (Ramos, 2023), entre otras fotografías que hacen invisible lo hecho por inteligencia artificial frente a lo realizado por el hombre o lo sucedido en la realidad.

4.2 Contrastación y discusión de las Hipótesis de la investigación

Hipótesis General

Los alcances de la imputación objetiva de la autoría mediata de programador de inteligencia artificial con fines delictivos en el Perú, devienen en vacíos jurídicos para establecer la imputación objetiva del autor mediato programador y la inteligencia artificial como ejecutor material del hecho delictivo.

Hipótesis Específicas

Las consecuencias jurídicas de los vacíos jurídicos en la imputación objetiva de la autoría mediata del programador de inteligencia artificial con fines delictivos en el Perú, es la falta imputación de acción y resultado la impunidad pese a la puesta en peligro o daños de bienes jurídicos.

Se superará los vacíos normativos en la imputación objetiva de la autoría mediata del programador de inteligencia artificial con fines delictivos en el Perú, mediante la adaptación de la imputación objetiva a los supuestos criminalidad mediante inteligencia artificial.

La Hipótesis contratada, evidencia prueba parcialmente en consideración al porcentaje de lo positivo y negativo conjuntivamente, que aprueba y disprueba, respectivamente y parcialmente la hipótesis, conforme a lo siguiente:

4.2.1 Argumentaciones de orden doctrinal

4.2.1.1 Inteligencia artificial como sujeto especial de derecho y mero instrumento de criminalidad

La inteligencia artificial ha irrumpido en la escena global, desencadenando un debate urgente sobre su estatus jurídico. ¿Es la inteligencia artificial un sujeto especial de derecho o simplemente un instrumento para la criminalidad? Es necesario enfrentar esta problemática desde una perspectiva equilibrada, que tenga en cuenta tanto la promesa como el potencial de abuso de la inteligencia artificial y considerar su posible autonomía e independencia de sus creadores, así como su uso abusivo.

El argumento de considerar la inteligencia artificial como un sujeto especial de derecho, esta perspectiva es particularmente relevante cuando se trata de inteligencia artificial fuerte o autónoma, que puede aprender y tomar decisiones sin

la intervención humana directa. En tal caso, puede ser razonable conceder a la inteligencia artificial una especie de "personalidad jurídica", similar a las personas jurídicas, para poder regular su comportamiento. Esta medida podría, de manera eficiente, proporcionar responsabilidad legal directa y permitir que las inteligencias artificiales sean responsables por sus propias acciones, en lugar de derivar toda la responsabilidad hacia los programadores o usuarios.

La perspectiva que considera a la inteligencia artificial como un mero instrumento de criminalidad. Aquí, el foco se sitúa en la responsabilidad de los programadores que diseñan los algoritmos o los usuarios que despliegan abusivamente a la inteligencia artificial. Esta visión tiene sus raíces en el principio jurídico de que solo los seres humanos pueden ser sujetos de derechos y deberes.

Es así, que a medida que la inteligencia artificial se vuelve cada vez más sofisticada, es imperativo que desarrollemos un marco legal que pueda navegar entre estas perspectivas. Un enfoque potencial puede ser combinar elementos de ambos enfoques, reconociendo a la inteligencia artificial como sujeto de derecho en ciertos contextos, mientras que en otros, se considera como un instrumento de criminalidad. Al final, lo más importante es que el marco legal evolucione para proteger a la sociedad y mantener la equidad, al mismo tiempo que fomenta la innovación y el avance tecnológico.

4.2.1.2 La inteligencia artificial, autoría penal e imputación objetiva

Para definir a la autoría penal tenemos al autor directo (Corcino, 2017), autor mediato e instrumental (Aboso, 2017) y coautoría (Arenas, 2017). En este sentido tendremos que aplicar dichos aspectos dogmáticos al fenómeno de la inteligencia artificial que puede contar con los siguientes sujetos: (i) programador o

programadores o empresas desarrolladoras, (ii) usuario de la inteligencia artificial y (iii) la misma inteligencia artificial que puede adquirir autonomía e independencia como agente racional que decida (Leyva et al., 2018), siendo discutible a favor o en contra que pueda imputársele personería jurídica al igual que se ha generado mediante ficción a la persona jurídica. Es así, que se puede dar diversas combinaciones:

- El autor directo el programador o creador, que utiliza la inteligencia artificial como instrumento para materializar el delito. Este sentido se pude hablar de autor directo y la inteligencia artificial solamente es un instrumento más, como lo sería un cuchillo o arma de fuego.
- El programador con autor mediato y la inteligencia artificial como autor material (instrumentalizado), en este supuesto se tendría que asignar personería jurídica a la inteligencia artificial reconocimiento su autonomía e independencia de los que lo programaron.
- El usuario como autor directo y la inteligencia artificial como instrumento, en este sentido el programador tendría una posición neutral o diligente pues debía de haber programado o tomar las medidas para que creación no pueda afectar bienes jurídicos, que pueden acaecer por la manipulación de los usuarios, quedando exento de responsabilidad el programador que demuestra su diligencia y cuidado.
- El usuario como autor mediato y la inteligencia artificial como autor material al tener condición de agente racional y autónomo a sus creadores, si bien es cierto el programador se puede eximir de responsabilidad demostrando diligencia y

cuidado, pero sería ello cuestionable su posición pues su creación a adquirido autonomía.

- Cuando el creador no tomó las condiciones mínimas de cuidado y diligencia para su creación de inteligencia artificial que luego adquirió autonomía y ello fue aprovechado por los usuarios para poder delinquir con esta tecnología, en este último supuesto podría darse una suerte de autoría mediata del programador y la autoría material del usuario y la inteligencia artificial autónoma.

La asignación de responsabilidad penal en delitos cometidos por Inteligencia Artificial constituye un tema de gran debate. Morales (2021) propone una tríada de responsabilidad que involucra al creador, programador o usuario de la inteligencia artificial, señalando que el control insuficiente es un factor de importancia. Añade que el problema se agrava debido a la insuficiente regulación jurídica de la inteligencia artificial, tanto fuerte como débil.

Determinar la responsabilidad penal requiere considerar diversos factores: el control del programador sobre la inteligencia artificial, la previsibilidad de las acciones de la inteligencia artificial y la intención del programador (Morales, 2021). Hallevy (2019) propone tres modelos de imputación. En el primer modelo, la inteligencia artificial es simplemente un instrumento, sin capacidad para delinquir; la responsabilidad recae en el programador o usuario. En el segundo modelo, la inteligencia artificial es propensa a delinquir, debido a la negligencia o dolo en su programación. En el último modelo destaca la dificultad de conectar el elemento interno con el externo, debido a la variabilidad en los sistemas cognitivos de cada inteligencia artificial.

4.2.1.3 Análisis de la imputación objetiva en la criminalidad cometida con inteligencia artificial

La criminalidad e inteligencia artificial, facilitan la ciberdelincuencia. Como lo hace notar Morales (2021) el uso de esta tecnología beneficia a la delincuencia y ataques a bienes jurídicos sin límites de fronteras maximizando sus alcances por medio de la web, que al adquirir autonomía hace pensar su imputabilidad diferente a su fabricante o creador.

4.2.1.2.1 Nivel alto de criminalidad

4.2.1.2.1.1 Suplantación de la identidad en audio y video

Descripción de la conducta criminal: La inteligencia artificial puede utilizarse para crear *deepfakes*, que son manipulaciones de audio y video que hacen parecer que una persona está diciendo o haciendo algo que en realidad no hizo. Esto puede tener graves consecuencias en la extorsión, la difamación y la desinformación.

A.- Imputación objetiva de la conducta

Riego permitido: En este caso, la creación de *deepfakes* para suplantar la identidad de una persona, distorsionando su imagen y voz a través de inteligencia artificial, no se considera un riesgo permitido. No es una actividad que se considere socialmente aceptada ni necesaria para el funcionamiento de la sociedad.

Disminución del riesgo: En la conducta en cuestión no se observa un intento de disminuir el riesgo creado. Al contrario, la creación y distribución de deepfakes aumenta el riesgo de daño a la reputación, la dignidad y la privacidad de la persona suplantada.

Riesgo insignificante: La creación de *deepfakes* plantea un riesgo significativo, no insignificante. Puede causar daños sustanciales, como la pérdida de reputación, la violación de la privacidad, la difamación y la desinformación.

Principio de confianza: El principio de confianza se ve gravemente vulnerado en este caso, ya que se confía en que los usuarios de la web y la inteligencia artificial actúen dentro de las normas éticas y legales, y no utilicen estas herramientas para actividades fraudulentas o perjudiciales.

Prohibición de regreso: Este principio podría aplicarse si la herramienta de inteligencia artificial fue creada con un propósito legítimo (por ejemplo, la edición de video), pero luego fue utilizada indebidamente por un tercero para crear *deepfakes*. Sin embargo, esto no exime de responsabilidad al que crea y difunde los *deepfakes*.

Ámbito de responsabilidad de la víctima: En este caso, la víctima no ha contribuido a la creación del riesgo. El riesgo es creado y controlado por el autor que utiliza la inteligencia artificial para crear y difundir los *deepfakes*.

B.- Imputación Objetiva de resultado:

Dado que los *deepfakes* pueden causar un daño real y significativo, el resultado de crear y difundirlos es imputable a la acción del autor.

Relación de riesgo: Existe una relación directa entre la acción de crear y difundir *deepfakes* y el resultado, que puede ser la violación de la privacidad, la difamación y la desinformación.

Nexos causales desviados: No parece haber una desviación en la cadena causal en este caso. La creación y distribución de *deepfakes* lleva directamente a los posibles daños mencionados.

Interrupción del nexo causal: No se observa una interrupción en el nexo causal. La acción de crear y distribuir *deepfakes* y el daño resultante son atribuibles al autor.

4.2.1.2.1.2 Vehículos sin conductor como armas

Descripción de la conducta criminal: Los vehículos autónomos pueden ser hackeados y utilizados como armas, causando daños a la propiedad y poniendo en riesgo la vida de las personas.

A.- Imputación objetiva de la conducta

Riesgo permitido: En la sociedad actual, el uso de vehículos autónomos e inteligencia artificial es aceptado y se considera un riesgo permitido. Sin embargo, el uso de estos sistemas para cometer actos criminales, como hackear un vehículo autónomo para usarlo como arma, claramente excede el límite de este riesgo permitido y, por lo tanto, no es aceptable.

Disminución del riesgo: En esta situación, no hay indicación de que el perpetrador haya hecho algo para disminuir el riesgo creado por su acción. En cambio, parecería que su intención era aumentar ese riesgo.

Riesgo insignificante: El riesgo creado por el hacking y uso malicioso de un vehículo autónomo para dañar a las personas es significativo y relevante. No puede considerarse un riesgo insignificante.

Principio de confianza: En esta situación, se violó el principio de confianza. Se supone que los usuarios y fabricantes de vehículos autónomos confían en que todos utilizarán la tecnología de manera segur. Al hackear un vehículo autónomo, el perpetrador violó esa confianza.

Prohibición de regreso: La neutralidad del fabricante del vehículo autónomo es evidente, ya que proporcionaron su producto para su uso seguro. El tercer partido que hackeó el vehículo y lo utilizó de manera delictiva es quien llevó la situación a un escenario de riesgo.

Ámbito de responsabilidad de la víctima: En este caso, la víctima no tuvo papel en la creación del riesgo. El riesgo fue creado y ejecutado completamente por el perpetrador.

B.- Imputación objetiva de resultado

Relación de riesgo: Existe una relación directa entre la acción del perpetrador (hackear el vehículo) y el resultado (daño causado por el vehículo).

Nexos causales desviados: No hay indicación de que el nexo causal se haya desviado. La acción del perpetrador llevó directamente al resultado dañino.

Interrupción del nexo causal: No hay interrupción en la secuencia causal. La acción del perpetrador condujo directamente al resultado dañino.

4.2.1.2.1.3 *Phishing* personalizado

Descripción de la conducta criminal: La inteligencia artificial puede mejorar las técnicas de phishing al personalizar los mensajes de correo electrónico y las redes sociales para aumentar la probabilidad de que las víctimas compartan información confidencial o realicen transacciones financieras fraudulentas.

A.- Imputación objetiva de la conducta

Riesgo permitido: En este caso, el uso de la inteligencia artificial para personalizar los mensajes y la experiencia del usuario es un riesgo permitido. Sin embargo, el uso de estas técnicas para engañar a las personas y robar su información confidencial excede el límite de este riesgo y no es aceptable.

Disminución del riesgo: No hay indicios de que el delincuente haya intentado disminuir el riesgo creado por su acción. Al contrario, parece que su objetivo era aumentar el riesgo.

Riesgo insignificante: El riesgo creado por el *phishing* personalizado es significativo y relevante. La pérdida de datos confidenciales puede causar daños financieros, de identidad y psicológicos a las víctimas.

Principio de confianza: Este principio se violó en esta situación. Se espera que los usuarios de internet confíen en que las plataformas y los mensajes que reciben son seguros y legítimos. Al utilizar tácticas de phishing, el delincuente violó esa confianza.

Prohibición de regreso: Los proveedores de correo electrónico y las plataformas de redes sociales ofrecen sus servicios para uso legítimo y seguro. Al utilizar estas plataformas para el phishing, el delincuente llevó la situación a un escenario de riesgo.

Ámbito de responsabilidad de la víctima: La víctima no tiene responsabilidad en la creación del riesgo. El riesgo fue creado y ejecutado completamente por el delincuente.

B. Imputación objetiva de resultado

Relación de riesgo: Existe una relación directa entre la acción del delincuente (el phishing) y el resultado (la pérdida de información confidencial).

Nexos causales desviados: No hay indicios de que el nexo causal se haya desviado. La acción del delincuente llevó directamente al resultado dañino.

Interrupción del nexo causal: No hay interrupción en la secuencia causal. La acción del delincuente condujo directamente al resultado dañino.

4.2.1.2.1.4 Interrumpir los sistemas controlados por inteligencia artificial

Descripción de la conducta criminal: Los ciberataques pueden dirigirse a sistemas controlados por inteligencia artificial, como infraestructuras críticas, con el objetivo de causar interrupciones y daños significativos.

A.- Imputación objetiva de la conducta

Riesgo permitido: En este caso, el riesgo permitido está relacionado con la operación normal de los sistemas de inteligencia artificial. Sin embargo, el ataque a estos sistemas, con el objetivo de alterar los datos de entrenamiento y causar interrupciones, va más allá de este riesgo permitido.

Disminución del riesgo: No hay indicaciones de que los perpetradores del ciberataque hayan intentado disminuir el riesgo creado por su acción. En cambio, su objetivo parecía ser aumentar este riesgo.

Riesgo insignificante: El riesgo creado por el ataque a los sistemas de inteligencia artificial es significativo. Esto puede resultar en daños financieros y de reputación, además de la interrupción de los servicios esenciales.

Principio de confianza: Este principio se ve violado en esta situación. Se espera que los sistemas controlados por inteligencia artificial sean seguros y operen de manera eficiente. Al atacar estos sistemas, los delincuentes rompen esta confianza.

Prohibición de regreso: El uso legítimo de la inteligencia artificial no incluye el ataque a sistemas operados por ella. Al hacerlo, los delincuentes violan la prohibición de regreso.

Ámbito de responsabilidad de la víctima: En este caso, la víctima es el sistema controlado por inteligencia artificial y no tiene responsabilidad en la

creación del riesgo. El riesgo fue creado y ejecutado completamente por los delincuentes.

B. Imputación objetiva de resultado

Relación de riesgo: Hay una relación directa entre la acción de los delincuentes (el ataque) y el resultado (la interrupción y daños).

Nexos causales desviados: No hay indicios de que el nexo causal se haya desviado. La acción de los delincuentes llevó directamente al resultado dañino.

Interrupción del nexo causal: No hay interrupción en la secuencia causal. La acción de los delincuentes condujo directamente al resultado dañino.

4.2.1.2.1.5 Noticias falsas creadas por inteligencia artificial

Descripción de la conducta criminal: La inteligencia artificial puede generar noticias falsas y desinformación a gran escala, lo que puede influir en la opinión pública y tener consecuencias políticas y sociales.

A.- Imputación objetiva de la conducta

Riesgo permitido: La utilización de inteligencia artificial en diversos aspectos de nuestra sociedad es un riesgo permitido y es un hecho cotidiano. Sin embargo, la generación de noticias falsas o "*fake news*" mediante inteligencia artificial sobrepasa el límite del riesgo permitido, ya que se está manipulando la información con intenciones engañosas, lo que puede afectar negativamente la opinión pública y provocar daños en la reputación de las personas y organizaciones implicadas.

Disminución del riesgo: Aquí se evalúa si los creadores de la inteligencia artificial que genera noticias falsas han tomado medidas para minimizar los riesgos

asociados con su uso. Por ejemplo, si han incorporado algún sistema de verificación de hechos o de detección de contenido falso.

Riesgo insignificante: El riesgo asociado a la generación de noticias falsas mediante inteligencia artificial no es insignificante. Al contrario, tiene un alto impacto en la sociedad y puede causar daños considerables, como la manipulación de la opinión pública y la propagación de desinformación.

Principio de confianza: En este caso, se ha roto el principio de confianza ya que las inteligencias artificiales se están utilizando para crear y propagar noticias falsas. Se espera que las inteligencias artificiales actúen de acuerdo con los límites éticos y legales establecidos, y en este caso, no se están cumpliendo.

Prohibición de regreso: La inteligencia artificial puede ser programada para generar contenido informativo, pero cuando se utiliza para crear noticias falsas, no se puede "regresar" a su estado original o a su propósito inicial sin alterar su programación.

Ámbito de responsabilidad de la víctima: Las víctimas de las noticias falsas generadas por inteligencia artificial no son responsables de la creación del riesgo, ya que no tienen control sobre la generación de estas noticias.

B. Imputación objetiva de resultado

Relación de riesgo: Existe una relación directa entre la creación de noticias falsas mediante inteligencia artificial y el riesgo de desinformación y manipulación de la opinión pública.

Nexos causales desviados: La causa directa de la generación de noticias falsas es la programación y uso de la inteligencia artificial con este fin, por lo que no hay un desvío en el nexo causal.

Interrupción del nexo causal: En este caso, no se presenta una interrupción en el nexo causal. La acción de la Inteligencia artificial, programada y utilizada para generar noticias falsas, conduce directamente al resultado de la propagación de desinformación.

4.2.1.2.2 Nivel medio

4.2.1.2.2.1 Robots militares

Descripción de la conducta criminal: La inteligencia artificial puede ser utilizada en la creación de robots militares, aumentando el riesgo de conflictos armados y violaciones de derechos humanos.

A.- Imputación objetiva de la conducta

Riesgo permitido: La creación de robots militares utilizando inteligencia artificial incorpora un grado de riesgo, especialmente en términos de posibles conflictos armados y violaciones de los derechos humanos. Sin embargo, en algunos contextos, este riesgo podría ser visto como permitido, si se considera que la defensa nacional y la seguridad son intereses legítimos de las naciones. Pero es un punto muy debatible y depende mucho del contexto y las garantías existentes para controlar estos riesgos.

Disminución del riesgo: Aquí se examinaría si los desarrolladores de los robots militares con inteligencia artificial están tomando medidas para reducir los riesgos asociados con su uso. Esto podría implicar la inclusión de salvaguardas y protocolos para prevenir su mal uso, o la implementación de funciones que limiten su capacidad para infligir daño.

Riesgo insignificante: Dado el poder destructivo potencial de los robots militares, es difícil argumentar que el riesgo asociado con su uso es insignificante.

Estos robots podrían infligir daños significativos y representar un riesgo relevante para el bien jurídico protegido.

Principio de confianza: Según este principio, los desarrolladores de robots militares pueden confiar en que sus productos serán utilizados de manera responsable por los militares. Sin embargo, esto depende en gran medida de las leyes y regulaciones que rigen el uso de dichos robots, y de si estas son respetadas.

Prohibición de regreso: Si un tercero, como un hacker, interviene y usa el robot militar para fines destructivos, el desarrollador original puede no ser considerado responsable del daño causado, siempre y cuando haya tomado medidas adecuadas para prevenir tal intervención.

Ámbito de responsabilidad de la víctima: En este caso, es difícil determinar el papel de la víctima, ya que los posibles "víctimas" serían aquellas personas que podrían ser afectadas en un conflicto armado. Ellos no tienen control sobre el uso de los robots militares.

B.- Imputación objetiva de resultado

Relación de riesgo: En el caso de los robots militares, existe una relación clara entre el riesgo creado (robots militares capaces de causar daño) y los posibles resultados (conflictos armados, violaciones de derechos humanos).

Nexos causales desviados: Si los robots militares se utilizan de manera que resulta en daño, hay un vínculo directo entre el desarrollo de los robots y el daño causado. Sin embargo, este vínculo puede verse afectado si hay intervención de terceros o si el uso de los robots se sale del propósito originalmente previsto.

Interrupción del nexo causal: Si se produce una interrupción en la secuencia causal, como la intervención de un tercero, entonces la responsabilidad del

desarrollador puede ser cuestionada. Sin embargo, si se puede probar que el desarrollador no tomó medidas adecuadas para prevenir dicha intervención, entonces todavía podrían ser considerados responsables.

4.2.1.2.2.2 Aceite de serpiente

Descripción de la conducta criminal: El "aceite de serpiente" se refiere a la promoción de productos y servicios de inteligencia artificial que hacen promesas engañosas o fraudulentas a los consumidores y empresas.

A.- Imputación objetiva de la conducta

Riesgo permitido: La conducta en cuestión, el "aceite de serpiente", supone la promoción de servicios de inteligencia artificial con promesas engañosas. Esto no puede considerarse como un riesgo permitido, dado que implica un engaño deliberado hacia consumidores y empresas.

Disminución del riesgo: No se aprecia ninguna acción que tenga como finalidad la disminución del riesgo o daño creado por la conducta descrita.

Riesgo insignificante: El riesgo no es insignificante en este caso, ya que puede conducir a la pérdida financiera o de recursos para los consumidores y empresas engañados.

Principio de confianza: Este principio se ve violado, ya que los consumidores y empresas confían en que los servicios de inteligencia artificial anunciados funcionarán como se promete, lo cual no sucede.

Prohibición de regreso: En este caso, si bien es posible que el software de inteligencia artificial proporcionado sea neutral, el uso fraudulento del mismo por parte del promotor del "aceite de serpiente" viola este principio.

Ámbito de responsabilidad de la víctima: Las víctimas, en este caso los consumidores y empresas, no contribuyen a la creación del riesgo, por lo que no se puede atribuirles ninguna responsabilidad.

B. Imputación objetiva del resultado

Relación de riesgo: Hay una clara relación entre la conducta del autor del "aceite de serpiente" y el resultado, que es la pérdida financiera o de recursos por parte de los consumidores y empresas.

Nexos causales desviados: No se aprecian nexos causales desviados, ya que el daño sufrido por los consumidores y empresas es directamente atribuible a la conducta del autor del "aceite de serpiente".

Interrupción del nexo causal: No se aprecia ninguna interrupción en el nexo causal, ya que el resultado dañoso es consecuencia directa de la conducta del autor del "aceite de serpiente".

4.2.1.2.2.3 Ciberataques basados en el aprendizaje

Descripción de la conducta criminal: La inteligencia artificial puede mejorar la eficacia de los ciberataques al adaptarse y aprender de las defensas y contramedidas implementadas por las víctimas.

A.- Imputación objetiva de la conducta

Riesgo permitido: No se puede considerar los ciberataques basados en el aprendizaje como un riesgo permitido. Estos ataques implican la alteración o daño intencionado a un sistema digital, lo que está claramente fuera de lo que sería aceptable en un entorno de interacción digital normal.

Disminución del riesgo: No se aprecia ninguna acción orientada a disminuir el riesgo asociado con esta conducta.

Riesgo insignificante: El riesgo que suponen estos ataques no es en absoluto insignificante, ya que pueden causar daños significativos a los sistemas digitales y a la información contenida en ellos.

Principio de confianza: Este principio se ve violado, ya que los sistemas digitales son diseñados con la expectativa de que no serán atacados o dañados intencionadamente.

Prohibición de regreso: Los ciberataques implican una transgresión deliberada de las normas y expectativas de conducta en el entorno digital, lo que viola el principio de prohibición de regreso.

Ámbito de responsabilidad de la víctima: En la mayoría de los casos, las víctimas de estos ataques (es decir, los sistemas digitales y su información) no son responsables de la creación del riesgo.

B. Imputación objetiva del resultado

Relación de riesgo: Hay una relación de riesgo clara entre la acción del atacante y el resultado dañoso.

Nexos causales desviados: No hay nexos causales desviados aparentes, ya que el resultado es directamente atribuible a la acción del atacante.

Interrupción del nexo causal: No hay interrupciones en el nexo causal, ya que el daño es el resultado directo del ciberataque.

4.2.1.2.2.4 Drones de ataque autónomo

Descripción de la conducta criminal: Los drones se fortalecen con la inteligencia artificial. Con base en Hernández (2019) son vehículos sin tripulación a control remoto que dotados de inteligencia artificial adquieren autonomía, por lo de ahí la preocupación por su uso. Los drones de ataque autónomo pueden ser

utilizados para llevar a cabo operaciones militares y terroristas sin la intervención humana directa, lo que plantea preocupaciones éticas y de responsabilidad.

A.- Imputación objetiva de la conducta

Riesgo permitido: El uso de drones de ataque autónomo para cometer actos delictivos no se encuentra dentro del riesgo permitido. Si bien los drones pueden ser utilizados para muchos fines legítimos y útiles, el uso intencionado de estos para actividades ilegales está fuera de lo que sería aceptable.

Disminución del riesgo: No hay ninguna acción orientada a disminuir el riesgo asociado con esta conducta. En cambio, el uso de drones de ataque autónomo para fines ilegales aumenta el riesgo.

Riesgo insignificante: El riesgo asociado a esta conducta no es insignificante. Los drones de ataque autónomo pueden causar daños materiales y humanos significativos.

Principio de confianza: Este principio se ve violado en esta conducta. Los drones se han desarrollado y se utilizan con la confianza de que se emplearán de manera responsable y legal.

Prohibición de regreso: El uso de drones de ataque autónomo para cometer actos ilegales viola claramente la prohibición de regreso.

Ámbito de responsabilidad de la víctima: Las víctimas de los ataques de drones autónomos no son responsables de la creación del riesgo.

Imputación objetiva del resultado

Relación de riesgo: Hay una relación de riesgo clara entre la acción de controlar un dron de ataque autónomo y el resultado dañoso.

Nexos causales desviados: En este caso, no parece haber nexos causales desviados.

Interrupción del nexo causal: No hay interrupción en el nexo causal, ya que el daño es causado directamente por el dron de ataque autónomo.

4.2.1.2.2.5 Engañar al reconocimiento facial

Descripción de la conducta criminal: La inteligencia artificial puede ser utilizada para desarrollar técnicas que engañen a los sistemas de reconocimiento facial, lo que puede tener implicaciones en la seguridad y la privacidad.

A.- Imputación objetiva de la conducta

Riesgo permitido: El acto de engañar a los sistemas de reconocimiento facial para fines malintencionados no se encuentra dentro del riesgo permitido. El reconocimiento facial se implementa con el fin de aumentar la seguridad y proteger la privacidad, por lo tanto, cualquier intento de burlar estos sistemas está claramente fuera de lo que sería considerado un uso legítimo y aceptable.

Disminución del riesgo: Aquellos que buscan engañar a los sistemas de reconocimiento facial están aumentando el riesgo, no disminuyéndolo.

Riesgo insignificante: El riesgo asociado con esta conducta no es insignificante. El engaño de los sistemas de reconocimiento facial puede tener graves consecuencias, como permitir el acceso no autorizado a áreas seguras o la usurpación de identidad.

Principio de confianza: El principio de confianza se ve violado en esta conducta. Los sistemas de reconocimiento facial se utilizan con la confianza de que funcionarán correctamente y proporcionarán un nivel adicional de seguridad.

Prohibición de regreso: La prohibición de regreso se viola cuando se burlan los sistemas de reconocimiento facial para obtener un beneficio ilegítimo.

Ámbito de responsabilidad de la víctima: Las víctimas de este tipo de engaño no son responsables de la creación del riesgo.

B. Imputación objetiva del resultado

Relación de riesgo: Hay una clara relación de riesgo entre la acción de engañar al sistema de reconocimiento facial y el resultado dañoso.

Nexos causales desviados: No parecen existir nexos causales desviados en este caso.

Interrupción del nexo causal: No hay interrupción en el nexo causal, ya que el daño es causado directamente por el engaño al sistema de reconocimiento facial.

4.2.1.2.2.6 Bombardeo de mercado

Descripción de la conducta criminal: La inteligencia artificial puede ser utilizada para manipular los mercados financieros mediante la generación de información falsa o la realización de transacciones fraudulentas.

A.- Imputación objetiva de la conducta

Riesgo permitido: La manipulación de los mercados financieros mediante el uso de inteligencia artificial no se encuentra dentro del riesgo permitido. Los mercados financieros se rigen por regulaciones estrictas diseñadas para promover la equidad y la transparencia, y cualquier intento de manipulación es claramente ilegal y no permitido.

Disminución del riesgo: Los actos que buscan manipular los mercados financieros aumentan el riesgo, no lo disminuyen.

Riesgo insignificante: La manipulación de los mercados financieros puede tener un efecto significativo en la economía en general y en la vida financiera de los individuos, por lo tanto, el riesgo asociado con esta conducta es todo menos insignificante.

Principio de confianza: El principio de confianza se ve violado en esta conducta. Los participantes en el mercado financiero confían en que las operaciones serán justas y transparentes.

Prohibición de regreso: La prohibición de regreso se viola cuando se manipulan los mercados financieros para obtener un beneficio ilegítimo.

Ámbito de responsabilidad de la víctima: Las víctimas de esta manipulación del mercado no son responsables de la creación del riesgo.

B.- Imputación objetiva de resultado

Relación de riesgo: Hay una clara relación de riesgo entre la acción de manipular el mercado financiero y el resultado dañoso.

Nexos causales desviados: No parecen existir nexos causales desviados en este caso.

Interrupción del nexo causal: No hay interrupción en el nexo causal, ya que el daño es causado directamente por la manipulación del mercado.

4.2.1.2.3 Nivel Bajo

4.2.1.2.3.1 Explotación de sesgos

Descripción de la conducta criminal: Los sistemas de inteligencia artificial pueden tener sesgos incorporados que pueden ser explotados para fines maliciosos, como la discriminación y la propagación de estereotipos.

A.- Imputación objetiva de la conducta

Riesgo permitido: En este caso, el uso de algoritmos para analizar y predecir tendencias es un riesgo permitido y una práctica común en el mundo de la inteligencia artificial. Sin embargo, el riesgo se vuelve no permitido cuando estos algoritmos están sesgados y se utilizan para fines dañinos, como la discriminación y la propagación de estereotipos.

Disminución del riesgo: Aquí, la disminución del riesgo podría ser difícil, ya que los algoritmos son diseñados y controlados por humanos. La responsabilidad caería sobre los desarrolladores de la inteligencia artificial para minimizar cualquier sesgo y prevenir el abuso de sus sistemas.

Riesgo insignificante: No se podría argumentar que el riesgo es insignificante en este caso. El sesgo en la inteligencia artificial puede tener consecuencias importantes, incluyendo la discriminación y la propagación de estereotipos, que son daños sociales relevantes.

Principio de confianza: Existe una violación del principio de confianza, ya que los usuarios de inteligencia artificial confían en que la tecnología será justa y no sesgada.

Prohibición de regreso: En este escenario, la inteligencia artificial se utilizó de manera que cruzó los límites de su uso normal y permitido, manipulándola para explotar sus sesgos para fines maliciosos.

Ámbito de responsabilidad de la víctima: En este caso, las víctimas (aquellos que son discriminados o estereotipados) no tienen control sobre el sesgo incorporado en la inteligencia artificial y, por lo tanto, no se les puede atribuir ninguna responsabilidad.

B. Imputación objetiva de resultado

Relación de riesgo: Existe una clara relación entre el riesgo creado (el sesgo en la inteligencia artificial) y el resultado (la discriminación y la propagación de estereotipos).

Nexos causales desviados: El resultado directamente atribuible al uso sesgado de la inteligencia artificial se manifiesta en la discriminación y la propagación de estereotipos.

Interrupción del nexo causal: No parece haber ninguna interrupción en el nexo causal. El sesgo de la inteligencia artificial directamente resulta en el resultado dañino.

4.2.1.2.3.2 *Bots* antirrobo

Descripción de la conducta criminal: Los *bots* antirrobo pueden ser utilizados para realizar compras en línea de productos de alta demanda, como entradas para eventos y productos electrónicos, y luego revenderlos a precios inflados.

A.- Imputación objetiva de la conducta

Riesgo permitido: Los *bots* son una tecnología permitida y comúnmente utilizada en la actualidad, aunque su uso para comprar en línea y luego revender a precios inflados puede no ser un riesgo permitido debido a las implicaciones éticas y posibles repercusiones legales.

Disminución del riesgo: La disminución del riesgo en este caso podría involucrar la regulación de la actividad de los *bots* y la implementación de medidas para prevenir o limitar la capacidad de los *bots* para comprar productos de alta demanda.

Riesgo insignificante: La compra de productos de alta demanda por *bots* y su reventa a precios inflados no puede ser considerada un riesgo insignificante, ya que puede tener un impacto significativo en el acceso a esos productos para los consumidores.

Principio de confianza: Los *bots* que compran productos y los revenden a precios inflados violan el principio de confianza, ya que los consumidores confían en la igualdad de acceso a los productos y en la transparencia en el sistema de precios.

Prohibición de regreso: Si los *bots* compran productos y luego los revenden a precios inflados, han cruzado los límites de lo que es normalmente aceptable o permitido en el comercio electrónico.

Ámbito de responsabilidad de la víctima: En este caso, la víctima (los consumidores que no pueden acceder a los productos o que tienen que pagar precios inflados) no tiene control sobre las acciones de los *bots* y por lo tanto, no se les puede atribuir responsabilidad.

B. Imputación Objetiva de resultado

Relación de riesgo: Existe una relación directa entre el riesgo creado por los *bots* y el resultado de los precios inflados.

Nexos causales desviados: El uso de *bots* para comprar y revender productos puede llevar a un aumento de los precios, que es un resultado dañino.

Interrupción del nexo causal: No parece haber una interrupción en el nexo causal, ya que el uso de *bots* lleva directamente a los resultados perjudiciales.

4.2.1.2.3.3 Evadir la detección de inteligencia artificial

Descripción de la conducta criminal: Los delincuentes pueden utilizar técnicas de inteligencia artificial para evadir la detección de sistemas de seguridad y vigilancia, lo que dificulta la prevención y el enjuiciamiento de delitos.

A. Imputación objetiva de la conducta

Riesgo permitido: La utilización de técnicas de inteligencia artificial para evadir la detección de sistemas de seguridad no es un riesgo permitido socialmente, ya que se violan las normas establecidas para el buen uso de la tecnología y se compromete la seguridad de las personas y los sistemas.

Disminución del riesgo: No se puede determinar una disminución del riesgo aquí, ya que el uso de Inteligencia Artificial en este contexto aumenta el riesgo de delitos y vulnerabilidad de los sistemas de seguridad.

Riesgo insignificante: La utilización de técnicas de inteligencia artificial para evadir la detección de sistemas de seguridad no es insignificante; por el contrario, representa un riesgo significativo debido a su potencial para facilitar delitos.

Principio de confianza: Aquí se está violando el principio de confianza. Se espera que los usuarios de inteligencia artificial actúen de acuerdo con las normas y regulaciones establecidas, y no abusen de la tecnología para cometer delitos.

Prohibición de regreso: La conducta descrita puede implicar la explotación de vulnerabilidades preexistentes en los sistemas de inteligencia artificial de seguridad, que podrían haber sido neutralmente diseñadas, pero son utilizadas de manera delictiva.

Ámbito de responsabilidad de la víctima: En este caso, la "víctima" podría ser el sistema de inteligencia artificial que se utiliza para seguridad. Su responsabilidad en el delito sería mínima, ya que su diseño y operación se lleva a cabo con fines legítimos, y su explotación es responsabilidad del delincuente.

B. Imputación objetiva de resultado

Relación de riesgo: Hay una relación directa entre la acción del delincuente (utilizar técnicas de inteligencia artificial para evadir la detección) y el resultado (la prevención exitosa de la detección).

Nexos causales desviados: El uso de inteligencia artificial en este contexto es decisivo para lograr el resultado final, es decir, evadir la detección.

Interrupción del nexo causal: No hay evidencia de una interrupción del nexo causal. La utilización de técnicas de inteligencia artificial con fines delictivos es una acción continuada que lleva a la consecuencia de evadir la detección.

4.2.1.2.3.5 Reseñas falsas creadas por inteligencia artificial

Descripción de la conducta criminal: La inteligencia artificial puede ser utilizada para generar reseñas falsas de productos y servicios en línea, lo que afecta la confianza del consumidor y distorsiona el proceso de toma de decisiones.

A. Imputación objetiva de la conducta:

Riesgo permitido: La generación de reseñas falsas utilizando inteligencia artificial no es un riesgo permitido. Esta conducta viola las normas éticas y legales al proporcionar información engañosa a los consumidores, manipulando así su comportamiento de compra.

Disminución del riesgo: El uso de la inteligencia artificial para crear reseñas falsas aumenta el riesgo de desinformación y de manipulación del comportamiento del consumidor, en lugar de disminuir cualquier riesgo.

Riesgo insignificante: El uso de inteligencia artificial para crear reseñas falsas es un riesgo significativo para los consumidores, las empresas y el mercado, dado que puede manipular las decisiones de compra y socavar la confianza en los sistemas de reseñas.

Principio de confianza: El uso de inteligencia artificial para este propósito viola el principio de confianza. Se espera que las reseñas y calificaciones sean honestas y auténticas para ayudar a los consumidores a tomar decisiones de compra informadas.

Prohibición de regreso: Esta conducta se puede considerar como un abuso del diseño neutro de la inteligencia artificial, la cual está diseñada para aprender y adaptarse a partir de los datos que se le proporcionan.

Ámbito de responsabilidad de la víctima: Las víctimas son principalmente los consumidores que confían en las reseñas para tomar decisiones de compra. La responsabilidad de las víctimas en este caso es mínima, ya que se espera que las reseñas sean genuinas.

B. Imputación objetiva de resultado

Relación de riesgo: Existe una relación de riesgo entre la acción de generar reseñas falsas utilizando inteligencia artificial y el resultado de confundir a los consumidores y alterar el comportamiento de compra.

Nexos causales desviados: En este caso, no hay desviación causal. El uso de inteligencia artificial para generar reseñas falsas lleva directamente al resultado de manipulación del comportamiento del consumidor.

Interrupción del nexo causal: No hay evidencia de una interrupción del nexo causal. El uso de inteligencia artificial para generar reseñas falsas es una acción continuada que lleva al resultado final.

4.2.1.2.3.5 Acecho asistido por inteligencia artificial

Descripción de la conducta criminal: El acecho asistido por inteligencia artificial implica el uso de tecnologías de inteligencia artificial para seguir, monitorear y acosar a las personas, lo que puede tener graves consecuencias en la privacidad y la seguridad personal.

A.- Imputación objetiva de la conducta

Riesgo permitido: En nuestra sociedad moderna, se permiten ciertos riesgos asociados con el uso de tecnologías, incluyendo la inteligencia artificial. Sin embargo, utilizar estas tecnologías para acosar y vigilar a individuos claramente excede el riesgo permitido y aceptable.

Disminución del riesgo: Aquel que utiliza la inteligencia artificial para acechar a una persona no está buscando disminuir el riesgo, sino todo lo contrario: está explotando la tecnología para aumentar el riesgo y el daño potencial al bien jurídico de la víctima, su privacidad.

Riesgo insignificante: En este caso, el riesgo no es insignificante. El uso de inteligencia artificial para acechar y acosar tiene un impacto significativo y perjudicial en la vida de la víctima.

Principio de confianza: Este principio se ve violado cuando se utiliza la inteligencia artificial para acechar. Se espera que los usuarios de tecnología respeten la privacidad y los derechos de los demás. Cuando esto no sucede, se rompe la confianza en la sociedad.

Prohibición de regreso: En el acecho asistido por inteligencia artificial, el autor inicial puede intentar alegar que el uso posterior de la tecnología por un tercero fue impredecible o ajeno a su control. Sin embargo, si el autor proporcionó o facilitó deliberadamente la tecnología con fines de acoso, no podría escudarse en esta prohibición.

Ámbito de responsabilidad de la víctima: La víctima no es responsable del acoso. En este caso, la víctima no ha contribuido a la creación del riesgo y, por lo tanto, no se puede atribuir responsabilidad a la víctima.

B. Imputación objetiva del resultado

Relación de riesgo: Existe una clara relación entre la acción (usar inteligencia artificial para acosar) y el resultado (violación de la privacidad y posible daño emocional).

Nexos causales desviados: No hay evidencia de desviación causal. El resultado es directamente atribuible a la acción del acosador.

Interrupción del nexo causal: No se percibe ninguna interrupción del nexo causal. A menos que un tercero intervenga para detener el acoso, el acoso y su impacto en la víctima continuarán.

4.2.1.2.3.6 Falsificación asistida por inteligencia artificial

Descripción de la conducta criminal: La inteligencia artificial puede utilizarse para crear falsificaciones más convincentes de documentos, obras de arte

y otros objetos, lo que puede tener implicaciones en la propiedad intelectual, la autenticidad y el comercio de bienes y servicios.

A.- Imputación objetiva de la conducta

Riesgo permitido: La utilización de la inteligencia artificial para la creación, aprendizaje y desarrollo de tecnología es un riesgo permitido y esperado en nuestra sociedad. Sin embargo, usarla para la falsificación de documentos u otros objetos supera este riesgo permitido.

Disminución del riesgo: La falsificación asistida por inteligencia artificial no disminuye el riesgo, sino que lo aumenta al facilitar actividades fraudulentas.

Riesgo insignificante: En este caso, el riesgo es considerable. Las falsificaciones pueden tener graves consecuencias legales y económicas para los individuos y las empresas.

Principio de confianza: El principio de confianza se viola cuando se utiliza la inteligencia artificial para la falsificación. Se espera que los usuarios de la tecnología respeten las leyes y las normas.

Prohibición de regreso: La prohibición de regreso se aplica cuando el autor del acto ilícito se desliga del resultado final argumentando que el uso que otros hagan de la tecnología no es su responsabilidad. En el caso de la falsificación, si la persona facilitó la tecnología sabiendo que se usaría con fines fraudulentos, esta defensa no sería válida.

Ámbito de responsabilidad de la víctima: La víctima de la falsificación no es responsable del acto criminal. No ha contribuido a la creación del riesgo y, por lo tanto, no se puede atribuir responsabilidad a la víctima.

B. Imputación objetiva del resultado

Relación de riesgo: Existe una clara relación entre la acción de utilizar inteligencia artificial para falsificar y el resultado de fraude o pérdida económica.

Nexos causales desviados: No hay evidencia de desviación causal. El resultado es directamente atribuible a la acción del falsificador.

Interrupción del nexo causal: No se percibe ninguna interrupción del nexo causal. A menos que un tercero intervenga para detener la falsificación, la actividad delictiva y su impacto continuarán.

4.2.2 Argumentaciones de orden normativo

El floreciente desarrollo y aplicación de la Inteligencia Artificial ha provocado cambios radicales en nuestra sociedad. Sin embargo, las legislaciones actuales, tanto nacionales como internacionales, se centran principalmente en los beneficios y avances de la inteligencia artificial, dejando en un segundo plano el análisis sobre la imputación objetiva en relación a los actos delictivos que puedan derivar de su uso.

A nivel nacional, como se refleja en el Proyecto de Ley 2775/2022 -CR, se promueve el uso de la inteligencia artificial para el desarrollo económico y social, poniendo especial énfasis en su carácter ético, sostenible y responsable. Este enfoque, aunque admirable, elude las cuestiones críticas sobre la atribución de responsabilidad legal en caso de comportamientos delictivos. La normatividad se inclina hacia el potencial de la inteligencia artificial para impulsar la eficiencia y la calidad de vida, sin abordar de manera exhaustiva las implicaciones legales de los delitos cometidos por sistemas autónomos.

En el escenario internacional, encontramos un enfoque similar. La Unión Europea ha desarrollado regulaciones en torno a la inteligencia artificial, enfatizando su legalidad, ética y robustez. No obstante, estas directrices parecen más preocupadas por proteger los datos personales y garantizar la fiabilidad de la inteligencia artificial que por abordar los problemas relacionados con la criminalidad y la atribución de responsabilidad.

La regulación de la inteligencia artificial necesita un equilibrio. Es imperativo que se promueva su uso beneficioso, pero también es crucial garantizar que existen mecanismos claros y equitativos para asignar responsabilidad en caso de delitos cometidos por inteligencia artificial. Esto implica abordar de manera directa y clara la imputación objetiva de los programadores, los usuarios y las inteligencias artificiales autónomas e independientes.

La normatividad debería ser un reflejo de las complejidades de la tecnología de la inteligencia artificial y de las diversas maneras en que se utiliza en la sociedad. Es necesario un marco legal que reconozca tanto las posibilidades positivas de la inteligencia artificial como las implicaciones legales de su mal uso. Es imprescindible que las legislaciones, tanto nacionales como internacionales, adopten un enfoque más equilibrado y profundo en lo que respecta a la regulación de la inteligencia artificial.

4.2.3 Argumentaciones en torno a los casos emblemáticos

La inteligencia artificial está adquiriendo cada vez mayor autonomía e independencia, generando dilemas éticos y legales en cuanto a su uso y regulación. A medida que se desarrolla la inteligencia artificial, su aplicación en varios campos ha demostrado el potencial tanto para beneficios transformadores como para riesgos

significativos. Los casos emblemáticos de ChatGPT y Midjourney IA ilustran este dilema de manera evidente.

ChatGPT, desarrollado por OpenAI, es un modelo generativo de texto que se basa en los patrones y la información aprendidos durante su entrenamiento. Aunque su capacidad para generar respuestas coherentes y contextualmente relevantes a preguntas y solicitudes es impresionante, también ha provocado dilemas significativos. Los problemas que rodean la originalidad y la autoría de la redacción científica, la utilización de datos privados o sensibles sin control y las implicaciones en la educación y el trabajo son ejemplos de cómo la inteligencia artificial puede tener efectos perjudiciales si no se regula adecuadamente.

En el caso de Midjourney IA, su capacidad para generar imágenes a partir de descripciones en lenguaje natural plantea interrogantes similares. La capacidad de producir representaciones fotorealistas detalladas, como la fotografía del Papa con vestimenta de cantante moderno, plantea preguntas sobre la autoría, la autenticidad y la representación de la realidad. Además, la generación de imágenes que retratan eventos que nunca ocurrieron, como el arresto de Donald Trump, abre un nuevo frente en el debate sobre las *'deepfakes'* y la desinformación.

Estos casos ilustran la necesidad urgente de un marco jurídico que aborde la responsabilidad objetiva en el uso de la inteligencia artificial. ¿Quién es responsable cuando un sistema de inteligencia artificial comete un acto que sería considerado delito si lo hubiera hecho un humano? ¿El programador? ¿El usuario? ¿O la propia inteligencia artificial? La creciente autonomía de la inteligencia artificial complica estas preguntas.

Los avances en inteligencia artificial están desafiando nuestras concepciones tradicionales de responsabilidad e imputación. En un mundo en el que la inteligencia artificial puede generar contenido original, manejar datos sensibles y potencialmente manipular la realidad percibida, necesitamos urgentemente leyes y normativas que definan y asignen responsabilidades de manera clara y justa.

A medida que la inteligencia artificial sigue evolucionando y adquiriendo mayor autonomía, es esencial que las legislaciones a nivel nacional e internacional sigan el ritmo de estos avances. Solo entonces podremos garantizar un uso de la inteligencia artificial que sea beneficioso y justo para todos.

Conclusiones

1.- Se ha determinado que los alcances de la teoría de la imputación objetiva en la autoría mediata del programador de inteligencia artificial para fines delictivos deviene en vacíos normativos frente la imputación objetiva del autor mediato programador y la inteligencia artificial, pues requiere enfoques de imputación objetiva especiales y paralelas para el programador o empresas responsables de la implementación de las inteligencias artificiales, otro tipo de imputación para la inteligencia artificial autónoma, así como también para el usuario que accede a esta tecnología.

2.- Se establece que las consecuencias jurídicas de los vacíos jurídicos en la imputación objetiva en la autoría mediata del programador de inteligencia artificial con fines delictivos, tales como la falta evaluación de los factores como la creación de riesgo provenientes de la la inteligencia artificial, pues aplicar la teoría de la imputación objetiva es desafiante dado que la "acción" y el "resultado" pueden ser ambiguos, y el principio de confianza se complica por la falta de intenciones en las máquinas, también se deslindar la responsabilidad entre programador, usuario y máquina es complejo, más aún con la creciente autonomía de las inteligencias artificiales. Se requiere un enfoque sofisticado que aborde la responsabilidad penal en este contexto, reflejando la influencia creciente de la inteligencia artificial en la sociedad y economía contemporáneas.

3.- Se ha establecido que se superará los vacíos normativos en la imputación objetiva de la autoría mediata del programador de inteligencia artificial con fines delictivos en el Perú, mediante la adaptación de la teoría precitada considerando la actuación humana y la autonomía de la inteligencia artificial detrás de la acción

delictiva, pues se debe establecer la concurrencias de modelos de imputación objetiva para cada el programador, usuario e inteligencia artificial, pues resulta importante tener en cuenta el peligro de la inteligencia artificial para potenciar las actividades delictivas, la capacidad de estas tecnología para emular decisiones humanas, la autonomía de las máquinas, el procesamiento del lenguaje y aprendizaje autónomo.

Recomendaciones

1.- Dada la complejidad que supone la aplicación de la teoría de la imputación objetiva en el contexto del programador de inteligencia artificial como autor mediato, se recomienda profundizar en la investigación sobre el desarrollo de un nuevo marco legal y ético para la inteligencia artificial. Este marco debería poder abordar los desafíos de la imputación objetiva, incluyendo la dificultad de determinar la acción y predecir los resultados, y la atribución de responsabilidad entre el programador, el usuario y la máquina.

2.- Tener en cuenta la propuesta de aplicación de la teoría de imputación objetiva para delitos cometidos con inteligencia artificial. En donde se recomienda a los operadores jurídicos que tengan en cuenta la siguiente propuesta para enfocar la imputación objetiva en supuestos de criminalidad por inteligencia artificial:

I.- Marco normativo híbrido para la inteligencia artificial (IA)

Considerando la naturaleza única de la IA, desarrollar un marco legal híbrido que reconozca tanto el potencial de autonomía como su uso e instrumento de criminalidad. Esto implicaría atribuir una "personalidad jurídica" limitada a la IA en determinados contextos, permitiendo la imputación directa de responsabilidad cuando la inteligencia artificial opere de forma autónoma y cause daño. En paralelo, el marco legal debería seguir permitiendo la imputación de responsabilidad a los humanos que utilicen la IA para cometer delitos, incluyendo programadores y usuarios.

II.- Adoptar una tríada de responsabilidad para delitos cometidos con IA

Siguiendo la propuesta de Morales (2021), la responsabilidad debería poder atribuirse al creador, al programador y al usuario de la IA. Esto requeriría

un análisis caso por caso, teniendo en cuenta factores como el control del programador sobre la IA, la previsibilidad de las acciones de la IA y la intención del programador.

III.- Establecer criterios de imputación objetiva para delitos cometidos con inteligencia artificial

Adaptar los principios de la teoría de la imputación objetiva para su aplicación en el contexto de la IA. Esto implicaría evaluar el riesgo permitido, la disminución del riesgo, el riesgo insignificante, el principio de confianza, la prohibición de regreso, el ámbito de responsabilidad de la víctima, la relación de riesgo, los nexos causales desviados y la interrupción del nexo causal. Estos criterios permitirían determinar si una acción u omisión con IA puede considerarse delictiva y si el resultado dañino puede atribuirse a la IA o al humano.

IV. Reforzar la regulación de la IA

Es necesario desarrollar regulaciones específicas que proporcionen directrices claras sobre la creación, programación y uso de la inteligencia artificial. Estas regulaciones deberían incluir requisitos de seguridad, estándares éticos y directrices sobre responsabilidad legal, y deberían ser reforzadas por leyes penales que penalizan el uso abusivo de la IA.

V.- Seguir investigando y debatiendo

Esta propuesta de teoría de imputación objetiva para delitos cometidos con IA intenta navegar el delicado equilibrio entre la protección de la sociedad, la promoción de la innovación y la justicia en la atribución de responsabilidad. Sin embargo, es necesario seguir investigando y debatiendo este tema para refinar aún

más estos principios y garantizar que nuestro marco legal esté a la altura de los desafíos que plantea la IA.

Tabla 1

Tabla de imputación objetiva en delitos cometidos con IA

Autoría e imputación	Inteligencia artificial como sujeto de derecho	Inteligencia artificial como instrumento de criminalidad
Autor directo: Programador o desarrollador	Se concede a la inteligencia artificial "personalidad jurídica", responsabilidad legal directa por sus propias acciones.	La inteligencia artificial es un mero instrumento utilizado por el programador para cometer un delito.
Autor mediato: Programador o desarrollador	Se otorga a la inteligencia artificial la capacidad de tomar decisiones autónomas, convirtiéndola en un sujeto legalmente responsable.	La inteligencia artificial se convierte en el medio a través del cual el programador ejecuta un delito
Coautoría: Usuario de Inteligencia de Artificial y programador	Se reconoce a la inteligencia artificial y al usuario como coautores, compartiendo responsabilidad.	El usuario se convierte en coautor al utilizar la inteligencia artificial diseñada por el programador para cometer un delito.
Responsabilidad indirecta: Programador negligente	Se responsabiliza al programador por crear una inteligencia artificial capaz de actuar de manera autónoma y cometer delitos	El programador se considera responsable si no tomó las medidas necesarias para prevenir el uso abusivo de la inteligencia artificial.
Autoría mediata y material: Programador, usuario e inteligencia artificial	La inteligencia artificial adquiere autonomía e independencia, se reconoce su capacidad para actuar de manera autónoma y se imputa responsabilidad.	El usuario utiliza la inteligencia artificial para cometer un delito y el programador no tomó las medidas adecuadas para prevenir tal uso.

Referencias bibliográficas

Aboso, G. (2017). *Limites de la Autoría Mediata*. B de F Editores.

Abreu, J. (2015). Análisis al Método de la Investigación. In *Daena: International Journal of Good Conscience* (Vol. 10, Issue 1). http://www.spentamexico.org/v10-n1/A14.10(1)205-214.pdf

Acosta, S. (2023). Los paradigmas de investigación en las Ciencias Sociales. In *Calidad de la educación superior: gestión estratégica, formación integral y soporte institucional* (pp. 60–79). Instituto de Investigación y Capacitación Profesional del Pacífico. https://doi.org/10.53595/eip.007.2023.ch.4

Alcocer, N. (2015). Teoría de la imputación objetiva en la jurisprudencia peruana.: Desarrollo jurisprudencial a partir del año 2011. *Derecho y Cambio Social*, *ISSN-e 2224-4131*, *Año 12*, *Nº. 42*, *2015*, *12*(42), 12. https://dialnet.unirioja.es/servlet/articulo?codigo=5456411

Aldana, G. (2007). Diseño de proyectos en la investigación Cualitativa. *Teoría y Praxis Investigativa*, *2*(2), 78–79. https://books.google.es/books?hl=es&lr=&id=Xkb78OSRMI8C&oi=fnd&pg=PA11&dq=Galeano,+M.+(2004).+Diseño+de+proyectos+en+la+investigación+cualitativa.+Medellin,+Colombia:+Fondo+Editorial+Universidad+EAFIT.+&ots=zsFudQSEqL&sig=ZFzwSc-Jvg1IsmETULKwO32K0Bs#v=one

Allué, A. (2017). *En torno a la teoría de la imputación objetiva del resultado en la dogmática penal*. Ficp.Es. https://ficp.es/wp-content/uploads/2019/03/Allué-Fuentes.-Comunicación.pdf

Amigone, F., Kogan, P., Michelan, G., & Rodríguez, J. (2018). Edimbrujo: Definiendo un modelo didáctico para la enseñanza de la Inteligencia Artificial en Juegos. *Revista Digital de Investigación En Docencia Universitaria (RIDU)*, *May*, 10. http://sedici.unlp.edu.ar/handle/10915/68912

Arenas, O. (2017). La comunicabilidad de las circunstancias del autor al partícipe en el Derecho penal panameño y alemán. *CENTROS*, *6*(2), 173–186. https://revistas.up.ac.pa/index.php/centros/article/view/14

Arráez, M., Calles, J., & Moreno de Tovar, L. (2006). La Hermenéutica: una actividad interpretativa. *SAPIENS*, *7*(2), 171–181.

http://ve.scielo.org/scielo.php?script=sci_arttext&pid=S1317-58152006000200012

Avila, D., & Torres, J. (2021). *Modelo de detección de intrusos para detectar y evitar la inserción de Malware en una red, basado en técnicas de aprendizaje automático.* [Universidad de Guayaquil]. http://repositorio.ug.edu.ec/handle/redug/52736

Ayasta, W. (2021). *Impacto de la inteligencia artificial en la gestión de las empresas distribuidoras de energía del Grupo Distriluz* [PE]. http://repositorio.unac.edu.pe/handle/20.500.12952/5737

Balcázar-Nava, P., González-Arratia, N., López-Fuentes, I., Gurrola-Peña, G., & Moysén-Chimal, A. (2013). Investigación cualitativa. *Ministerio de Educación*. https://repositorio.minedu.gob.pe/handle/20.500.12799/4641

Barrios, H., Diaz, V., & Guerra, Y. (2020). Subjetividades e inteligencia artificial: desafíos para 'lo humano.' *Veritas*, *47*(47), 81–107. https://doi.org/10.4067/S0718-92732020000300081

Bibiana, N., Cardozo, J., & Mejía, S. (2023). Posturas del paradigma socio-crítico como aportes a la educación y gestión educativa en Colombia. *Revista Dialogus*, *10*(6), 119–133. https://doi.org/10.37594/DIALOGUS.V1I10.678

Borromeo, N., Muller, M., Pardo, F., Pérez Badón, L., Grillo, I., & Gonzales, G. (2019). *Aplicación de técnicas de inteligencia artificial de videojuegos en nuevos contextos*. http://sedici.unlp.edu.ar/handle/10915/88677

Bustamante, S., Castillo, H., & Gómez, J. (2020). *Diseño de una aplicación móvil de apoyo a la solución de juegos de lógica basada en procesamiento de imágenes e inteligencia artificial*. https://doi.org/10.2/JQUERY.MIN.JS

Cabrera-Ramírez, S., & Cepeda-Retana, J. (2022). La epistemología, guía para el conocimiento científico. *Portal de La Ciencia*, *3*(2), 123–133. https://doi.org/10.51247/pdlc.v3i2.317

Caceres, E. (2023). La inteligencia artificial aplicada al derecho como una nueva rama de la teoría jurídica. *Inteligencia Artificial y Derecho*, *57*(31/01&2023), 63–89. https://revistaseug.ugr.es/index.php/acfs/article/view/26281

Cancio, M. (2020). La teoría de la imputación objetiva, Claus Roxin y América Latina. *Revista Criminalia Nueva Época*, *86*(1).

https://www.criminalia.com.mx/index.php/nueva-epoca/article/view/23

Carretero, J. (2018). *La aplicación de la imputación objetiva para accidentes de tránsito, en el distrito judicial de Lima y Lima Este, año 2015* [Universidad Nacional Federico Villarreal]. https://repositorio.unfv.edu.pe/handle/UNFV/2154

Coca, I. (2019). La business judgment rule ante la determinación del riesgo permitido en el delito de administración desleal. *Revista Do Instituto de Ciências Penais*, *4*(1), 83–115. https://doi.org/10.46274/1809-192xricp2019v4p83-115

Coloma, J., Vargas, J., Sanaguano, C., & Rochina, A. (2020). Inteligencia artificial, sistemas inteligentes, agentes inteligentes. *RECIMUNDO: Revista Científica de La Investigación y El Conocimiento, ISSN-e 2588-073X, Vol. 4, Nº. 2, 2020, Págs. 16-30*, *4*(2), 16–30. https://doi.org/10.26820/recimundo/4.(2).mayo.2020.16-30

Comisión Europea. (2019). *DIRECTRICES ÉTICAS para una IA FIABLE. Grupo de expertos de alto nivel sobre inteligencia artificial*. Oficina de Publicaciones. https://data.europa.eu/doi/10.2759/14078

Contreras, L. (2019). Tratamiento penal de los casos de concurrencia de riesgos en el tráfico rodado a través de la teoría de la imputación objetiva del resultado. *Revista de Estudios de La Justicia*, *30*, 95–110. https://doi.org/10.5354/0718-4735.2019.53779

Corcino, F. (2017). *Autoría mediata en aparatos organizados de poder. Fundamentos dogmáticos y consecuencias prácticas*. https://idus.us.es/handle/11441/74634

Deroncele-Acosta, A. (2020). Paradigmas de investigación científica. Abordaje desde la competencia epistémica del investigador. *Arrancada*, *20*(37), 211–225. https://revistarrancada.cujae.edu.cu/index.php/arrancada/article/view/331

Diaz, D. (2023). Inteligencia artificial vs.Turnitin: implicaciones para el plagio académico. *Revista Cognosis*, *8*(1), 15–26. https://doi.org/10.33936/COGNOSIS.V8I1.5517

Doubront, L., Doubront, M., & Gómez, A. (2021). Abordaje epistemológico en la

investigación educativa para la producción de teorías. *Correspondencias & Análisis*, *13*, 127–152. https://doi.org/10.24265/cian.2021.n13.05

Escuela, C. (2019). Síntesis social y abstracción idealista. Tentativas materialistas sobre la filosofía del idealismo. *Anales Del Seminario de Historia de La Filosofía*, *36*(2), 517–536. https://doi.org/10.5209/ashf.58636

Faliero, J. (2021). Limitar la dependencia algorítmica. Impactos de la inteligencia artificial y sesgos algorítmicos. *Nueva Sociedad*, *294*, 120–129. https://www.proquest.com/docview/2569414432/125EADB67FA343E4PQ/1?accountid=14747

Gadea, W., Cuenca, R., & Chaves, A. (2019). *Epistemología y Fundamentos de la Investigación Científica*. CENGAGE. http://rabida.uhu.es/dspace/handle/10272/18574#.ZGuny3fF0KI.mendeley

García, S. (2019). Ética e inteligencia artificial. *Cuadernos de La Cátedra CaixaBank de Responsabilidad Social Corporativa*, *42*(Setiembre). https://doi.org/10.15581/018.ST-522

Garrido, J. (2022). Inteligencia artificial y automatismo. Anatomía de un conflicto. In *Inteligencia Artificial y filosofia del derecho* (pp. 169–187). Laborum. https://idus.us.es/handle/11441/137258

Gimbernat, E. (2020). En defensa de teoría de la imputación objetiva contra sus detractores y, también, contra algunos de sus partidarios. *Anuario de Derecho Penal y Ciencias Penales, ISSN 0210-3001, Tomo 73, Fasc/Mes 1, 2020, Págs. 9-20*, *73*(1), 9–20. https://dialnet.unirioja.es/servlet/articulo?codigo=7655321&info=resumen&idioma=SPA

Gonzales, E. (2018). Paradigmas en Investigación: Una mirada desde lo planos del conocimiento. *Jornadas de Investigación: Universidad, Investigación y Sociedad En Un Estado de Nuevo Signo. Memorias Arbitradas.*, 39–46. Ediciones Uney

Guevara, G., Verdesoto, A., & Castro, N. (2020). Metodologías de investigación educativa (descriptivas, experimentales, participativas, y de investigación-acción). *RECIMUNDO*, *4*(3), 163–173. https://doi.org/10.26820/recimundo/4.(3).julio.2020.163-173

Hallevy, G. (2019). The Basic Models of Criminal Liability of AI Systems and Outer Circles. *SSRN Electronic Journal*. https://doi.org/10.2139/SSRN.3402527

Hashimoto, E. (2010). *Cómo elaborar proyectos de investigación desde los tres paradigmas de la ciencia.* Oficina de Investigación de la Universidad Nacional de Cajamarca.

Hernández, M. (2019). Inteligencia artificial y derecho penal. *Actualidad Jurídica Iberoamericana*, *2*(10), 792–843. https://dialnet.unirioja.es/servlet/articulo?codigo=6978830&info=resumen&idioma=ENG

Kaufmann, A. (2020). ¿«Atribución objetiva» en el delito doloso? *Revista Peruana de Ciencias Penales*, *34*, 287–308. https://rpcp.pe/index.php/RPCP/article/view/14

Leal, N. (2012). *El Método Fenomenológico: Principios, Momentos Y Reducciones*. *1977*, 52–60. http://revistadip.una.edu.ve/volumen1/epistemologia1/lealnestorepistemologia.pdf

Leyva, M., Escobar, R., Espín, C., & Pérez, K. (2018). Facebook como herramienta para el aprendizaje colaborativo de la inteligencia artificial. *Didasc@lia: Didáctica y Educación*, *9*(1), 27–36. http://revistas.ult.edu.cu/index.php/didascalia/article/view/728

Lopera, J. (2010). *El método analítico como método natural*. *1*. http://bibliotecadigital.udea.edu.co/handle/10495/5501

Loza, R., Mamaní, J., Mariaca, J., & Yanqui, F. (2020). Paradigma sociocrítico en investigación. *PSIQUEMAG/ Revista Científica Digital de Psicología*, *9*(2), 30–39. https://doi.org/10.18050/PSIQUEMAG.V9I2.2656

Marín, J. (2018). El uso de drones comerciales como vectores terroristas. *Ieee*, *02/2018*(Documento Marco), 1–35. https://dialnet.unirioja.es/servlet/articulo?codigo=6467970

Marquisio, R. (2015). Tres modelos de postpositivismo jurídico. *Anales de La Facultad de Ciencias Juridicas y Sociales de La Universidad Nacional de La Plata*, *47*. https://revistas.unlp.edu.ar/RevistaAnalesJursoc/article/view/4277

Martín, E. (2017). Usos hostiles de sistemas roboticos y autonomos por actores no estatales. *Cuaderno de La Guardia Civil*, *55*, 65–84. https://intranet.bibliotecasgc.bage.es/intranet-tmpl/prog/local_repository/documents/documents/20114_21356.pdf#page=85

Martinez, F. (2007). *El método inductivo*. http://eprints.uanl.mx/5599/1/1080071376.PDF

Mendez, C., Gonzales, J., El Fakih, F., & Lucero, V. (2022). Epistemología jurídica desde la perspectiva del constructivismo jurídico complejo de Enrique Cáceres. *Revista Conrado*, *18*(S3), 265-274. https://conrado.ucf.edu.cu/index.php/conrado/article/view/2660

Merino, L. (2023). Epistemologia, Naturaleza, Fundamentos de la Investigación Cientifica. *Revista Cientifica Emprendimiento Científico Tecnologico*, *5*. https://revista.ectperu.org.pe/index.php/ect/article/download/125/131

Meza, C. (2020). *Los criterios de imputación objetiva de resultado del derecho penal aplicados a la responsabilidad extracontractual de la administración colombiana, al margen del acto terrorista* [Universidad Libre de Bogotá]. https://repository.unilibre.edu.co/bitstream/handle/10901/19315/TESIS DOCTORAL - CESAR HERNANDO MEZA MERCADO - CORRECCIONES SUSTENTACION 31-10-2020.pdf?sequence=1&isAllowed=y

Morales, Á. (2021). Inteligencia artificial y derecho penal: primeras aproximaciones. *Revista Jurídica de Castilla y León*, *53*, 177–202. https://dialnet.unirioja.es/servlet/articulo?codigo=7788274&info=resumen&idioma=ENG

Morales, F. (2023). ¿Qué tan irrelevantes son las tesis definitorias del positivismo jurídico? *Doxa. Cuadernos de Filosofía Del Derecho*, *46*, 321–334. https://doi.org/10.14198/DOXA2023.46.18

Muñoz, C. (2023). ¿ChatGPT en la universidad? ¿Complementar el aprendizaje y cambiar el modelo educativo? *Diario La Ley, ISSN 1989-6913, Nº 10283, 2023*, *10283*, 3. https://dialnet.unirioja.es/servlet/articulo?codigo=8934531&info=resumen&i

dioma=SPA

Navas, S. (2017). Derecho e inteligencia artificial desde el diseño. Aproximaciones. In Tirant lo Blanch (Ed.), *Inteligencia artificial, Tecnología Derecho* (pp. 23–71).

Padrón, J. (2007). Tendencias epistemológicas de la investigación científica en el siglo XXI. *Cinta de Moebio*, *28*, 1–28. https://www.redalyc.org/articulo.oa?id=10102801

Panisello, J. (2022). Causalidad e imputación de responsabilidad. *CEFLegal. Revista Práctica de Derecho*, *256*, 35–58. https://doi.org/10.51302/CEFLEGAL.2022.9199

Paoli, F. (2019). Multi, inter y transdisciplinariedad. *Problema Anuario de Filosofía y Teoría Del Derecho*, *13*(13), 347–357. https://doi.org/10.22201/IIJ.24487937E.2019.13

Paz-López, M. (2018). *Riesgo permitido y responsabilidad penal*. Disciplinas Jurídicas Básicas. https://riull.ull.es/xmlui/handle/915/9549

Pineda, X. (2017). *La autoría mediata como forma de participación reconocida en la legislación penal ecuatoriana*. http://repositorio.utmachala.edu.ec/handle/48000/10343

Ramirez, A. (2014). *El Diseño de investigación en ciencias sociales*. https://doi.org/10.13140/RG.2.2.28918.19521

Ramos, E. (2023, March 23). *Estas fotos de Donald Trump "siendo arrestado" no son reales: fueron hechas con inteligencia artificial*. La República. https://larepublica.pe/verificador/2023/03/23/estas-fotos-de-donald-trump-siendo-arrestado-no-son-reales-fueron-hechas-con-inteligencia-artificial-246238

Reyes, O., & Bringas, J. (2006). *La Modelación Teórica como método de la investigación científica*.

Rodas, A. (2021). *Diseño e implementación de un sistema de generación de trayectoria para el control de un robot móvil, utilizando inteligencia artificial*. Universidad del Azuay. http://dspace.uazuay.edu.ec/handle/datos/11228

Rodríguez, J. (2022). Filosofía y modelos de humanidad. Algunas concepciones predominantes. *Eikasía Revista de Filosofía*, *108*, 77–100.

https://doi.org/10.57027/eikasia.108.313

Rodríguez, T. (2022). *Estado del arte sobre el paradigma sociocrítico en la educación* [Pontificia Universidad Católica del Perú]. https://tesis.pucp.edu.pe/repositorio/handle/20.500.12404/23323

Romeo, C. (2018). Riesgo, procedimientos actuariales basados en inteligencia artificial y medidas de seguridad. *Revista de Derecho, Empresa y Sociedad*, *13*, 39–55. https://dialnet.unirioja.es/descarga/articulo/6859383.pdf

Rondo, G. (2020). Inteligencia Artificial en la Seguridad de TI. *Revista PGI. Investigación, Ciencia y Tecnología En Informática*, *8*, 99–101. https://ojs.umsa.bo/ojs/index.php/inf_fcpn_pgi/article/view/59

Rouhiainen, L. (2018). Inteligencia Artificial. In Planeta (Ed.), *Inteligencia Artificial*. https://static0planetadelibroscom.cdnstatics.com/libros_contenido_extra/40/39308_Inteligencia_artificial.pdf

Rusell, S., & Norvig, P. (2016). Inteligencia Artificial. Un Enfoque Moderno. In *Inteligencia Artificial*.

Salamanca, A. (2015). La investigación jurídica e intercultural e interdisciplinar: Metodología, epistemología, gnoseología y ontología. *Revista de Derechos Humanos y Estudios Sociales*, 59–92. https://docplayer.es/90027079-La-investigacion-juridica-intercultural-e-interdisciplinar-1-metodologia-epistemologia-gnoseologia-y-ontologia-antonio-salamanca-serrano-2.html

Sánchez, M. (2011). *La Metodología en la Investigación Jurídica : Características peculiares y Pautas Generales*. 317–358. http://www.nunezdearco.net/PDF/Metodo cientifico invest derecho SANCHEZ_1.pdf

Sempere, J., & Arenas, M. (2023). Garante Italiano ordena suspender el tratamiento de datos personales realizado por dos aplicaciones (Replika y ChatGPT) de Inteligencia Artificial. *La Ley Privacidad, ISSN-e 2659-8698, Nº. 15, 2023 (Ejemplar Dedicado a: Enero-Marzo)*, *15*, 16. https://dialnet.unirioja.es/servlet/articulo?codigo=8921520&info=resumen&idioma=SPA

Solís, R. (2019). Modelo inteligente cognitivo basado en métodos de inteligencia

artificial para el desarrollo de aplicaciones móviles [Universidad Nacional Federico Villarreal]. In *Universidad Nacional Federico Villarreal*. http://repositorio.unfv.edu.pe/handle/UNFV/3729#.Yb9nuJUPHtw.mendeley

Suárez, P. (2020). *Gobernanza, inteligencia artificial y justicia predictiva: Los retos de la administración de justicia ante la sociedad en red* [Universidad de Málaga]. https://dialnet.unirioja.es/servlet/tesis?codigo=286995&info=resumen&idioma=SPA

Tantaleán, R. (2015). El alcance de las investigaciones jurídicas. *Derecho y Cambio Social*, 22. http://www.revistas.upagu.edu.pe/index.php/AV/article/view/133

Terrones, A. (2021). *Inteligencia artificial responsable. Humanismo tecnológico y ciencia cívica* [Universitat de València]. https://dialnet.unirioja.es/servlet/tesis?codigo=286366&info=resumen&idioma=SPA

Túñez-López, J., Toural-Bran, C., & Cacheiro-Requeijo, S. (2018). Uso de bots y algoritmos para automatizar la redacción de noticias: percepción y actitudes de los periodistas en España. *Profesional de La Información*, *27*(4), 750–758. https://doi.org/10.3145/EPI.2018.JUL.04

Vallejo-Jiménez, G. (2017). La valoración jurídica del riesgo como criterio para la determinación de la responsabilidad penal del médico. *Revista Colombiana de Anestesiologia*, *45*, 58–63. https://doi.org/10.1016/j.rca.2017.08.003

Villavicencio, F. (2007). La imputación objetiva en la jurisprudencia peruana. *Derecho PUCP: Revista de La Facultad de Derecho*, 253–279. https://dialnet.unirioja.es/ejemplar/397579

Villota, O. (2019). Cómo la inteligencia artificial altera el paisaje de las seguridades. *Revista Conjeturas Sociológicas*, *19*(7 (Mayo-Agosto)), 157–198. https://revistas.ues.edu.sv/index.php/conjsociologicas/article/view/1492

Zavia, M. (2023, March 28). *La foto viral del abrigo del papa es fruto de la IA y las drogas*. GiZMODO - Tecnología, Ciencia y Cultura Digital. https://es.gizmodo.com/foto-viral-papa-abrigo-inflado-drogas-ia-midjourney-1850276597

Zornoza, A. (2020). *Vehículos automatizados y Derecho. La influencia de la*

conducción automatizada en la responsabilidad civil automovilística y en el seguro obligatorio de automóviles [Universidad Carlos III de Madrid - España]. https://e-archivo.uc3m.es/handle/10016/31089

Anexos

1.- Matriz de consistencia lógica

2.- Tabla aplicativa del método dogmático-jurídico

1.- Matriz de consistencia lógica

TÍTULO: Imputación objetiva y autoría mediata del programador de inteligencia artificial para fines delictivos en el Perú

PROBLEMAS	OBJETIVOS	HIPÓTESIS	CATEGORÍAS Y SUB-CATEGORÍAS	MARCO TEORICO	METODOLOGÍA
General	**General**	**General**	**CATEGORÍAS DE LA HIPÓTESIS**	**SUMARIO**	Este estudio utiliza un enfoque cualitativo y descriptivo, siguiendo una investigación jurídico-filosófica para explorar la teoría de la imputación jurídica y los alcances de la inteligencia artificial. El diseño es no experimental y transversal, siendo flexible debido a su naturaleza cualitativa. Los métodos de investigación incluyen deductivo, inductivo, analítico, entre otros. En el ámbito jurídico se utilizan métodos jurídico-dogmático, jurídico-social y de argumentación jurídica. La muestra consiste en la doctrina, jurisprudencia y normatividad internacional sobre imputación objetiva e inteligencia artificial aplicable al Perú. Las técnicas de recolección de datos son documentales y entrevistas, para luego ser procesados e interpretados a través de revisión, organización, preparación, definición de unidad de
¿Cuáles son los alcances de la imputación objetiva de la autoría mediata del programador de inteligencia artificial con fines delictivos en el Perú?	Determinar los alcances de la imputación objetiva de la autoría mediata del programador de inteligencia artificial con fines delictivos en el Perú.	Los alcances de la imputación objetiva de la autoría mediata de programador de inteligencia artificial con fines delictivos en el Perú, devienen en vacíos jurídicos para establecer la imputación objetiva del autor mediato programador y la inteligencia artificial como ejecutor material del hecho delictivo.	**Categoría Independiente (1)** • Imputación Objetiva *Dimensión: Tipos* **Sub-categorías** • Imputación objetiva de la Conducta • Imputación objetiva del resultado **Categoría Independiente (2)** • Autoría penal *Dimensión: Tipos* **Sub-Categorías** • Autoría directa • Autoría mediata. • Coautoría. **Categoría independiente** • Inteligencia artificial *Dimensión: Enfoque.* **Sub-Categorías** • Comportamiento humano: Enfoque de la prueba de Turing. • Pensar como humanos: El enfoque del modelo cognitivo. • El pensamiento racional: El enfoque de las leyes del pensamiento. • Actuar en forma racional: El enfoque del agente racional *Dimensión: Aplicaciones* **Indicadores**	I.- Imputación Objetiva II.- Autoría penal III.- Inteligencia Artificial	

			• Planificación autónoma • Juegos • Control autónomo • Diagnosis • Planificación logística • Robótica • Procesamiento de lenguaje y resolución de problemas. *Dimensión: Criminalidad* **Indicadores** Nivel Alto • Suplantación de la identidad en audio y video • Vehículos sin conductor como armas • Phishing personalizado. • Interrumpir los sistemas controlados por IA • Noticias falsas creadas por IA Nivel Medio • Robots militares • Aceite de serpiente • Ciberataques basados en el aprendizaje. • Drones de ataque autónomo • Engañar al reconocimiento facial • Bombardeo de mercado Nivel Bajo • Explotación de sesgos • Bots antirrobo • Evadir la detección de IA • Reseñas falsas creadas por IA • Asecho asistido por IA • Falsificación		análisis y codificación.
Específico 1	**Específico 1**	**Específico 1**			

¿Cuáles son las consecuencias jurídicas de los vacíos normativos en la imputación objetiva de la autoría mediata del programador de inteligencia artificial con fines delictivos en el Perú?	Establecer las consecuencias jurídicas de los vacíos normativos en la imputación objetiva de la autoría mediata del programador de inteligencia artificial con fines delictivos en el Perú.	Las consecuencias jurídicas de los vacíos jurídicos en la imputación objetiva de la autoría mediata del programador de inteligencia artificial con fines delictivos en el Perú, es la falta imputación de acción y resultado la impunidad pese a la puesta en peligro o daños de bienes jurídicos.			
Específico 2	**Específico 2**	**Específico 2**			
¿Cómo se superará los vacios normativos en la imputación objetiva de la autoría mediata del programador de inteligencia artificial con fines delictivos en el Perú?	Exponer cómo se superará los vacíos normativos en la imputación objetiva de la autoría mediata del programador de inteligencia artificial con fines delictivos en el Perú.	Se superará los vacíos normativos en la imputación objetiva de la autoría mediata del programador de inteligencia artificial con fines delictivos en el Perú, mediante la adaptación de la imputación objetiva a los supuestos criminalidad mediante inteligencia artificial.			

2.- Tabla aplicativa del método jurídico-dogmático

Etapa	Descripción	Aplicación a la tesis doctoral
Elección y delimitación del tema	Esta etapa consiste en seleccionar y precisar el objeto de estudio de la tesis.	Título de la tesis: Teoría de la imputación objetiva y autoría mediata del programador de inteligencia artificial para fines delictivos en el Perú.
Fundamentación filosófica y epistemológica	Esta etapa implica establecer las bases filosóficas y epistemológicas que soportarán la tesis.	La tesis se filosóficamente en el paradigma sociocrítico, en la filosofía del derecho en el pospositivismo. La tesis se fundamenta epistemológicamente en el cuestionamiento de la ciencia del derecho como cocimiento científico, mientras desde la epistemología del derecho desde la complejidad e interdisciplinariedad.
Marco teórico y conceptual	Esta etapa involucra la recopilación y síntesis de las teorías y conceptos relevantes para el estudio.	Se presenta la teoría de la imputación jurídica, la autoría penal y la actualidad de la inteligencia artificial.
Estudio de la normativa y la jurisprudencia	Esta etapa implica un estudio detallado de las leyes, regulaciones y jurisprudencia relacionadas con el tema.	Se ha procurado ubicar normatividad y jurisprudencia sobre inteligencia artificial
Metodología de la investigación	En esta etapa se describirá y justificará el método de investigación que se utilizará.	No solo se utiliza la metodología jurídica-dogmática, sino diversos métodos generales y específicos del derecho
Argumentación y crítica	En esta etapa se elaborarán argumentos basados en el análisis del marco normativo y jurisprudencial y se realizarán críticas constructivas.	En los argumentos y puntos críticos podemos encontrar el problema de la imputación objetiva cuando se comete delitos con inteligencia artificial y así como la posibilidad de la asignación de personería jurídica especial a la inteligencia artificial para asignar autoría penal o instrumentalización.
Conclusión y propuestas	Esta etapa consiste en resumir los hallazgos de la investigación y proponer mejoras o nuevas ideas.	La adaptación de la imputación objetiva para delitos con inteligencia artificial conlleva a modelos que contemplan al desarrollador, usuario y la inteligencia artificial autónomo e independiente, con capacidad de decisión.