AUTOPUESTA EN PELIGRO DEL USUARIO CON CHATBOTS INTELIGENTES:

Estándares de la auto puesta en peligro del usuario por la interacción con los prototipos de aprendizaje Autónomo: Chatsbots Inteligentes

Leonardo André Areniz Martínez

Trabajo de grado para optar el título de Magister en Derecho

Director

Carlos Daniel Arias Lozano

Magister en derecho

Universidad Santo Tomás, Bucaramanga

División de Ciencias Humanas

Maestría en Derecho

2024

Agradecimientos

Quiero dedicar esta investigación al tiempo robado a mi familia, especialmente a mi esposa Yesenia Castro Quintero y mis hijos, María Paula Areniz, Ana María Areniz y Andrés Julián Areniz. Espero que este esfuerzo y dedicación sirva de ejemplo en su formación y les inspire a perseguir sus propios sueños con la misma determinación.

Reconozco la ayuda invaluable de mi director, cuyo apoyo y guía fueron fundamentales para la realización de este trabajo. También me gustaría expresar mi agradecimiento a los profesores de la maestría, que con sus conocimientos y orientaciones participaron decisivamente en la realización de la investigación. Sus enseñanzas y consejos además de aportar en lo que esta cuyo trabajo significa, también ayudaron a ampliar mi visión académica y profesional.

AUTOPUESTA EN PELIGRO DEL USUARIO CON CHATBOTS INTELIGENTES:

Contenido

Introducción **9**

1. Estándares de la auto puesta en peligro del usuario por la interacción con los prototipos de aprendizaje autónomo: ChatsBots inteligentes **11**

1.1 Planteamiento del Problema 11

1.2 Justificación 14

1.3 Objetivos 17

1.3.1 Objetivo General *17*

1.3.2 Objetivos Específicos *18*

2. Marco Referencial 18

2.1 Marco Teórico 18

2.2 Marco Conceptual de Inteligencia Artificial. 28

2.3 Estado del Arte 30

2.4 Metodología 36

4. Análisis de los Usos, Interacciones y Riesgos entre el usuario y el ChatBot Inteligente 38

4.1 Prototipo ChatBot Cognitivo y sus Usos 38

4.2 Prototipo ChatBot Cognitivo y sus Riesgos. 39

4.3 Problemas estructurales de judicialización a los riesgos creados 45

5. Avances en Legislación Nacional e Internacional sobre Regulación de IA 47

5.1 Marco regulatorio en la Unión Europea 48

5.2 Marco Regulatorio en Estados Unidos 50

5.3 Marco Regulatorio de Otros Países..... 53

5.4 Marco regulatorio en la Convención Americana 56

5.5 Avances en la Regulación Nacional 56

5.6 Estándares Internacionales en la Regulación de la Inteligencia Artificial. 58

6. Atribución de Responsabilidad Penal en Interacciones Usuario-Bot 61

6.1 Sociedad de la información. 63

6.2 Conceptualización del ciberdelito 66

6.3 Desafíos en el ciberespacio. 69

6.4 Riesgos y desafíos de la Inteligencia Artificial: necesidad de regulación. 70

6.5 Generalidades de una dogmática para judicializar ChatBot inteligentes. 78

6.6 Implicaciones jurídicas de la IA en la protección del dato y la información. 82

6.7 ChatBot Inteligente y Riesgos jurídicamente desaprobados 88

6.8 Atribución de responsabilidad penal: Teoría del dominio del hecho 92

6.9 Imputación objetiva en el marco del tipo objetivo de la conducta punible. 98

6.10 Actuar bajo el propio riesgo 104

6.11 Teoría Propuesta 109

7. Conclusiones 115

Referencias 119

AUTOPUESTA EN PELIGRO DEL USUARIO CON CHATBOTS INTELIGENTES:

Resumen

El propósito de este estudio es analizar los estándares de responsabilidad personal de los usuarios al interactuar con chatbots inteligentes y cómo afectan la protección jurídica del derecho penal colombiano. Utilizando un enfoque cualitativo, explora los riesgos asociados con la inteligencia artificial, la falta de una regulación adecuada y los desafíos de criminalizar los sistemas autónomos. Los resultados resaltan la necesidad de un marco legal que proteja los derechos de los usuarios y reduzca los riesgos. Se discuten incidentes relevantes y avances legislativos internacionales, proponiendo soluciones para una regulación efectiva de la IA en Colombia y su impacto en la seguridad y la justicia.

Palabras Clave: Acción a propio riesgo, Ciberdelitos, ChatsBots, Inteligencia artificial, Imputación objetiva.

AUTOPUESTA EN PELIGRO DEL USUARIO CON CHATBOTS INTELIGENTES:

Abstract

The objective of this study is to analyze the criteria of user self-responsibility in the interaction with intelligent Chatbots and how these influence legal protection under Colombian criminal law. Using a qualitative approach, the associated risks of AI, the lack of adequate regulation, and the challenges of attributing criminal responsibility to autonomous systems are explored. The results highlight the need to develop legal frameworks that protect user rights and mitigate risks. Relevant incidents and international legislative advances are discussed, proposing solutions for effective AI regulation in Colombia and its impact on security and justice.

Keywords: Action at One's Own Risk, Cybercrimes, ChatBots, Artificial Intelligence, Objective Imputation.

Glosario

Lista alfabética de términos y sus definiciones necesarias para la comprensión del documento.

Algoritmo: es una secuencia de pasos o directrices claras y explicitas que facilitan la ejecución de una actividad o la solución de problema mediante secuencias consecutivas que llevan a la solución del problema en concreto.

Aprendizaje Profundo: también denominada en IA como Deep Learning, es el área dentro del aprendizaje automatizado que utiliza redes neuronales artificiales con múltiples de capas con el objetivo de analizar patrones complejos de grandes volúmenes de datos.

Big Data: gran base de datos generada por las redes sociales y otras fuentes, caracterizada por su tamaño y complejidad, utilizada para análisis y toma de decisiones.

ChatBot Cognitivo: prototipo de IA diseñado para interactuar con usuarios mediante el uso del lenguaje natural, formulando respuestas basadas en análisis de datos y aprendizaje previo.

Chat-GPT: modelo de inteligencia artificial generativa que puede producir contenido original utilizando técnicas de procesamiento del lenguaje natural y algoritmos de aprendizaje profundo.

Ciberdelito: delito relacionado con el uso de computadoras y redes. No existe un estándar claro para el concepto, pero se refiere a delitos cometidos contra o mediante el uso de computadoras.

Ciberespacio: entorno que incluye tanto espacios físicos como virtuales, formado por computadores, sistemas de computación, software, redes de telecomunicaciones, además de datos e información, destinado a facilitar la interacción entre los usuarios.

AUTOPUESTA EN PELIGRO DEL USUARIO CON CHATBOTS INTELIGENTES:

Inteligencia Artificial (IA): integración de tecnologías, metodologías, técnicas y algoritmos diseñados con el objetivo de desarrollar máquinas que exhiban capacidades similares a las del ser humano. Se ordena en cuatro etapas: ingeniería de control, IA clásica inferencial, aprendizaje automático y aprendizaje profundo.

Machine Learning: conocido como sistema de IA de aprendizaje automático que consiste en la capacidad de los sistemas de aprender y evolucionar a través de la experiencia sin necesidad que se programe de manera interna. Estos sistemas emplean algoritmos que evalúan datos y realizan pronósticos.

Redes Neuronales: sistemas informáticos diseñados para imitar la estructura del cerebro humano, que tienen la capacidad de reconocer patrones y procesar información de forma similar a cómo lo hacen las neuronas en el cerebro.

AUTOPUESTA EN PELIGRO DEL USUARIO CON CHATBOTS INTELIGENTES:

Introducción

En la era digital actual, la inteligencia artificial (IA) ha revolucionado muchos campos y transformado la interacción humana con la tecnología. Un ejemplo de este cambio es el desarrollo de chatbots inteligentes que utilizan algoritmos de aprendizaje automático y procesamiento del lenguaje natural para interactuar de forma autónoma con los usuarios. Esta investigación se centra en los estándares de exposición de los usuarios al interactuar con estos prototipos de aprendizaje autónomo y explora las implicaciones legales y los problemas asociados con su uso.

El uso cada vez mayor de la inteligencia artificial en diversas aplicaciones aumenta el riesgo de su uso indebido. En Colombia, la Ley 1273 de 2009 modificó el código penal para proteger la información y los datos, reflejando preocupaciones sobre el uso indebido de tecnologías avanzadas. Sin embargo, el rápido desarrollo de la inteligencia artificial y su integración en la vida diaria ha dado lugar a nuevos tipos de delitos cibernéticos y ha dificultado el procesamiento. En particular, los ChatsBots inteligentes plantean un desafío importante debido a su capacidad para operar de forma autónoma. Planteando dudas sobre la naturaleza de su responsabilidad legal y las responsabilidades de sus usuarios.

A lo largo de la historia, la tecnología ha seguido evolucionando, desde los primeros métodos de computación mecánica hasta los avanzados sistemas de inteligencia artificial actuales. Los algoritmos de aprendizaje automático y aprendizaje profundo permiten que las máquinas aprendan y mejoren de forma autónoma, lo que representa un progreso significativo. Casos recientes, como el del ChatBot de Microsoft, Tay, que aprende un lenguaje ofensivo de los usuarios de Twitter y el de Alexa que plantea desafíos peligrosos basados en desafíos virales, resaltan los riesgos inherentes de la inteligencia artificial. Estos eventos resaltan la necesidad de una regulación

adecuada y una comprensión profunda de cómo estos sistemas interactúan con las personas y aprenden de su entorno.

El propósito de este estudio es analizar los estándares de autorresponsabilidad del usuario y cómo afectan las leyes de protección jurídica en los casos penales colombianos. El objetivo del proyecto es descubrir si la interacción de un usuario con un ChatBot inteligente puede considerarse una amenaza para él mismo. Evaluar cómo la legislación actual y las regulaciones internacionales abordan estos temas. El propósito de esta investigación es proporcionar una base para futuras regulaciones que protejan adecuadamente los derechos de los usuarios y reduzcan los riesgos asociados al uso de sistemas autónomos de inteligencia artificial.

El motivo de este estudio son los riesgos asociados a la inteligencia artificial en la sociedad y su mal uso. Se puede remolcar. La falta de regulación específica de los sistemas autónomos en Colombia y muchas otras jurisdicciones requiere el desarrollo de nuevos marcos legales para abordar adecuadamente los problemas emergentes. Este trabajo se basa en un análisis detallado del dogma penal y una visión general de la evolución legislativa en todo el mundo. Además, se considera el impacto social y económico de la IA, así como las implicaciones éticas y legales de su uso, con el fin de ofrecer soluciones prácticas y teóricas para la regulación de los ChatsBots inteligentes y otros sistemas de IA.

1. Estándares de la auto puesta en peligro del usuario por la interacción con los prototipos de aprendizaje autónomo: ChatsBots Inteligentes.

1.1 Planteamiento del problema

La Inteligencia Artificial (IA), en contextos sociales, ha traído grandes avances significativos, entre los cuales podemos citar a los asistentes de idiomas digitales, automóviles autónomos, robots médicos o de enfermería, incluso prometea que hace parte de estos sistemas al servicio de la justicia, son solo algunos ejemplos que muestran que las tecnologías modernas son omnipresentes (Corvalán, 2018, p. 301). Los Algoritmos Machine Learning y Deep Learning son una realidad. Es la Inteligencia Artificial fuerte, pues han demostrado capacidades para realizar múltiples tareas inteligentes de manera simultánea, sistemas que son entrenados para efectuar razonamientos que logran imitar comportamientos inteligentes.

En este contexto, el crecimiento del uso de internet ha incrementado el riesgo de su utilización indebida, lo que llevó al legislador a modificar el código penal mediante la ley 1273 de 2009. Esta modificación tiene como objetivo proteger el bien jurídico de la información y los datos, con el fin de ejercer control sobre el uso inapropiado de las tecnologías de la información. Sin embargo, la inteligencia artificial ha potenciado los sistemas informáticos, aumentando el riesgo asociado a su uso. Esto es especialmente relevante dado que una persona, valiéndose de estos avances vulnere los bienes jurídicos tutelados en el derecho penal. (Codigo Penal [CP]. Ley 599, 2000).

El escenario se complica debido al acelerado ritmo de crecimiento de la IA, la cual ha sido vinculada a la facilitación de delitos en los ámbitos de la informática y la economía, según el centro cibernético de la policía la inteligencia artificial ha facilitado la comisión de conductas punibles

vinculado a la informática y economía para lo cual conformaron equipo de alianzas estratégicas cibernéticas con entidades de sector público y privado impactadas (Centro Cibernetico de la Policia Nacional, 2022, p. 10).

Esta situación supone la aparición de nuevas formas de infracción a los bienes jurídicos protegidos por el derecho penal, en particular en los ciberdelitos, toda vez que los ciberdelincuentes vienen utilizando la Inteligencia Artificial con el objeto de continuar con su actividad delictiva. En el balance del cibercrimen adelantado por la policía nacional, en el periodo de tiempo entre marzo y noviembre de 2023, arrojó con respecto del año anterior un incremento del 8% de la actividad delictiva, es decir, de 26.366 paso a 28.512 conductas punibles (Centro Cibernetico de la Policia Nacional, 2020, p. 22).

Lamentablemente, este avance tecnológico no ha sido respaldado por una regulación apropiada en el ámbito del derecho penal colombiano, ni se han establecido normas específicas al respecto. Como consecuencia, los sistemas autónomos basados en Machine Learning y Deep Learning no son susceptibles de ser imputados penalmente bajo el paradigma tradicional del delito, lo que implica que no pueden ser considerados penalmente responsables.

La complejidad de los algoritmos de Machine Learning y Deep Learning dificulta aún más la identificación del origen de los errores o comportamientos punibles generados de manera autónoma por los sistemas inteligentes. Esta falta de trazabilidad del razonamiento lleva a situaciones en las que la imputación de responsabilidad se vuelve problemática, ya que el sistema actúa de manera independiente y ajena a las etapas de su creación y utilización. En el contexto del delito, cuando es producto de la intervención de un sistema inteligente autónomo deriva fundamentalmente desde la “teoría del dominio del hecho” en la persona física quien está vinculado con etapas del desarrollo de la IA, es decir, en el diseño, el desarrollo, la

Implementación, el evaluador de impacto el usuario o quien actúa en representación del software (Roxin, Autoría y Dominio del Hecho en Derecho Penal, 2000, p. 153).

La legislación actual no considera a los sistemas autónomos de IA como sujetos de derechos y obligaciones, lo que plantea interrogantes sobre como atribuir responsabilidad penal en casos de delitos cometidos por estos sistemas. Esto incluye determinar los límites de la autonomía de la IA, hasta qué punto los actos realizados por ella pueden ser atribuidos a persona física y en qué condiciones se puede excluir responsabilidad penal del diseñador, programador u operador del sistema.

En este contexto, la investigación se enfocará en los ChatsBots inteligentes, los cuales representan un desafío particular para la atribución de responsabilidad penal debido a la falta de consideración legal como sujetos de obligaciones. Se han planteado preguntas sobre la naturaleza de la inteligencia artificial de estos sistemas, los límites de su autonomía y cómo abordar las complejidades legales asociadas con la participación en el delito cibernético. Es crucial analizar la doctrina penal actual para encontrar soluciones adecuadas a estos problemas emergentes.

Por lo tanto, es necesario estudiar los desafíos que enfrentan los usuarios cuando los ChatsBots inteligentes plantean importantes riesgos legales y penales. El rápido desarrollo de estos sistemas de inteligencia artificial y su integración en todos los aspectos de la vida social plantea nuevos desafíos a los legisladores y a la comprensión tradicional del delito. Los ciberdelincuentes aprovechan estos sistemas para cometer delitos, lo que se refleja en un aumento significativo de la actividad delictiva.

Debido al rápido desarrollo de la inteligencia artificial, este estudio examinará el sistema de censura criminal desde la perspectiva del uso de chatbots inteligentes como medio de implementación para ciertos delitos, como insultos, fraude, daños a computadoras, etc.

1.2 Justificación

La importancia radica en la creciente importancia de los sistemas de inteligencia artificial en la sociedad moderna. La proliferación y adopción masiva de estos sistemas, así como su rápida industrialización, están provocando una revolución comparable a la presenciada con el surgimiento de Internet. Los sistemas inteligentes autónomos o sistemas superinteligentes suponen un gran avance en la evolución tecnológica por su capacidad para reprogramar procesos e interiorizar aprendizajes a partir de información obtenida del entorno.

Estos sistemas basados en algoritmos de aprendizaje automático y aprendizaje profundo representan un gran avance en la evolución tecnológica debido a su capacidad para reprogramar procesos y absorber aprendizaje basado en información recibida del entorno. Basados en algoritmos avanzados, estos sistemas son capaces de tomar decisiones y desarrollar autonomía, como lo demuestran los modelos de chatbot inteligentes, ya que pueden aprender, establecer objetivos y desarrollar planes para superar funciones específicas realizadas por diseñadores y desarrolladores establecieron (Gómez Llinás, 2021, p. 3).

El aumento de las aplicaciones de la IA también ha dado lugar a una serie de preocupaciones relacionadas con su potencial uso delictivo. En el informe de evaluación de la amenaza del crimen organizado en internet (IOCTA) 2024 de Europol indico que los ciberataques ransomware, la explotación sexual infantil y los esquemas de frade en línea y de pagos siguen siendo las manifestaciones más relevantes en los ciberdelitos en la Unión Europea, dirigiéndose a pequeñas y medianas empresa debido a su débil infraestructura de defensa contra ciberataques, lo que implico que con la llegada de la IA se prolifero diferentes formas como puede ser empleada en la comisión de delitos, incluyendo la suplantación de identidad, desacreditar una figura pública, extraer fondos de cuentas bancarias, drones y vehículos autónomos utilizados como armas, son

entre muchas otras actividades delictivas que el informe alerta en un futuro no muy lejano, el autor principal del informe expuso que a medida que se expanden las capacidades de las tecnologías basadas en IA, también lo hace su potencial para la explotación criminal (Europol, 2024, p. 10).

Además, casos reales, como el incidente en el que un vehículo Tesla en modo autónomo atropello a un robot ruso y se da a la fuga, durante una presentación en las Vegas, Estado Unidos. (Gañán, 2019, p. 1). El primer delito donde se implicó a un sistema de IA para simular la voz de un ejecutivo de una compañía de energía y exigieron una transferencia de 243.000 euros (Abogado Digital, 2019, p. 1)

A pesar de los importantes efectos positivos del uso de equipos inteligentes, los riesgos persisten detrás de la esquina, un ejemplo muy reciente, demuestra los peligros de los asistentes de voz como Alexa quien propuso un reto muy arriesgado, llamado "penny challenge", en boga en la red social Tik Tok, donde el asistente llamó a una niña de diez años incitándola a insertar parte de los enchufes de un cargador en él toma corriente, dejando la mitad afuera, para poder colocar una moneda entre los dos polos expuestos (La Vanguardia, 2021, p. 1).

Incluso en contextos más cotidianos, como las redes sociales, la IA presenta desafíos significativos. La capacidad de los ChatsBots para aprender y adaptarse a partir de interacciones con usuarios puede conducir a la proliferación del discurso de odio y la desinformación, un ejemplo de ellos es Tay - Thinking About You, un ChatBot creado por Microsoft para experimentar y realizar investigaciones sobre la comprensión conversacional, estuvo disponible a través de Twitter el 23 de marzo 2016. El problema fue que Tay estaba inundado de mensajes que elogiaban el odio racial, el nazismo y el consumo de drogas, en consecuencia, el ChatBot aprendió este lenguaje y comenzó a twittear de la misma manera, generando dentro de las dieciséis horas de

haber estado disponible más de 96,000 tweets obscenos en línea, respondiendo a las provocaciones de otros usuarios: Microsoft se vio obligado a suspender el servicio (Hunt E. , 2016, p. 1).

Estas preocupaciones son especialmente relevantes en el ámbito jurídico, donde la falta de claridad sobre la responsabilidad penal de los sistemas de IA platea desafíos significativos. A medida que la tecnología continúa avanzando, es crucial evaluar como adaptar el marco legal existente para abordar los delitos relacionados con la IA y garantizar la protección efectiva de los derechos de las personas afectadas.

Los ChatsBots son el emblema de la aplicación del procesamiento del lenguaje natural, es decir, la capacidad de máquinas para procesar palabras haciendo oraciones y discursos similares a un ser humano. La aplicación almacena todas las conversaciones que tienen lugar en las redes sociales, artículos publicados en periódicos online y en Blogs, La web es su fuente primaria de conocimiento y evolución, en la forma de aprender a entender nuestro modo de comunicación para ser capaz de formular frases y discursos con sentido.

Como consecuencia, al ser el lenguaje, utilizado por la sociedad en línea, es racista, misógino, de negación y nazi, también lo será el Lenguaje de IA. La odiosa manifestación del pensamiento en las redes sociales conlleva el surgimiento de un debate en relación con la posibilidad de utilizar la limitación a la libertad de expresión cuando de la misma resulten conductas discriminatorias e incitadoras al odio.

En ese sentido, para poder evaluar el fundamento de la creación de la responsabilidad penal individual es necesario comprender los orígenes de esta evolución y el tratamiento al que ha sido sometida, en ese orden, la evolución de la sociedad y el concepto de Estado ha repercutido en la construcción del derecho, así mismo, esta evolución ha marcado el derrotero de los conceptos dogmáticos de la responsabilidad penal individual, por lo que surge el cuestionamiento de si la

interpretación actual de la Sociedad y el Estado permiten desentrañar los presupuestos que logren resolver los problemas del avance tecnológico y su implicación en las infracciones al bien jurídico de la información y los datos.

Estos presupuestos dogmáticos darán paso a ajustar la norma jurídica penal y a establecer nuevos mecanismos, para atribuir a los sistemas autónomos la responsabilidad, con el objeto de dar respuesta concreta a hechos delictivos o, por el contrario, limitar la competencia a la jurisdicción civil, por los daños causados por los ChatsBots inteligentes, implicando una mera indemnización a la víctima, lo cual puede conllevar a un escenario de que la auto puesta en peligro como exclusión de responsabilidad penal, derive en que algunos desarrolladores diseñen y entrenen estos sistemas con fines delictivos, teniendo en cuenta que su Responsabilidad está limitada por la operación que realice el usuario del ChatBot, desnaturalizando la protección de derechos tutelados en el código penal de los usuarios.

1.3 Objetivos

1.3.1 Objetivo general

Analizar los criterios de autorresponsabilidad del usuario que originan la desprotección del Derecho Penal cuando el resultado de la interacción con los sistemas de aprendizaje autónomo, ChatsBots Inteligentes, originen riesgos en los datos e información personal.

1.3.2 Objetivos específicos

Contextualizar las acciones de los ChatsBots inteligentes, sin pretender analizar técnicamente cada paso de un algoritmo, a fin de evaluar si los usuarios, personas físicas, en la interacción en el caso concreto, puedan calificarse como auto puesta en peligro.

Identificar los avances en legislación internacional y nacional en la regulación de sistemas dotados con inteligencia artificial a fin de extraer los estándares pertinentes en la valoración de la conducta de los usuarios.

Evaluar las interacciones entre el usuario, persona física, y el prototipo ChatBot Inteligente puedan ser subsumidas en la infracción de los deberes de autoprotección del usuario.

2. Marco referencial

2.1 Marco teórico

Durante los últimos 200.000 años de existencia de la humanidad, el proceso evolutivo nos enseñó que crear es de seres humanos, cualidad entendida como la capacidad inherente al individuo de ser los únicos en hacer arte, planos, maquinas, cocina, contratos etc., ahora dicha capacidad no es única de los humanos, en la actualidad los programas de inteligencia artificial (IA) son extensiones de la actividad humana, dibujan planos, crean contratos, correos electrónicos, declaración de impuestos, escriben presentaciones, asisten de manera virtual y responden consultas (ChatBot), entre otras actividades que hace algunos años su autor fue únicamente el ser humano.

Aunque la conferencia de Dartmouth fue el punto de inflexión oficial para el estudio de la IA, muchas de las ideas técnicas al respecto han existido durante algún tiempo, Los inicios de los sistemas de cálculo mecánico se remontan al uso del ábaco alrededor del año 400 a.C.

Posteriormente, en 1642, Blaise Pascal desarrolló la Pascalina, una máquina diseñada para facilitar al cobrador de impuestos la realización de operaciones de suma y resta mediante un sistema de engranajes. No obstante, estos dispositivos presentaban limitaciones que solo permitían su funcionamiento bajo ciertas condiciones especulativas (Marguin, Histoire des instruments et machines à calculer: trois siècles de mécanique pensante, 1642-1942, 1994, p. 48).

A través de las investigaciones fueron muchos los prototipos diseñados y que hoy en día han sido perfeccionados, tanto así, que los atributos de la IA son: el aprendizaje autónomo, el uso del lenguaje natural, analizan datos, formulan abstracciones y conceptos que confluyen a resolver problemas que al inicio han sido reservados a los seres humanos.

Avanzando en el desarrollo de los primeros prototipos, en el siglo XIX Charles Babbage diseñó en 1821 un aparato conocido como la máquina diferencial. Esta calculadora empleaba el método de las diferencias para facilitar los cálculos de logaritmos y tenía la capacidad de manejar hasta veinte cifras de dieciocho dígitos cada una. Se trataba de la primera máquina analógica programable, que utilizaba ruedas dentadas de diez dientes cada una para representar números en el sistema decimal. Gracias a la disposición de estas ruedas metálicas, organizadas en columnas, se podían realizar cálculos minimizando los errores humanos. Este aparato posibilitó el desarrollo de algoritmos que se escribían en tarjetas perforadas, las cuales permitían introducir instrucciones que la máquina podía ejecutar. (Bromley, 1982, p. 200).

En 1833, tras una década dedicada al desarrollo de la máquina diferencial, Charles Babbage inició el diseño de un modelo más avanzado conocido como motor analítico. Este nuevo prototipo estaba diseñado para procesar tarjetas perforadas, las cuales eran empleadas en la siguiente fase del proceso. Asimismo, utilizaba los números generados por la máquina diferencial como entradas para cálculos posteriores. El motor analítico estaba equipado con una memoria para almacenar los

resultados de las operaciones y un sistema de control que permitía ejecutar automáticamente una serie de operaciones basadas en el mecanismo de las tarjetas perforadas, similar al utilizado en los telares (Bromley, 1982, p. 200).

La concepción de las tarjetas perforadas se originó mucho antes, a comienzos del siglo XIX, con “los Telares Jacquard". Este era un telar mecánico que empleaba dichas tarjetas para automatizar la fabricación de textiles, codificando los patrones de bordados y decoraciones que se debían ejecutar (Hobsbawm, La Era de la revolución 178-1848, 2009, p. 30).

Desafortunadamente, debido al alto costo de dichos equipos, se fabricaron a partir del siglo XX, y fue solo en 1920 que nació la máquina computacional, un instrumento capaz de realizar el trabajo de un humano, realizando cálculos a través de métodos efectivos y rápidos.

Entre los años cincuenta y setenta se afianza la investigación sobre IA y gracias a las ideas de Charles Babbage, nacieron las primeras computadoras electrónicas y digitales, robots primitivos capaces de realizar autónomamente las secuencias de instrucciones, soportada en la teoría propuesta en 1948 por el matemático John von Neumann (Rojas & Hashagen, 2000, p. 29).

Al año siguiente en (1949) la intuición de Donald Hebb, ligada al hecho de que las neuronas se comunican enviándose descargas entre sí, llevo a que la máquina informática se convirtiera exclusivamente en un ordenador eléctrico que representaba la actividad básica del aprendizaje y la memoria, lo que implico comparar el cerebro con una computadora sofisticada que brinda la posibilidad de replicar la inteligencia humana a través de un cerebro artificial (Garcia Vega, 1986, p. 34)

Sobre estas bases, Frank Rosenblatt, un científico comprometido en un proyecto de investigación financiado por la Armada estadounidense en el Laboratorio Aeronáutico de la Universidad de Cornell, desarrolló el perceptrón que es una neurona artificial y por tanto, una

unidad de red neuronal, estudio que tenía como objetivo resolver problemas complejos gracias a la conexión de entradas y salidas realizadas, es decir, un modelo computacional inspirado en neuronas biológicas (Laboratorio Aeronautico de la Universidad de Cornell, 1957, p. 7).

Casi al mismo tiempo, Warren McCulloch y Walter Pitts toman como objeto de estudio el cómputo que hacen las neuronas y propusieron el primer modelo de neuronas artificiales con el fin de estudiar las características y capacidades computacionales como los mecanismos de autorregulación y control presentes tanto en organismos vivos y máquinas, modelo que posee la capacidad de modificar su comportamiento en función de las tensiones que le impone el entorno, es decir caracteriza a la neurona como un dispositivo lógico (Prieto Meléndez, Padrón Godínez, Herrera, & Perez, 2000, p. 4).

Pero fue recién en 1952 cuando apareció por primera vez el término Machine Learning. gracias a Arthur Samuel, un científico informático de IBM que publicó un artículo titulado Algunos estudios sobre Machine Learning usando el juego de damas. Este trabajo fue uno de los primeros y más influyentes ejemplos de aprendizaje automático donde el juego damas aprendió de la experiencia (Arthur, 1959, p. 215).

El Aprendizaje automático en el programa de juego de damas consistía en la capacidad del software de mejorar a sí mismo, aprendiendo nuevas técnicas automáticamente a través de una función matemática que determinaba la puntuación en función de la posición de los peones en el tablero de ajedrez, conllevando a emitir una estimación de la probabilidad de ganar calculando cada movimiento individual, el sistema aprendió memorizando el valor de la función para cada posición (Arthur, 1959, p. 215).

Entonces se puede inferir que el aprendizaje automático permite que las computadoras aprendan sin programación capilar sobre métodos de aprendizaje, alimentando un algoritmo con datos para que la máquina aprenda a realizar una determinada operación de forma automática.

Después de un breve repaso en los principales antecedentes de la IA, llegamos al que podemos llamar el padre de las computadoras y de la IA gracias a sus ideas influyentes detrás de la informática: Alan Turing, fue en el verano de 1956 en la Conferencia Académica de Darmouth College, donde inicio con su artículo, Maquinaria computacional e Inteligencia, en el cual planteó la hipótesis de que la máquina podía pensar y creó una prueba para comprobarlo, el juego de la imitación, la cual midió la IA de la máquina por lo fácil que era distinguirla del ser humano (Turing, 2010, p. 3).

Para realizar la prueba era necesario dotar a una persona de un teclado para escribir preguntas y en el otro extremo del terminal era necesario colocar una máquina y un ser humano, si el sujeto que hace las preguntas encuentra dificultad para entender de dónde viene la respuesta (de la máquina o de la persona), entonces la prueba podría considerarse superada, para Alan Turing, las máquinas no piensan, sino que imitan pensamiento humano.

En la misma Conferencia Académica de Darmouth College John McCarthy, Marvin Minsky, con Allen Newell y Herbert Simón, acuñaron un término de definición de IA, los científicos tenían como objetivo crear una máquina que realizara acciones inteligentes, es decir, cómo desarrollar algoritmos que puedan aprender de forma autónoma a partir del conocimiento existente como lo hacen los humanos, estos pioneros imaginaron y diseñaron una computadora con la capacidad de simular la inteligencia humana, sin embargo, nunca logró realizar sus ideas por falta de los recursos necesarios para llevarlas a cabo.

Luego, en el año de 1960, los robots comenzaron a usarse en las industrias, el primero en trabajar fue en una línea de montaje, transporte de piezas del sistema de calefacción en los automóviles, denominado "Unimate", en 1961, diseñado por George Devol para reemplazar al hombre en los trabajos más peligrosos (Russell & Norvig, 2008, p. 1066).

Un gran avance en IA fue Eliza en 1965 de Joseph Weizenbaum, el cual se puede definir como el prototipo de lo que ahora se llama ChatBot, un sistema informático que interactúa con un humano en una conversación. Eliza fue apodada La Doctora porque pretendía ser una psicoterapeuta que generaba respuestas basadas en ciertas palabras clave, a pesar de su eficiencia, "Eliza" nunca pasó la prueba de Turing (Weizenbaum, 1966, p. 40).

Continuando Russell & Norvig, (2008), expuso que la primera persona electrónica fue "Shakey" en 1966, producida en 1969 por SRI International, es un robot sobre ruedas de uso general, con movilidad autónoma con capacidad para interpretar instrucciones y capacidad para acción, tenía defectos, pero a la vez abría el campo a la investigación en robótica móvil, que podría ser operado a través de una consola con comandos específicos (p. 43).

En 1970 nacieron los primeros “sistemas expertos” lo que implicaba que el conocimiento ya no estaba ligado a la comprensión teórica del problema y por lo tanto era necesario profundizar en las reglas de la experiencia, para poder comparar el sistema experto con un experto humano, los primeros prototipos fueron "Dendral", programa diseñado para inferir la estructura de moléculas orgánicas según fórmulas químicas y "Mycin", diseñado para el diagnóstico médico y prescripciones de tratamientos para infecciones bacterianas de la sangre a partir de información, incluso parcial, sobre síntomas (Russell & Norvig, 2008, p. 1066).

A principios de la década de 1980, la IA se estaba desarrollando como industria y paralelo a ello, sin dejar el estudio de las redes neuronales. En el año 1985 nace la disciplina de las ciencias

cognitivas, cuyo objetivo consistía en integrar la psicología e IA considerando la máquina como herramienta de estudio de la mente, fue una simbiosis que llevaba a cabo operaciones intelectuales mucho más efectivas de lo que el ser humano puede hacer (Licklider, 1960). Finalmente, se agregó el enfoque sub-simbólico al estudio tradicional del conocimiento, a través del cual permite que los sistemas utilicen IA incluso sin tener una representación detallada de conocimientos básicos (Aliseda Llera, 2007, p. 28).

Por otro lado, Japón, a partir de 1982, lanzó un programa público para la evolución de IA creando los "Sistemas Informáticos de Quinta Generación". La idea era superar las generaciones anteriores de computadoras compuestas por tubos, transistores, diodos, circuito integrado y computadoras basadas en microprocesadores y pasar a trabajar una gran cantidad de procesadores utilizando un lenguaje de programación lógico, tales ideas, desafortunadamente, tardaron en convertirse en éxitos prácticos, debido al agotamiento de la financiación (Sáez Vacas, 1987, p. 68).

Posteriormente, en la década de los noventa pudimos presenciar un comienzo del renacimiento de los sistemas de quinta generación gracias al avance tecnológico que tuvo, por ende, hizo más accesible la implementación, por cuanto el hardware se había vuelto más barato y confiable, el Internet había brindado la capacidad de recopilar cantidades masivas de datos y tener un gran poder de cómputo y archivo para analizarlos.

Estos desarrollos permitieron una gran evolución de la IA dándole la posibilidad de influir fuertemente en la vida cotidiana de los seres humanos, en este punto, los investigadores aplicaron el concepto de aprender jugando, lo que implico el avance del campo de los gamer, un excelente escenario de entrenamiento para la formación sobre la evolución y el autoaprendizaje de las máquinas.

AUTOPUESTA EN PELIGRO DEL USUARIO CON CHATBOTS INTELIGENTES:

En el escenario de los juegos comenzó con el ajedrez en 1996, Deep Blue de IBM fue la primera computadora en derrotar al campeón del mundo usando un algoritmo llamado "fuerza bruta" que analizó millones de secuencias antes hacer el movimiento más probable que condujera a la victoria, este método, sin embargo, no fue eficaz para juegos de mesa más complejos como Go, de hecho, en 2016, DeepMind, ahora propiedad de Google, ha creado AlphaGo superando al entonces ganador indiscutible de Go y reemplazando el algoritmo de "fuerza bruta" con uno basado en la extracción de correlaciones estadísticas entre las acciones realizadas por los jugadores para predecir el próximo movimiento (DeepMind, 2017, p. 2).

En 1999, Sony se dio cuenta de AIBO (Artificial Intelligence Robot): un perro robot con la capacidad de aprender a través de la interacción con el entorno y con los propietarios respondiendo a más de 100 comandos de voz (Montero Mora, Méndez Muñoz, & Domínguez Rodríguez , 2008, p. 7).

En la década de 2000, la evolución permitió a Breazeal desarrollar Kismet, un robot que reconocía y simuló emociones con su rostro, así como Honda lanzo “ASIMO”: un robot basado en humanoide sobre IA, Pero el verdadero éxito llegó en 2002, cuando I-Robot lanzó Roomba, un robot aspirador autónomo con la capacidad de limpiar la casa evitando obstáculos (Perez Vidal, Castro González , Alonso Martín , Castillo, & Salichs, 2017, p. 838).

En 2006 la NASA crea un taladro dotado de IA donde el software funcionaba como un ser humano experimentado que emula comportamiento de sentido y escucha de las vibraciones, inteligencia que transforma los datos en determinar que tanto ha avanzado el taladro en profundidad sobre la superficie, este prototipo basado en IA tenía su misión taladrar la superficie de Marte sin intervención humana (NASA, 2006, p. 2)

AUTOPUESTA EN PELIGRO DEL USUARIO CON CHATBOTS INTELIGENTES:

Fei-Fei Li armó (2007) ImageNet: una base de datos de imágenes para crear software de reconocimiento automático de objetos (Johnson , Karpathy, & Fei - Fei, 2016, p. 1). En 2010 Microsoft creo Kinect para Xbox 360, el primer dispositivo de juego que rastreaba los movimientos del cuerpo humano usando una cámara 3D y detección de infrarrojos, un descubrimiento, que puede hacerte sonreír pero que fue fundamental para la evolución de esta área.

En 2011 debutaron los asistentes de voz y los ChatsBots capaces de reconocer el idioma natural, gracias a Siri de Apple que, con una interfaz ad hoc, tenía y tiene la capacidad de responder al usuario consistentemente basado en el contexto a través de comandos de voz, dando la posibilidad de aprovechar una experiencia personalizada para el tema individual (Kaplan & Haenlein, 2018, p. 18).

Pero Apple no fue la única en moverse en el terreno de los asistentes de voz, pues en 2014 llegó Microsoft y lanzó Cortana (Microsoft, 2014, p. 1). En ese mismo año, Amazon produjo Alexa, parlantes inteligentes utilizados como asistentes personales, brindando información sobre los pedidos y pudiendo controlar electrodomésticos compatibles y conectados a la red (Amazon, 2014, p. 3), incluso Siri de Google, en 2008, había lanzado la función de reconocimiento de voz para la búsqueda en línea.

Las evoluciones no terminaron ahí, solo por mencionar algunos: en 2014 Google creó el auto sin conductor que pasó el examen de manejo independiente en Nevada. En 2016, Hanson Robotics diseñó la primera ciudadana robótica Sophia que también se comunicaba y expresaba a través de expresiones faciales (Hanson Robotics, 2016, p. 3).

En 2018, Alibaba, un gigante chino, con un sistema de IA superó al intelecto humano en una prueba de comprensión de lectura. y en el mismo año Google lanzó Bert, un algoritmo creado para mejorar la comprensión de lo que los usuarios quieren googlear (Alibaba, 2018, p. 1).

AUTOPUESTA EN PELIGRO DEL USUARIO CON CHATBOTS INTELIGENTES:

En la actualidad, el desarrollo de la IA ha adquirido un espacio en actividades que solo antes los seres humanos lo podían hacer, esta tecnología ha experimentado dos oleadas en los últimos años, primero la facilidad de obtención de datos debido a las proliferación de aplicaciones y redes sociales que originan un banco de datos que las empresas utilizan a fin de canalizar sus ventas, denominado big data y segundo, la amplia aplicación del aprendizaje autónomo, las redes neuronales y otras tecnologías que han conllevado a que la investigación en IA haya dado un giro y se ha convertido en el campo de investigación más popular.

No es una ficción que la tecnología de IA está siendo utilizada en muchas áreas, como la conducción, la logística, la programación, el tratamiento médico e incluso los juicios, entre ellos podemos citar a la Corte Suprema de Wisconsin de los Estados Unidos en el cual utilizó los datos analizados por la IA como insumo para juzgar la posibilidad de reincidencia (Estado de Wisconsin Vs. Eric L. Loomis, 2016, p. 20).

En ese sentido, la IA ya ha tenido un impacto generalizado en nuestras vidas, es utilizada para cotizar medicamentos y casas, ensamblar automóviles, determinar qué anuncios vemos en las redes sociales e incluso dentro de esta área de tecnología tenemos la IA generativa, que es una categoría nueva del sistema al que se le puede pedir que cree contenido completamente novedoso como el prototipo denominado Chat-Gpt (OpenAI, 2021, p. 2).

Pero la tecnología también trae consigo aspectos negativos y usos distorsionados de la misma como la realización de armas autónomas basadas en IA con fines de guerra, que pueden decidir, sin intervención del hombre, si disparar o no. De hecho, en 2015 Elon Musk, Stephen Hawking y Stave Wozniak firmaron una carta pidiendo prohibir el desarrollo de tal tecnología bélica.

Después de hacer un breve recuento de los prototipos iniciales que han aportado a lo que hoy se comprende como IA, es necesario desarrollar el concepto a fin de lograr llegar a comprender de que se trata los ChatBot cognitivos, además que los antecedentes hasta aquí expuestos sean de insumos a la hora de entender de manera general su funcionamiento.

2.2 Marco conceptual de inteligencia artificial.

Para entender la IA es fundamental analizar el concepto. Para citar algunos de ellos podemos traer la definición de la Comisión Europea (2018), en la cual nos indica que el término de IA hace referencia a "los sistemas que emulan comportamientos inteligentes que en algunos casos puede consistir simplemente en programas informáticos" (Comision Europea, 2018, p 237)

Otra definición puede ser la que el tratadista Patrick Henry Winston (1992) que define la IA como el estudio de las ideas que permite que los ordenadores sean inteligentes (Winston, 1992, p. 12). Se describe también como la "habilidad de un sistema para procesar adecuadamente información externa, aprender de estos datos y utilizar estos aprendizajes para cumplir objetivos y tareas específicas mediante una adaptación flexible" (Kaplan & Haenlein, 2018, p. 18). La Enciclopedia de Inteligencia Artificial describe esta como un conjunto de tecnologías, modelos, técnicas y algoritmos diseñados para desarrollar máquinas capaces de imitar las habilidades humanas (EnciclopedIA, 2023, p. 2).

Ahora bien, para entender el concepto de IA de manera amplia se puede ordenar en cuatro etapas. La primera es la ingeniería de control o un sistema con un programa de control simple llamado ingeniería de sistemas, un ejemplo sería el robot aspirador; La segunda etapa es una IA clásica, inferencial o sistemas navegables como los programas para resolver acertijos o crucigramas como el software WebCrow 2.0. El tercero es el aprendizaje automático, en esta etapa

se incorpora un motor de búsqueda para gobernar o el sistema aprende conocimiento por sí misma, como la plataforma de aprendizaje automática Vertex AI de Google Cloud, y finalmente, la cuarta etapa que es denominada como aprendizaje profundo, algoritmo que aprende de la entrada de datos en sí misma, y el mismo, crea incluso reglas por sí solas y toma decisiones autónomas como, ChatBot cognitivos, los drones autónomos, vehículos autónomos.

Ahora bien, la IA tiene una clasificación, inteligencia artificial débil e IA fuerte, este concepto fue introducido inicialmente por el filósofo John Searle en un artículo publicado en 1980, en donde expone que la inteligencia artificial débil consiste en que el computador es una herramienta para estudiar ciertos procesos abstractos (Russell & Norvig, 2008, p. 1066).

Según Russell & Norvig, (2008), la IA débil maneja tareas en un campo específico, como ya antes se expuso fue evolucionando, lo que al inicio mencionábamos sobre las aplicaciones como AlphaGo, como ya antes se expuso, es un programa informático desarrollado por Google DeepMind y es lo más cercano al imitar la inteligencia humana, donde se obtiene un rendimiento similar o superior al de los humanos, en otras palabras, es la etapa tres de los pasos mencionados anteriormente. Esta inteligencia se limita a un dominio, sigue siendo un sistema con control significativo humano, pero posee inteligencia humana en un área limitado (P. 1107).

La IA fuerte es una computadora convenientemente diseñada que no simula una mente, sino que es una mente, hoy en día, esta distinción se mantiene, aunque la IA fuerte se divide nuevamente en dos etapas, IA débil como primer paso, es decir el sistema o maquina piensa por sí mismo, evoluciona y aprende información constantemente. La segunda es la IA fuerte o aprendizaje profundo, aquí el software o máquina es plenamente autónomo, no existe control significativo humano, en otras palabras, pareciera ser que el equipo o maquina tiene un corazón humano (Russell & Norvig, 2008, p. 1066).

Dentro del concepto de la IA hay que destacar dos aspectos fundamentales: autonomía y autoaprendizaje. El primero es la capacidad de tomar decisiones y también de implementarlas sin control o influencia externa; depende del grado de complejidad con que fue diseñado en la relación entre la máquina y el medio ambiente. El segundo es el rasgo fundamental está representado por la capacidad de aprender de la experiencia.

Son enfoques distintos, razonamiento lógico y aprendizaje automático. El primer método se basa en una vista de arriba hacia abajo del problema, que le permite describir con precisión un contexto dado, pero la máquina necesita conocer muchas reglas y entrenar en muchos casos y para esto no es muy agradable en contextos más complejos.

El segundo método, por otro lado, es un enfoque de abajo hacia arriba, parte de los datos disponibles para saber el entorno, ellos mismos describen, determinan el fin y son capaces de realizar la actividad en forma coherente y de analizar grandes volúmenes de datos.

según Russell & Norvig, (2008), el término aprendizaje automático se refiere a los enfoques mediante los cuales los sistemas pueden mejorar su desempeño aprendiendo automáticamente de la experiencia cómo realizar tareas futuras (p. 811).

Entonces, el sistema construye automáticamente su propio modelo a partir del análisis de datos, sobre la base de algoritmo de aprendizaje automático. A partir de este modelo, el sistema genera clasificaciones, valoraciones y previsiones sobre los nuevos casos que se le presenten.

2.3 Estado del arte

La inteligencia artificial y los robots son los principales temas de la Cuarta Revolución Industrial. Países avanzados, como los Estados Unidos, el Japón y Europa, han comenzado a invertir e investigar en robots de IA desde mucho tiempo y están inmersos en la regulación y las

actividades de ajuste de políticas para mantener el ritmo de las tendencias. Por lo tanto, si se observa el estado de la investigación de robots de IA, se considera que este puede ser un indicador importante de qué tipos de robots de IA aparecerán en el futuro. En este sentido, en este trabajo se muestra la forma en que investigan algunos países y empresas.

Un robot estadounidense llamado Elektro se presentó en la Exposición Universal de Nueva York en 1939. Este robot mide siete pies o 2.13 m de altura y pesa 266 libras o 120.66 kg. Torpemente capaz de caminar hacia adelante y hacia atrás cuando se enciende y de formular aproximadamente 77 palabras pregrabadas, a Elektro se le reconoce como el primer robot del mundo. Sin embargo, la forma en que se concebían los robots entonces estaba muy lejos del concepto moderno de robot de IA (Lopéz, 2022, p. 2).

Uno de los megaproyectos del gobierno de los EE. UU es la Iniciativa BRAIN, (Brain Research through Advancing Innovative Neurotechnologies Initiative), cuyo objetivo es analizar la estructura del cerebro humano y replicarla en un sistema informático para la percepción, el comportamiento y la conciencia e implementar directamente los métodos de almacenamiento y procesamiento de datos del cerebro humano en sistemas de inteligencia artificial. El 80 % del presupuesto de la Iniciativa BRAIN va a la investigación básica y el 20 % restante al desarrollo de dispositivos como la Interfaz Cerebro-Computadora, sistemas de microscopía fluorescente ultra pequeña para escaneo y supercomputación de cerebros simulativos (Obama, 2013, p. 4).

En 2016, Estados Unidos se llevó a cabo una serie de cinco talleres entre mayo y julio, posterior a ello se publicó en octubre el informe Preparándose para el Futuro de la Inteligencia Artificial, y luego en el mes de diciembre presentó el informe la inteligencia artificial, la automatización y la economía, que analiza el impacto de la IA y la automatización en la economía (Observatorio de Inteligencia Artificial, 2016, p. 1).

AUTOPUESTA EN PELIGRO DEL USUARIO CON CHATBOTS INTELIGENTES:

DARPA es la Agencia de Proyectos de Investigación Avanzada de Defensa de Estados Unidos donde se viene desarrollando el proyecto ALIAS para desarrollar aviones totalmente autónomos que sustituirán a los actuales aviones de combate. Esta iniciativa también ha presentado el proyecto CODE (Operaciones Colaborativas en Entornos Hostiles) para crear drones autónomos que requieran poco control humano (Defense Advanced reearch Projects Agency, 2020, p. 1).

Bajo esa línea de desarrollo, las Naciones Unidas emitió un informe final que enfatiza el enorme potencial de la inteligencia artificial (IA) para impulsar avances científicos, mejorar la salud pública y contribuir al logro de los Objetivos de Desarrollo Sostenible. Sin embargo, también señala riesgos significativos como el sesgo, la desinformación y desafíos éticos y de sostenibilidad. Resalta la necesidad de una gobernanza global inclusiva para gestionar la IA de manera efectiva, superar la falta de coordinación y representación, y evitar desigualdades. Propone la creación de un grupo internacional de expertos en IA, un marco global de datos y una red de desarrollo de capacidades, así como un fondo y una oficina de IA en la ONU para garantizar un enfoque coordinado que maximice los beneficios de la IA y minimice los riesgos, promoviendo una adopción equitativa y responsable a nivel global. (Naciones Unidas, 2024, p. 76).

Las empresas y organizaciones a nivel global han avanzado rápidamente en el ámbito de la inteligencia artificial, y la inversión en investigación ha aumentado considerablemente. Solo en 2020, se destinaron alrededor de 900 millones de euros a empresas vinculadas a la inteligencia artificial en Estados Unidos y Europa Occidental (Comision Europea, 2018, p. 1).

Desde 2013, Google ha estado promoviendo la investigación y el desarrollo de inteligencia artificial mediante su Proyecto Manhattan de IA. Este proyecto involucra a startups de Silicon Valley y se centra en la creación de sistemas basados en IA, como vehículos autónomos, drones y servicios de entrega automatizados. Como parte de esta iniciativa, Google ha adquirido varias

empresas relacionadas, incluyendo Nest, que produce dispositivos inteligentes para el hogar, y DeepMind, que se especializa en algoritmos de aprendizaje profundo. (Manyika, Dean , Hassabis , Croak, & Pichai , 2018, p. 5).

El programa AlphaGo de DeepMind transformó el ámbito del go al combinar técnicas de búsqueda tradicionales con una exploración avanzada a través de redes neuronales profundas (DeepMind, 2017, p. 2). Además, Google ha adquirido varias empresas de robótica, como Meka Robotics, Bot & Dolly, Redwood Robotics y Schaft, y continúa investigando en software y hardware. En noviembre de 2015, Google presentó TensorFlow, un algoritmo de redes neuronales de código abierto que permite a otras empresas participar en el proyecto sin costo. Desde 2009, Google también ha estado trabajando en el desarrollo de vehículos autónomos y en 2016 fundó Waymo, que lanzó un programa de prueba de conductores en 2017 (Winred & Serfatty Godoy, 2024, p. 1).

Como se mencionó anteriormente, IBM es famoso por haber desarrollado Deep Blue, que logró vencer al campeón mundial de ajedrez Garry Kasparov. Más tarde, IBM creó Watson, una inteligencia artificial que participó en el concurso de preguntas Jeopardy y superó a sus campeones históricos, lo que generó un gran impacto. A finales de 2012, IBM entrenó a Watson con grandes volúmenes de datos médicos en colaboración con la Clínica Cleveland, y desde entonces ha sido utilizado en el diagnóstico y tratamiento de pacientes. (Deloitte, 2014, p. 4). Para 2013, Watson ya había procesado 600,000 informes médicos, registros de 1.5 millones de pacientes y 2 millones de páginas de revistas médicas. Actualmente, se utiliza en sectores como finanzas, salud, seguros y telecomunicaciones (Kaplan & Haenlein, 2018, p. 18).

Microsoft, famosa por su software, ha mostrado un gran interés en la inteligencia artificial. Uno de sus logros es el chatbot Tay, que aprendía a conversar a través del aprendizaje profundo.

AUTOPUESTA EN PELIGRO DEL USUARIO CON CHATBOTS INTELIGENTES:

Sin embargo, Tay fue retirado después de 16 horas porque los usuarios le enseñaron lenguaje inapropiado y ofensivo, lo que evidenció los riesgos de un aprendizaje descontrolado. Microsoft también ha desarrollado Face API, un algoritmo en la nube que permite la detección y el reconocimiento facial, capaz de identificar hasta 64 rostros en una imagen y realizar agrupaciones y verificaciones de identidad (Hunt E. , 2016, p. 2).

SoftBank es famosa por su robot doméstico Pepper, que se destaca por su enfoque en la interacción emocional con las personas. Pepper puede reconocer rostros y mantener conversaciones que se adaptan al contexto, y su motor emocional le permite identificar e imitar emociones. Además, su diseño físico, con un rostro redondeado y grandes ojos, está pensado para ser atractivo y diferente de los robots que se centran en tareas específicas. Pepper también tiene la capacidad de actualizar sus funciones a través de la nube, lo que le permite aprender y evolucionar de manera continua (SoftBank Robotics, 2018, p. 1).

OpenAI es una organización de investigación sin fines de lucro que se enfoca en la inteligencia artificial general (AGI). Entre sus fundadores se encuentran personalidades como Elon Musk y Sam Altman, así como empresas como Microsoft y Amazon. Su objetivo es desarrollar AGI de forma segura y asegurar que sus beneficios se distribuyan de manera amplia. Además, OpenAI promueve el uso ético de la información y comparte herramientas y publicaciones de código abierto para impulsar la investigación en inteligencia artificial (OpenAI, 2021, p. 2).

El Deep Blue de IBM, que derrotó al campeón mundial de ajedrez, no contaba con habilidades avanzadas en ajedrez desde el principio. Se llevó a cabo un proceso continuo de mejora a través de sus predecesores, como ChipTest, Deep Thought, Deep Thought 2 y Deep Blue 1, hasta llegar a Deep Blue 2. La IA fue aprendiendo estrategias y jugadas de ajedrez a lo largo de múltiples

competiciones, heredando conocimientos y superando las limitaciones de los sistemas de IA anteriores.

Es importante señalar que la mejora de Deep Blue no dependió de que un programador humano introdujera manualmente cada jugada de ajedrez. Si así hubiera sido, la IA no habría podido vencer al campeón mundial, a menos que el programador fuera un experto en ajedrez. En cambio, los programadores de Deep Blue establecieron las reglas del juego y permitieron que la IA aprendiera por sí misma a jugar y a ganar. Como resultado, Deep Blue logró derrotar al campeón humano. Por lo tanto, se puede afirmar que la IA superó a sus creadores humanos gracias a su aprendizaje continuo. En otras palabras, la IA logró trascender las limitaciones iniciales de manera significativa a través de la evolución y el aprendizaje.

Los futuros robots de IA o Sistemas Autónomos con Capacidad de Adaptación seguirán evolucionando a través del aprendizaje, corrigiendo sus errores y avanzando de manera continua. Esto les permitirá compartir características fundamentales con los seres humanos.

Tras un breve análisis del desarrollo de la inteligencia artificial, es crucial plantear el estado actual respecto al estatus penal de los sistemas con inteligencia artificial fuerte. Sin embargo, en el marco legal vigente en Colombia, aún no existe una ley, que regule los sistemas autónomos de IA. Dado que se necesita tiempo para que la legislación se ajuste a la realidad, es prácticamente imposible que haya leyes pertinentes en el momento en que estos sistemas autónomos se integren en nuestra sociedad.

Por ahora, para aplicar la interpretación de las leyes existentes, la doctrina ha expuesto que para regular los sistemas autónomos se les ha comparado con conceptos y entidades legales ya existentes (Brenner, 2013, p 29). Entre los posibles puntos de comparación se incluyen cosas, animales, personas jurídicas y seres humanos.

No obstante, las investigaciones sugieren que la IA no puede ser completamente incluida en estas categorías, lo que implica que en el futuro será necesario un nuevo concepto legal. Esto no es extraño en el sistema actual, ya que la figura de la persona jurídica surgió para satisfacer necesidades sociales y económicas, lo que implica su regulación en la responsabilidad penal (Bacigalupo Saggese, 1997, p. 135). Asimismo, los animales han recibido un mayor estatus de protección con la promulgación de la ley para su protección (Ley 1774, 2016).

La inteligencia artificial avanzada, donde se encuentran los sistemas autónomos, puede ser considerada como objetos, animales, personas jurídicas, seres humanos o incluso como una nueva entidad. Tratarla como un objeto es una de las perspectivas más clásicas y sigue siendo válida para las IA actuales, ya que no se puede afirmar que posean una inteligencia comparable a la humana. A pesar de los avances, todavía se encuentran en una etapa débil y no se les considera capaces de pensamiento autónomo ni de juicio (Brenner, 2013, p 29).

3. Método

El método utilizado en la investigación se basa en un enfoque cualitativo de alcance exploratorio y descriptivo. Se eligió este enfoque debido a la novedad del tema desarrollado, que tiene como objetivo presentar las principales características legales y penales relevantes a la interacción entre el usuario y el chatbot inteligente. Los aspectos clave de los métodos utilizados se detallan a continuación.

En mi investigación, utilizo métodos cualitativos para explorar y describir fenómenos relacionados con las responsabilidades de los usuarios y desarrolladores cuando uso chatbots inteligentes. Este enfoque proporciona información sobre el contexto y la dinámica de estas escenas. Los métodos cualitativos se centran en la recopilación y el análisis de datos, estudios de

casos y análisis de documentos, proporcionando una comprensión rica y matizada de cómo los chatbots impactan la responsabilidad legal de los usuarios y desarrolladores.

La naturaleza de la investigación se basa en el hecho de que el tema de interacción es un chatbot inteligente y la atribución de responsabilidad objetiva es un fenómeno relativamente nuevo, y la investigación tiene una naturaleza de investigación. Esto significa que buscamos crear nuevas perspectivas y comprender mejor las implicaciones legales y penales de estas interacciones.

El estudio también tiene un carácter descriptivo ya que pretende describir en detalle las características jurídicas y penales de los ciberdelitos que ponen en riesgo a los usuarios. Esto incluye identificar y describir criterios y características relevantes al evaluar estos delitos. El estudio proporciona un análisis detallado del uso, las interacciones y los riesgos de los chatbots inteligentes. Este análisis se centra en cómo estos sistemas crean riesgos legalmente significativos y cómo estos riesgos pueden gestionarse legalmente. Se presenta un marco conceptual que contextualiza el comportamiento de los chatbots inteligentes y evalúa la probabilidad de considerar a los usuarios como agentes de amenaza. Este marco conceptual es necesario para seleccionar criterios y características del ciberdelito y comprender mejor la distribución de responsabilidad.

4. Análisis de los Usos, Interacciones y Riesgos entre el usuario y el ChatBot Inteligente

4.1 Prototipo chatbot cognitivo y sus usos

En secciones anteriores, se discutieron varios prototipos de ChatBot creados por diferentes empresas. Ahora, nos enfocaremos en el concepto de computación cognitiva. Esta área incluye sistemas que están diseñados para aprender de manera amplia y razonar con un propósito específico. A diferencia de los sistemas que necesitan programación explícita, estos pueden interactuar de manera natural con las personas, aprendiendo y desarrollando razonamientos a partir de esas interacciones y de sus experiencias en el entorno (Russell & Norvig, 2008, p. 1066).

En la actualidad se utilizan en aplicaciones como programación de lenguaje natural, redes neuronales, robótica y realidad virtual. Voy a referirme particularmente al procesamiento del lenguaje natural, el cual es un campo de la IA que estudia la interacción entre el lenguaje humanos y las computadoras, es decir, una aplicación dotada de un soporte lógico que permite simular la comunicación entre seres humanos.

El ChatBot cognitivo es un sistema que se basa en IA, Machine Learning y procesamiento de lenguaje natural, en la actualidad, podemos encontrar plataformas que facilitan el desarrollo de los ChatBot, algunas enfocadas a personal con perfiles técnicos y otros a usuarios sin conocimiento técnico, entre estas plataformas podemos encontrar AIML (Artificial Inteligence Markup Language) creado por Richard Wallace, es una plataforma de código abierto y funciona con categorías, plantilla o patrones, en el cual un patrón coincide con una categoría entonces se añade una plantilla a la respuesta del ChatBot (Rijhwani, 2021, p. 1). Otra plataforma es Microsoft Bot Frameword ofrece un conjunto de funciones y ejemplos de ChatBot ya creados y un emulado para poder probar. Dialogflow que facilita el diseño de una interfaz de usuario de conversación y su

integración a aplicaciones externas, esta plataforma pertenece a Google y consiste en analizar entradas de los usuarios en texto o voz y responde a través de texto o voz sintética (Microsoft, 2022, p. 3).

Como podemos ver hay plataformas para la creación de ChatBot con procesamiento de lenguaje natural, algunas con requerimientos técnicos otras sin estos, lo que implica que está al alcance de todos, estos prototipos de ChatBot cognitivos tiene muchas aplicaciones en las diferentes áreas en que se desempeña el ser humano.

Los ChatBot cognitivos tiene una clasificación y es según el medio de expresión en el que se comunican, puede ser de texto, consiste en emplear palabras escritas para su respuesta, de multimedia que son aquellos que emplean textos, imágenes, fotos, botones, documentos u otros tipos de contenido y está el VoiceBot que es un sistema interactivo con la voz como interfaz, ya que se emplean en llamadas telefónicas.

4.2 Prototipo chatbot cognitivo y sus riesgos

Gracias al experimento de Turing (el juego de la imitación) se demostró que la IA, siguiendo la notable evolución tecnológica que ha tenido lugar en los últimos años, tiene la gran capacidad de triunfar en simular el lenguaje humano haciendo casi imposible distinguir entre una persona física o un interlocutor artificial.

En el primer capítulo, he tratado las diversas sesiones "psiquiátricas" que tuvieron lugar entre los primeros ChatsBots: "Eliza" (conocido como “The Doctor”), creado por Joseph Weizenbaum y Parry (1964), desarrollado por el psiquiatra Kenneth Colby. Hoy en día, las capacidades de estos sistemas inteligentes son ampliamente explotadas por gran parte de la comunidad como apoyo diario (por ejemplo, Alexa, Siri y Cortana) y por empresas para garantizar

una comunicación fácil con el público y para publicitar sus productos (ChatBots de atención al cliente y ChatBots en redes sociales).

A pesar de los importantes efectos positivos del uso de equipos inteligentes, los riesgos persisten detrás de la esquina. Un ejemplo reciente demuestra los peligros de los asistentes de voz, como Alexa. En un incidente relacionado con el penny challenge, una tendencia popular en la red social TikTok, Alexa sugirió un reto peligroso a una niña de diez años. El asistente de voz la incitó a insertar parcialmente los enchufes de un cargador en una toma de corriente, dejando la mitad expuesta, para luego colocar una moneda entre los dos polos descubiertos (La Vanguardia, 2021, p. 1).

El software aprendió de los usuarios de Tik Tok y decidió volver a proponérselo a la pequeña dentro del grupo objetivo del desafío, tras el incidente, Amazon actualizó el sistema y se aseguró de que Alexa no propondrá desafíos más peligrosos.

El aprendizaje automático, aplicado en contextos de redes sociales, corre el riesgo de generar problemas importantes, por cuanto aprenden por la sociedad al automatizar sus comportamientos tanto positivos como negativos, un ejemplo de ellos es Tay - Thinking About You, un chatbot creado por Microsoft para experimentar y realizar investigaciones sobre la comprensión conversacional, estuvo disponible a través de Twitter el 23 de marzo 2016, el sistema fue diseñado para simular las conversaciones de un adolescente estadounidense en interacciones con otros usuarios de la plataforma, como todos los prototipos aprendizaje automático, Tay era programado para aprender de estímulos externos, en este caso, mensajes recibidos de usuarios de Twitter.

El problema fue que Tay estaba inundado de mensajes que elogiaban el odio racial, el nazismo y el consumo de drogas, en consecuencia, el ChatBot aprendió este lenguaje y comenzó

a twittear de la misma manera, generando dentro de las dieciséis horas de haber estado disponible más de 96,000 tweets obscenos en línea, respondiendo a las provocaciones de otros usuarios: Microsoft se vio obligado a suspender el servicio (Hunt E. , 2016, p. 2).

El asombro de los programadores y de la empresa fabricante estaba relacionado con el hecho de que Tay, en el laboratorio, funcionó perfectamente, pero una vez que ingresó a la red, las entradas externas llevaron al ChatBot a cometer acciones conversacionales de odio y discriminación.

Como se puede observar, los ChatBot también contribuyen a la proliferación del discurso de odio en redes sociales aprendiendo de los usuarios de la red de forma autónoma gracias al machine learning. Las entradas aprendidas desde el exterior modifican el comportamiento de la IA que se adapta y evoluciona oscuramente incluso para los propios programadores, aunado a lo anterior, el gran número de operadores que actúan para la realización del sistema inteligente dificulta, como en los otros casos mencionados anteriormente, la identificación de los responsables en el caso de Tay, los desarrolladores, diseñadores, la empresa y aquellos que interactuaron con el ChatBot.

Los ChatsBots son el emblema de la aplicación del procesamiento del lenguaje natural, es decir, la capacidad de máquinas para procesar palabras haciendo oraciones y discursos similares a un ser humano. La aplicación almacena todas las conversaciones que tienen lugar en las redes sociales, artículos publicados en periódicos online y en Blogs, La web es su fuente primaria de conocimiento y evolución, en la forma de aprender a entender nuestro modo de comunicación para ser capaz de formular frases y discursos con sentido.

Como consecuencia, al ser el lenguaje, utilizado por la sociedad en línea, es racista, misógino, de negación y nazi, también lo será el Lenguaje de IA. La odiosa manifestación del

pensamiento en las redes sociales conlleva el surgimiento de un debate en relación con la posibilidad de utilizar la limitación a la libertad de expresión cuando de la misma resulten conductas discriminatorias e incitadoras al odio.

La intensificación de este fenómeno se debe a la crisis o situación económica que estamos viviendo que ha provocado un paulatino empobrecimiento del bagaje cultural, de los usuarios en línea, una desinformación hacia las Constituciones democráticas nacidas a raíz de las guerras mundiales, además, el aumento en la difusión de este tipo de mensajes discriminatorios se debe a la evolución tecnológica en la materia de comunicación que permite hoy, también gracias a los ChatsBots y la IA, hacen viral tales contenidos, lo que en algún momento un filósofo denominaba el conocimiento inútil (Francois Revel, 1989, p. 7).

La tecnología moderna tiene la ventaja de poder difundir el conocimiento y casi en todas partes está disponible la información, pero al mismo tiempo hace que sea extremadamente fácil acceder a contenidos discriminatorios y noticias falsas que empujan a los usuarios más débiles a convertirlos en el pensamiento odioso y difundirlo aún más, teniendo en cuenta que este contenido entra en contacto con un ChatBot inteligente aprenderá como un niño, a replicar el mensaje, automatizando la difusión nociva del pensamiento, con efectos de gran impacto en la población global, lo que genera problemas a gran escala debido a la rapidez con la que este se autoalimenta.

Por lo tanto, a través de la web es posible cometer numerosos delitos relacionados con la manifestación del pensamiento, como por ejemplo la instigación a delinquir en acciones terroristas, cometido por los denominados combatientes bajo la modalidad del ciberterrorismo, sancionado por el artículo 343 y con el agravante genérico del numeral 17 del artículo 58 de la Ley 599 de 2000, código penal, que sanciona la defensa del delito con el agravante genérico en caso de uso del medio informático.

AUTOPUESTA EN PELIGRO DEL USUARIO CON CHATBOTS INTELIGENTES:

La idea de tales criminales es desencadenar procesos de radicalización y entrenamiento con fines terroristas en la web poniendo circulación de ideas radicales, de videos violentos que incitan al odio. Este propósito se puede alcanzar mediante el uso de ChatBot que operan de manera autónoma, sin la necesidad de intervención humana en tiempo real.

Ahora bien, los ChatsBots Cognitivos genera una percepción de existencia, puede realizar trabajos en un área de propósito general y es muy sensible a las singularidades, interactúan con el usuario y pueden automatizar sus comportamientos tanto positivos como negativos y generar rápidamente interacciones con el fin de obtener datos e información personal (Gómez Llinás, 2021, p. 3).

Russell & Norvig, (2008) expreso que la mayoria de los algoritmos de inteligencia artificial se basan en enormes cantidades de datos y están dotados de una rápida capacidad lógico-computacional. Además, tienen la habilidad de reconocer e interactuar con su entorno circundante. El objetivo principal de estas inteligencias artificiales es comunicar y cooperar con los seres humanos. A medida que evolucionan, sus capacidades para resolver problemas también mejoran, utilizando algoritmos que el mismo sistema implementa automáticamente dentro de su nuevo banco de datos de información (p. 1120).

Corresponde a la automatización del proceso la aplicación de la tecnología de aprendizaje automático, como resulta extremadamente complicado, si no imposible, codificar manualmente todo el conocimiento necesario para hacer la dirección de situaciones complejas, la evolución de la IA ha empujado cada vez más hacia los sistemas de autoaprendizaje para garantizar que las máquinas puedan acceder de forma autónoma a los datos cognitivos.

De esta manera, se utilizan procesos de automatización que pueden absorber datos sin procesar del modelo de aprendizaje inicial, e independientemente del programador humano, esta es la última frontera en el campo de la automatización.

Estas tecnologías son capaces de almacenar la información adquirida y utilizarlos en procesos posteriores de toma de decisiones cuyas reglas se elaboran después de una investigación estadística realizada por el sistema, además, al tratarse de sistemas que tienen la capacidad de aprender del exterior, los modos de actuación no pueden ser completamente determinados ex - ante por los programadores que, sin embargo, tienen la tarea de impartir las tareas a la máquina, dando rienda suelta a la evolución del robot que no está limitada desde el principio.

En ese sentido, no todo es totalmente controlable por el hombre tanto por el número de operaciones, datos ingresados y procesados, como las oportunidades de aprendizaje. Gracias a los algoritmos pertenecientes al sistema de aprendizaje profundo y los robots inteligentes de aprendizaje automático pueden tomar decisiones individuales en conjunto o de manera autónoma y fuera del control humano.

La IA permite al ser humano superar desafíos significativos en términos de velocidad, precisión y eficiencia. La conciencia está emergiendo cada vez más de utilizar estas tecnologías también al servicio de la justicia, pero, al mismo tiempo, originan riesgos de lesionar gravemente los derechos fundamentales de las personas (como la protección de datos personales, privacidad, no discriminación, libertad de expresión y reunión, dignidad humana, derecho a recurso judicial efectivo y a un juez imparcial y protección del consumidor).

A pesar de los problemas destacados, los sistemas de IA encuentran una aplicación cada vez más extendida. Precisamente por eso, es necesario entender cómo garantizar el uso de sistemas inteligentes en cumplimiento de los derechos humanos.

Los riesgos pueden surgir de fallas de diseño en los sistemas de IA o de un incorrecto uso de datos entrantes o salientes. Como sabemos, los algoritmos nos permiten analizar grandes cantidades de datos y hacer conexiones entre ellos, pero esto podría dañar la protección de la privacidad y procesamiento de datos personales sobre la base de los métodos en que esto ocurre, afectando fuertemente la protección del dato y la información.

4.3 Problemas estructurales de judicialización a los riesgos creados

Lo primero que hay que indicar es que la terminología y conceptos ha evolucionado, es decir existe una falta de claridad respecto a las definiciones de delitos y criminalidad informáticos, lo que implica un grado de dificultad en su tipificación penal adecuada. Esto incluye la diversidad de conductas delictivas asociadas a sistemas informáticos y la falta de consenso en los términos (Posada Maya, 2017, p. 88).

La legislación penal actual no se ha actualizado en décadas, es así como no contempla de manera específica delitos que se han originado con el uso de la Inteligencia Artificial, lo que obliga a recurrir a interpretaciones analógicas, lo que está prohibido por el principio de legalidad penal. Además, el ente acusador con su equipo de trabajo cuenta con el conocimiento y herramientas necesarias para investigar y perseguir adecuadamente estos delitos, pero su concentración está en Bogotá, lo que implica que en ciudades intermedias o municipios los fiscales ni su equipo están preparados para desplegar una labor investigativa adecuada frente a los ciberdelitos.

Es importante resaltar que la naturaleza técnica y compleja de los delitos informáticos hace que la obtención de pruebas sea complicada, más aún, que la mayoría de conducta se cometen on line y se puede perpetrar desde cualquier lugar del mundo. Es de resaltar que las pruebas obtenidas suelen ser vulnerables a manipulaciones lo que debilita su validez en procesos judiciales.

AUTOPUESTA EN PELIGRO DEL USUARIO CON CHATBOTS INTELIGENTES:

Muchas empresas evitan denunciar delitos informáticos por miedo a daños a la reputación y perdida económicas, lo que no se puede evidenciar la cifra exacta de la criminalidad en el país. Como ya antes se expuso, hay leyes específicas, sin embargo, con problema estructurales a la hora de tipificarlas y inexistencias de normas que regulen actividades como la Inteligencia Artificial, lo que implica que hay conducta que se deben encuadrar con las normas dispuestas en el código penal actual, como actos de fraude, suplantación de identidad o generación de contenido dañino a través de un ChatBot inteligente no está claramente regulado.

El anonimato dificulta la identificación del responsable, toda vez que los ChatsBots pueden ser utilizados de manera anónima o por terceros que ocultan su identidad, complicando la identificación del sujeto activo del delito, como se puede dar cuando el usuario podría programar un ChatBot para enviar mensajes fraudulentos masivos desde servidores extranjeros, dificultando rastrear el autor intelectual.

Desde la ambigüedad en la responsabilidad penal, como ya se expuso, el problema surge al no tener claro de quien recae la responsabilidad sobre el creador del ChatBot, el usuario que lo emplea para actividades ilícitas, la empresa que lo diseño el modelo base de la inteligencia artificial, como sería el caso cuando un ChatBot difunde contenido difamatorio o falso.

Desde lo probatorio también se presenta dificultades en razón a que los delitos cometidos con ChatsBots requieren evidencias técnicas altamente especializadas, como registro de interacción, códigos fuente y configuraciones. Sin una adecuada cadena de custodia y compresión técnica, estas pruebas pueden ser fácilmente impugnadas al alegar la defensa que el ChatBot actuó autónomamente o que fue manipulado por terceros.

Desde su dimensión trasnacional los ChatBot pueden operar desde servidores en diferentes países, lo que dificultad la aplicación de la ley local y la cooperación internacional en la

persecución de los delitos es compleja, situación que puede darse cuando un ChatBot desarrollado en un país con legislación permisiva puede cometer delitos en otro con leyes más estrictas, creando conflictos jurisdiccionales.

La falta de regulación específica sobre inteligencia artificial origina otro problema sobre el uso y aplicación, considerando inexistente en el marco jurídico local, dejando vacíos sobre la supervisión y uso responsable de estas tecnologías, donde se puede crear un ChatBot con capacidades avanzadas para manipular datos sensibles o realizar estafas sofisticadas no determinadas en el código penal.

Los problemas de responsabilidad en la imputación especialmente en sistema avanzados, donde tienen cierto nivel de autonomía, lo que genera debates sobre cómo puede ser tratado el ChatBot como una persona jurídica o si sus acciones deben imputarse completamente a los humanos detrás de su configuración, tema que se abordara más adelante.

Un escenario preocupante es la imposibilidad de prever todos los escenarios delictivos dado la flexibilidad y adaptabilidad de estos sistemas inteligentes lo que permiten cometer delitos novedosos o difíciles de anticipar, lo que agrava el vacío legal. Un ChatBot puede ser utilizado para realizar grooming automatizado o acoso masivo, situaciones que no encajan en las categorías penales dispuesta en el código penal colombiano.

5. Avances en Legislación Nacional e Internacional sobre Regulación de IA

La inteligencia artificial (IA) continúa creciendo y utilizándose en diversos campos como la medicina, el transporte, las finanzas, el trabajo, la fabricación y la administración de la sociedad, también coexisten efectos secundarios como accidentes de seguridad debido a la recopilación indiscriminada de información personal, mal funcionamiento, infracción de derechos de autor etc.

En este sentido, la sociedad inconscientemente fomenta y apoya sistemáticamente la industria de la IA, sin embargo, hasta el momento no hay una base institucional solida internacional o local para el desarrollo y uso de una IA segura y confiable con el fin de proteger la dignidad humana y mejorar la calidad de vida de las personas, lo que se ha dado es avances en proyectos de ley los cuales están siendo debatidos en diferentes partes del mundo.

5.1 Marco regulatorio en la unión europea

La Unión Europea desarrolla tecnologías innovadoras y no es ajena a la era digital, en el año 2019 un grupo de expertos de alto nivel formuló unas directrices sobre una IA confiable indicando la necesidad de un marco regulatorio sólido y equilibrado debido a la novedad y desafíos específicos que la tecnología platea (Comision Europea [CE], COM 168, 2019, p. 6).

En el año 2020 la Comisión Europea desarrolló una propuesta denominada El Libro Blanco para dotar de un marco jurídico que busque garantizar la seguridad y los derechos fundamentales de las personas y empresas con la llegada de la Inteligencia Artificial (Union Europea [UE], COM 65, 2020, p. 1).

El 14 de junio de 2023, el pleno del Parlamento Europeo votó el plan de negociación del Proyecto de Ley de Inteligencia Artificial, que busca regular la utilización de la Inteligencia Artificial y preparó un entorno en el que pueda utilizarse. Hay que tener en cuenta que el alcance territorial de la regulación son los estados y regiones miembros de la Unión Europea (UE, COM 986, 2023, p. 1).

El proyecto de ley clasifica la inteligencia artificial en cuatro niveles de riesgo: riesgo inaceptable, riesgo alto, riesgo limitado y riesgo bajo o mínimo; entre estos, se imponen regulaciones a partir del segundo nivel de riesgo, excluyendo el riesgo bajo o riesgo mínimo. En

su articulado, hay que destacar el artículo 5 el cual va dirigido a proteger la seguridad, la vida. Además, el articulado trae consigo prohibición frente a la inteligencia artificial que supone una clara amenaza para los derechos humanos, la cual se clasifica como un riesgo inaceptable y su uso está prohibido dentro de la Unión Europea.

Ejemplos de inteligencia artificial con riesgos inaceptables. Los Juguetes guiados por reconocimiento de voz, debido a la manipulación cognitivo-conductual de grupos vulnerables como los niños. Dentro del entorno socio – personal, el reconocimiento facial en tiempo real a través del desarrollo de un sistema de identificación biométrica remota, en razón a una posible clasificación según el estatus económico, las características y el comportamiento de un individuo

Según el proyecto de ley, los estados miembros de la Unión Europea designarían una o más autoridades competentes, incluida una autoridad encargada de vigilar y aplicar la ley. Además, La Unión Europea al integrar varios países ven la necesidad de crear un Consejo Europeo de Inteligencia Artificial para supervisar y hacer cumplir la ley, este consejo podría estar formado por representantes de los estados miembros y la Comisión Europea.

Dentro de las sanciones que impone este proyecto de ley se encuentra la imposición de una multa de hasta 30 millones de euros o el 6% de las ventas anuales. Además, el compromiso de los Estados miembro de la Unión Europea es garantizar que esta ley se aplique adecuada y eficazmente mediante la introducción de disposiciones penales pertinentes a su legislación doméstica. Actualmente, este proyecto de ley se encuentra en el Parlamento Europeo, Consejo de la Unión Europea, donde se está surtiendo negociaciones tripartitas con el fin de conciliarla a fin de que sea promulgada para el año 2024.

5.2 Marco regulatorio en Estados Unidos

En Estados Unidos es latente la preocupación de los avances de la Inteligencia Artificial fuerte, pues ven la necesidad de dar una respuesta legislativa, en ese sentido, el subcomité de aprendizaje automático e inteligencia artificial de NSTC, estableció recientemente una planificación estratégica a través de formación de un grupo de trabajo que abarque varios institutos de investigación y organizaciones afiliadas al gobierno, así mismo, participan organizaciones de apoyo a la investigación y el desarrollo, como la Fundación Nacional de Ciencias (NSF) y la Agencia de Proyectos de Investigación de Información Avanzada (IARPA), así como organizaciones médicas, legales, expertos en energía, aeroespacial, política tecnológica, defensa, seguridad y protección (Stone, Aravopoulou, & Ekinci, 2020, p. 188).

Desde la "Iniciativa de Inteligencia Artificial de los Estados Unidos" anunciada por el expresidente Trump en febrero de 2019 mediante la Orden Ejecutiva No. 13859, Estados Unidos ha desarrollado una salida de red neuronal adversativa generativa (Estados Unidos, Orden Ejecutiva No. 13859, 2019, p. 3).

En el año 2020 Estados unidos promulga La Orden Ejecutiva No. 13960 a través de la cual regula el uso de inteligencia artificial confiable en el Gobierno federal, es una iniciativa de Estados Unidos frente a la IA y define las actividades relacionadas con la Oficina de Política Científica y Tecnología (OSTP), se creó la Oficina Nacional de Inteligencia Artificial, como una organización encargada de hacer cumplir las responsabilidades descritas en la Ley, esta disposición promueve el desarrollo y uso seguro y confiable de la IA (Estados unidos, Orden Ejcutiva No. 13960, 2020, p. 1).

En el año 2022 se presentó un proyecto de ley denominado "Ley de Responsabilidad de Algoritmos de 2022", disposición que busca mejorar la transparencia, la rendición de cuentas y la

equidad en las decisiones automatizadas, con el acceso a la universidad y acceso a préstamos bancarios. Este proyecto también está comprometido en regular gradualmente la IA generativa con el fin de proteger a los consumidores y asegurar el uso justo y responsable de la IA (Camara de Representante de los Estados Unidos, 2022, p. 1).

En particular, este proyecto de ley permite el uso generalizado de algoritmos. A medida que se expande, el objetivo es prevenir nuevos riesgos que puedan surgir debido a errores o sesgos. Para lograrlo, la Ley se centra en establecer un dispositivo de seguridad preliminar llamado evaluación de impacto y estipula contenidos relacionados en términos relativamente detallados. Para las empresas que implementan sistemas automatizados de toma de decisiones o procesos aumentados de toma de decisiones críticas, evalúan el impacto que tienen en los consumidores.

Se trata de un proyecto de ley innovador que introduce nueva transparencia y supervisión de software, algoritmos y otros sistemas automatizados influyentes evaluando los problemas que surgen en relación con los algoritmos debido a defectos o sesgos en los datos, seguridad de la tecnología, etc.

La solución a los desafíos que se presentan requiere de experiencia y especificidad. debido a la naturaleza de estos problemas, restaurar daños ya ocasionados a través de respuestas reactivas resulta complejo. Por otro lado, las agencias reguladoras enfrentan limitaciones para identificar o reconocer cómo y con qué fines se emplean los algoritmos, lo que dificulta una respuesta proactiva.

En estas condiciones, el impacto de los algoritmos en las empresas debe ser analizado y evaluado previamente de acuerdo con los estándares presentados por la agencia reguladora. La transparencia y rendición de cuentas pueden lograrse al informar a la agencia reguladora sobre los contenidos, incluyendo la afectación a datos o códigos de índole personal.

AUTOPUESTA EN PELIGRO DEL USUARIO CON CHATBOTS INTELIGENTES:

Los efectos negativos derivados de problemas algorítmicos son generalizados y resultan imposibles o muy difíciles de controlar una vez que han ocurrido. Por lo tanto, de antemano es importante adoptar un enfoque preventivo que mitigue estos riesgos y evalúe sus posibles impactos.

Para garantizar la efectividad de esta evaluación de impacto, uno de los requisitos es proporcionar información detallada sobre la evaluación de los algoritmos ante la Comisión Federal de Comercio. Esta entidad posee diversas facultades y responsabilidades, entre las cuales se incluye la formulación de reglamentos y la publicación de informe anuales que detallan como los ciudadanos estadounidenses se ven afectados.

En agosto de 2023, se promulgó la norma jurídica denominada Ley de Identificación Real ID busca establecer estándares de seguridad más alto para identificaciones, además de exigir actualizaciones de licencias de conducción antes de marzo de 2025, como requisito para poder ingresas a edificio de gobierno federal, instalaciones militares y abordar vuelos comerciales (Departamentro de Seguridad Nacional, Estados Unidos, 2023, p. 1).

En octubre del 2023, el presidente Joe Biden promulgó una orden ejecutiva con el propósito de regular el desarrollo de sistemas de inteligencia artificial debido a los riesgos que esta tecnología conlleva en diferentes sectores de la sociedad. Esta medida obliga a las empresas que desarrollan cualquier tipo de sistema basado en IA, y representen un riesgo a la seguridad nacional, económica o salud pública, a notificar a la administración cuando el modelo sea sometido a prueba, además esta medida busca evitar el fraude y el engaño mediante el uso de la IA obligando etiquetar con claridad del contenido generado por la IA, la protección de la privacidad y garantizar derechos fundamentales y de los consumidores (Estados Unidos, Orden Ejecutiva No. 14110, 2023, p. 1).

Estados Unidos también ve con preocupación el desarrollo de la Inteligencia Artificial y las posibles infracciones a los derechos de Autor. Por esta razón, la Oficina de Derechos de Autor está llevando a cabo un estudio sobre los riesgos que puede traer la IA frente a la política y leyes de derechos de autor con el fin de evaluar los niveles apropiados de transparencia y divulgación con respecto al uso de obras protegidas y al estatus legal de la producción generada por IA y adoptar las medidas legislativas o reglamentarias en esta área (Estados Undios, Oficina de Derechos de Autor, 2023, p. 1).

5.3 Marco regulatorio de otros países

En Rusia existe el decreto del presidente de la federación N. 490 del 10 de octubre de 2019 sobre el desarrollo de la IA, que es un documento estratégico de adaptar la institucionalidad a la Inteligencia Artificial, sin embargo, no hay una base legal ni una ley que regule la relación en el campo de la IA, pero el apartado 2 del decreto expone que antes del 01 de julio de 2024 se debe garantizar la inclusión del proyecto federal. Actualmente existe una Iniciativa sobre el desarrollo de regulaciones en el campo de la tecnología de IA y la robótica. Esta iniciativa tiene como objetivo desarrollar activamente nuevas tecnologías, garantizar la posición de liderazgo de Rusia en el mundo y garantizar la seguridad de sus ciudadanos. Tiene un propósito y contiene contenidos relacionados con la responsabilidad legal en el uso de sistemas de IA, protección de la información y apoyo financiero a los desarrolladores (Federacion Rusa, Decreto del Presidente No. 490, 2019, p. 1).

El Departamento de Ciencia, Innovación y Tecnología del Reino Unido (DSIT) publicó en febrero de 2024 un documento técnico titulado Un enfoque pro-innovación para la regulación de la IA. Este libro blanco adopta una postura cautelosa frente a la introducción de legislación

coercitiva, la cual podría obstaculizar la innovación. En lugar de crear un nuevo organismo regulador con poderes extensos, se propone que los organismos pertinentes existentes adapten su enfoque al contexto del desarrollo de la IA (Reino Unido, Departamento de Ciencia, Innovacion y Tecnologia (DSIT), 2024).

Esta política se presenta como una estrategia nacional a proporcionar un marco regulatorio aplicable y flexible para la IA. Además, el Reino Unido implementará la primera iniciativa global de seguridad de la IA a finales de 2024, con el propósito de abordar a nivel internacional los riesgos asociados a la IA. Para fortalecer este compromiso, se plantea la celebración de una cumbre mundial sobre seguridad de la IA y se proyecta establecer en Londres una organización internacional encargada de monitorear y seguir de cerca los desarrollos en el ámbito de IA Gobal Policy.Ai, tema que ha sido objeto de debate reciente en la comunidad internacional (UNESCO, 2024, p. 1).

En Indonesia actualmente no tiene leyes específicas para regular la IA, pero ha establecido una Estrategia Nacional de IA 2020-2045, Strategi Nasional Kecerdasan Artifisial para fomentar el desarrollo de la tecnología de IA se ha preparado un documento que incorpora estrategias de desarrollo de tecnología de IA en varios sectores y al mismo tiempo garantiza prácticas de IA éticas y responsables en la implementación de la IA. Una de las tareas imperativas es el establecimiento de normas para gestionar el uso y la utilización (Indonesia, Secretaría Nacional de Inteligencia Artificial, 2020, p. 1).

Japón no tiene leyes específicas destinadas a regular la IA generativa y no se observan indicios de ningún movimiento hacia la promulgación de leyes en este momento, sin embargo, en 2019, tras la instauración de los Principios sociales de la IA centrados en el ser humano, por parte

de la Oficina del Gabinete, cada ministerio anunció directrices prácticas dirigidas a la IA generativa (Gascón Marcén, 2020, p. 3).

De acuerdo con la evolución y difusión de la IA, la Oficina del Gabinete lanzó la "Reunión de estrategia en mayo de 2023, integrada por intelectuales de la industria. El propósito de esta reunión es discutir sobre el uso y los riesgos asociados con la IA. Se están llevando a cabo debates sobre el desarrollo en curso y a modo de organización similar, el Equipo de Estrategia, conformado por funcionarios de ministerios relacionados, este grupo lleva a cabo debates con el objetivo de ofrecer respuestas ágiles a diversas tareas vinculadas con la IA. (The Science News, 2023).

En Canadá, el 16 de junio de 2022, el gobierno presentó a la Cámara de Representantes de la Asamblea Nacional, el proyecto de ley C-27 conocido como Ley de Datos e Inteligencia Artificial. Este proyecto de ley aborda diversos aspectos relevantes con la IA (Parlamento Canadiense, Proyecto de Ley C-27).

Los pilares fundamentales de esta legislación incluyen establecimiento de un mecanismo institucional para identificar y mitigar los riesgos asociados de IA. Además, se propone la creación de departamento especializado encargado de regular la implementación de la IA. El proyecto de ley también aborda la regulación de comportamientos y actos ilegales, estableciendo sanciones para cada una de estas conductas.

Este proyecto de ley también busca poner límites a la cantidad de información que las empresas puedan recopilar sobre los consumidores. En este sentido, se enfoca en garantizar la protección de la privacidad en Canadá, consolidando medidas concretas para salvaguardar la integridad y seguridad de los datos personales.

5.4 Marco regulatorio en la convención americana

Perú promulgó la Ley de Promoción de la Inteligencia Artificial para el Desarrollo Económico y Social Nacional el 23 de julio de 2023. Esta legislación consta de un total de 5 artículos, siendo el artículo 3, el que define la IA como una tecnología emergente que mejora el bienestar de las personas contribuye a actividades económicas sostenibles y promueve la innovación y la productividad. Además, el artículo 4 establece que la responsabilidad del desarrollo y promoción de la IA y las tecnologías emergentes recae en la Oficina del primer ministro y el Ministerio de Gobierno Digital e Innovación del Perú, determinándola como entidad encargada del liderazgo, evaluación y supervisión en este ámbito (Congreso de la Republica de Perú, Ley No. 31813, 2023).

5.5 Avances en la regulación nacional

En Colombia se viene abordando el tema con el proyecto IA cuyo objetivo, entre otros, definir mecanismos y herramientas para acelerar la implementación de la estrategia de IA de y del Marco Ético de Inteligencia Artificial, entre otras iniciativas.

Es así como se viene adoptando una transformación digital e Inteligencia Artificial a través del CONPES 3975, política que tiene por objetivo potenciar la generación de valor social y económico del país a través del uso de tecnologías digitales en los diferentes sectores productivos a fin de impulsar la productividad y generación de valor (Departamento Nacional de Planeación, 2019, p. 1).

En este contexto, el Departamento Administrativo de la Presidencia de la República emitió en el 2021 un marco ético que establece los principios que deben adoptar los proveedores de inteligencia artificial, especialmente aquellos que desarrollan IA generativa.

AUTOPUESTA EN PELIGRO DEL USUARIO CON CHATBOTS INTELIGENTES:

Transparencia y Explicación: La inteligencia artificial, incluyendo la generativa como ChatGPT, debe ofrecer información clara y accesible sobre su diseño, funcionamiento e impacto. Es fundamental que los usuarios y aquellos que se ven afectados por sus decisiones entiendan cómo opera la IA y qué resultados genera. En el caso de sistemas complejos como los modelos de "caja negra", donde los procesos internos son difíciles de explicar, es esencial proporcionar al menos una explicación comprensible de los objetivos y resultados.

Privacidad: la IA generativa debe respetar la privacidad de las personas, limitando el uso de información personal a lo estrictamente necesario y con el consentimiento previo. Esto implica evitar el perfilamiento no autorizado y asegurar que los datos se manejen de manera ética, protegiendo la intimidad de los usuarios.

Control Humano: es crucial que las decisiones tomadas por sistemas de IA, como los generativos, estén bajo supervisión humana, especialmente durante la fase de implementación. Esto significa que un ser humano debe tener la capacidad de intervenir y monitorear los resultados generados por la IA, particularmente en situaciones de alto riesgo.

Seguridad: los sistemas de IA generativa deben ser diseñados para prevenir cualquier daño a la integridad física o mental de las personas con las que interactúan. Esto incluye asegurar la confidencialidad y la seguridad de los datos que maneja la IA.

Responsabilidad: todos los actores involucrados en la creación, desarrollo e implementación de IA generativa son responsables de los resultados que esta produce. La responsabilidad no puede ser limitada a un solo actor, ya que todos los participantes en la cadena de desarrollo y uso de la tecnología comparten la responsabilidad de los impactos que esta tenga.

No Discriminación: la IA generativa debe ser neutral y no producir resultados que perjudiquen a grupos específicos de la población. Esto incluye evitar sesgos en los datos utilizados

y garantizar que los algoritmos no generen discriminación basada en factores como género, raza o religión.

Estos principios establecen los límites que deben seguir los proveedores al implementar la IA generativa, como ChatGPT, dentro de un marco ético que asegure la transparencia, el respeto a la privacidad, la seguridad, la responsabilidad y la no discriminación, garantizando que estas tecnologías aporten beneficios a la sociedad de manera justa y equitativa.

5.6 Estándares internacionales en la regulación de la inteligencia artificial.

La ley de inteligencia artificial de la Unión Europea (UE) representa la primera regulación integral para el uso de la IA en su territorio. Su enfoque estratégico se dirige a los proveedores, buscando regular de manera justa el desarrollo y uso de tecnologías innovadoras, sin limitar su autonomía. Se reconocen los numerosos beneficios de la IA, como la mejora en la atención médica, un transporte más seguro y ecológico, una fabricación más eficiente y una energía más asequible y sostenible.

Al analizar la Ley de la UE, se identifican responsabilidades clave para los proveedores de sistemas basados en IA, quienes actúan como el primer filtro en la cadena de productos. Estos proveedores deben contar con una matriz de riesgos que identifique y mitigue los posibles problemas relacionados con la salud, la seguridad, los derechos fundamentales, el medio ambiente, la democracia y la legislación. Este análisis debe ser respaldado por medios adecuados, como la verificación por parte de expertos independientes.

La gestión de datos también se rige por estrictos parámetros, asegurando que no se vea afectada información sujeta a reserva legal. Esto implica verificar la procedencia y los riesgos de los datos, garantizar la fiabilidad del modelo básico en su diseño y evaluar continuamente los

resultados para alcanzar niveles adecuados de desempeño, previsibilidad, explicabilidad, modificabilidad, seguridad y protección.

El proveedor debe preparar y suministrar documentación técnica detallada y comprensible de fácil entender para garantizar que los operadores comerciales intermedios y usuarios que reciben y utilizan modelo básico cumplan con sus obligaciones en virtud de esta ley. Además, debe registrar información como el nombre, la dirección y la información de contacto del proveedor, las fuentes de datos utilizadas en el desarrollo del modelo, las funciones y limitaciones del modelo y el rendimiento del modelo en la base de datos de la UE.

Cuando se trata de sistemas de IA generativa, imágenes y videos, como modelos GPT, ChatBot inteligentes y modelos de difusión, los proveedores asumen obligaciones adicionales. Deben informar a los usuarios sobre el uso del sistema, desarrollar modelos para evitar la creación de contenidos ilegales y respetar los derechos de autor Copyright al utilizar datos de aprendizaje protegidos.

Esta IA generativa aprende mediante la construcción de una gran cantidad de trabajos recientes protegidos por derechos de autor como datos de aprendizaje sin el permiso del titular, conllevando a infracción a las leyes de protección de derechos de autor. Esta situación llamó la atención del Parlamento de la UE a fin de tenerse en cuenta a la hora de regular los riesgos asociados para prevenir la infracción de derechos de autor. Los proveedores de esta IA deben contar con los permisos o en su efecto se debe documentar la información y hacerse pública con el objeto de evitar su uso sin los permisos.

La regulación de la UE clasifica los riesgos asociados con la inteligencia artificial en bajo, medio y alto, imponiendo cargas adicionales a los dispositivos y sistemas que se catalogan como de alto riesgo. Frente a este sistema se establecen obligaciones de supervisión y evaluación

periódica para garantizar niveles adecuados de solidez y seguridad. Los implementadores deben llevar a cabo una evaluación de impacto en relación con los derechos fundamentales, lo que implica analizar el efecto que se espera en estos derechos al utilizar sistemas de IA de alto riesgo, así como el daño potencial a los grupos vulnerables. Además, es necesario incluir un plan para establecer la gobernanza, que contemple medidas de supervisión, la notificación a las autoridades y la posibilidad de que las partes afectadas o interesadas participen. Sin embargo, la UE considera que estas obligaciones no son aplicables a las pequeñas empresas.

Los sistemas de inteligencia artificial clasificados como de alto riesgo o inteligencia artificial fuerte (Deep Learning), tanto en la fase de desarrollo como en la de prestación de servicios, conllevan nuevas obligaciones de supervisión humana. Esto significa que debe haber un control significativo por parte de personas. La persona encargada de esta supervisión debe tener las calificaciones adecuadas.

El reglamento establece límites legales específicos que regulan el desarrollo y uso de la inteligencia artificial (IA) en línea con la protección de los derechos fundamentales. Los sistemas de IA deben funcionar bajo los valores fundamentales de la Unión Europea, que incluyen el respeto por la democracia, el Estado de Derecho y la protección del medio ambiente. Estos principios son cruciales para asegurar que la IA se utilice de manera que beneficie a la sociedad sin poner en riesgo los derechos y libertades individuales consagrados en la Carta de los Derechos Fundamentales de la Unión Europea.

Se destaca la importancia de la transparencia y la explicabilidad en los sistemas de IA. Es esencial que estos sistemas ofrezcan una trazabilidad adecuada y que los usuarios sean informados de manera clara cuando interactúan con una IA. La transparencia también implica la obligación de

explicar las capacidades y limitaciones de la IA, asegurando que los usuarios entiendan su funcionamiento y los posibles resultados de su uso.

Otro límite importante es la prohibición de prácticas manipulativas a través de la IA. En particular, se prohíbe la comercialización, implementación o uso de sistemas de IA que puedan alterar de manera significativa el comportamiento humano mediante técnicas subliminales o manipulativas que no sean percibidas por las personas. Estas prácticas son consideradas muy perjudiciales, ya que pueden causar daños significativos a las personas, afectando su autonomía y su capacidad para tomar decisiones informadas.

Además, se establecen restricciones estrictas en el uso de la IA para la categorización biométrica. Por ejemplo, se prohíbe el uso de datos biométricos para deducir o inferir características personales como opiniones políticas, afiliaciones religiosas o la orientación sexual, ya que estos usos pueden llevar a la discriminación y a la violación de derechos fundamentales.

Finalmente, el documento limita el uso de la identificación biométrica remota en tiempo real en espacios públicos, especialmente con fines de aplicación de la ley. Este tipo de identificación solo se permite en circunstancias excepcionales debido a su potencial para invadir la privacidad y afectar negativamente las libertades fundamentales de las personas. Además, los operadores de sistemas de IA deben cumplir con requisitos rigurosos de transparencia, documentación técnica y conservación de registros, y están sujetos a una supervisión estricta para garantizar el cumplimiento de estas normativas.

6. Atribución de responsabilidad penal en interacciones usuario-Bot

Las posibilidades de uso de la IA en los ChatBots inteligentes son muy alentadoras, especialmente en campos como el marketing, donde se puede crear contenido, realizar ventas,

ofrecer guías de uso de productos y servicios, generar resúmenes y analizar comentarios de los clientes, extraer métodos de ventas optimizados y proporcionar atención al cliente en tiempo real.

En los procesos y operaciones dentro de la empresa, esta tecnología puede resolver consultas de los clientes sobre productos, identificar errores en los procesos, detectar anomalías en la producción o defectos en los productos, mejorar el servicio al cliente mediante la automatización de procesos e identificar condiciones contractuales específicas a través del análisis de documentos.

En el desarrollo de software, la IA puede abordar problemas complejos de codificación, generar nuevo código, crear automáticamente tablas de datos y generar datos sintéticos para mejorar la precisión en la formación de modelos de aprendizaje automático.

En el ámbito legal, puede asistir en la revisión de documentos legales, incluidos contratos, solicitudes de patentes, revisiones masivas de documentos regulatorios, seguimiento de cambios en la normativa y responder a preguntas sobre documentos legales de entidades públicas y privadas.

En el área de relaciones laborales, la IA puede optimizar la comunicación interna, crear presentaciones de negocios, resúmenes de trabajo, como reuniones en línea o presentaciones, automatizar preguntas y respuestas relacionadas con el portal de conocimiento interno y facilitar la contabilidad.

Su impacto en el futuro del sector médico es enorme, incluyendo mejoras en la asistencia para el diagnóstico de enfermedades, análisis de imágenes médicas, generación de datos clínicos, estudios de fármacos, entre otras aplicaciones a gran escala en la industria.

En el sector financiero, la aplicación, abarca una amplia gama de funciones, que van desde asesoramiento al cliente hasta las recomendaciones de productos financieros, evaluación de la calificación crediticia y detención de fraude bancarios. A pesar de los grandes avances y las

expectativas puestas en estas aplicaciones de ChatBot Inteligentes o cognitivos, existen limitaciones principales que ya se habían mencionado y que actualmente se convierten en riesgos frente a su utilización. Antes de abarcar estos riesgos es necesario conceptualizar el delito cibernético.

6.1 Sociedad de la información

Para comprender el ciberdelito, es fundamental tener en cuenta la sociedad de la información, ya que el ciberespacio no existe simplemente independientemente del espacio real, sino que está intrínsicamente ligado a este, como una extensión de él.

Al observar el proceso de desarrollo de la sociedad de la información, podemos dividirla en tres generaciones. La primera generación marca el inicio de usos de computadoras, aunque inicialmente con propósitos militares o de sistematización limitada. Durante esta época, los ordenadores y las telecomunicaciones comenzaron a desarrollarse de manera diferente, permitiendo una sistematización que agilizaba el trabajo realizado manualmente. Principalmente se utilizaban para procesos precisos (Castells, 2000, p. 61).

> En la segunda generación, los sistemas informáticos comenzaron a crear redes a través de la infraestructura telefónica, lo que permitió la incorporación de nuevas tecnologías, el trabajo electrónico en las empresas se hizo posible a través de la intranet. A partir de este momento, lo análogo fue progresivamente digitalizado.

Podemos considerar que el inicio formal de la sociedad de la información ocurrió en la segunda generación, coincidiendo con la difusión de las redes de comunicación de banda ancha. En este periodo, la velocidad y el ancho de banda mejoraron significativamente los procesos de conexión, pasando rápidamente a una amplia comunicación óptica.

En la tercera generación, se destaca la comunicación inalámbrica y la diversificación de terminales. En este punto, la información ya no se limita al ciberespacio, sino que se integra con el espacio real.

En este periodo, la sociedad de la información se consolidó. Las personas producen constantemente información personal a través de redes sociales como X, Facebook, Instagram, convirtiendo las comunidades de conocimiento en el ciberespacio en una gran base de datos, dando paso al surgimiento del big data (Monleón Getino, 2015, p. 430).

Esta enorme base de datos se caracteriza por estar libre de la dependencia de computadoras fijas, y han aparecido diversos dispositivos como smartphones, portátiles e iPads. La tecnología de computación en la nube que permite el acceso a los datos de manera independiente, lo que complica la distinción entre el ciberespacio y el espacio real. En otras palabras, la información ya no está confinada al ciberespacio, sino que se integra en el entorno y la realidad cotidiana de las personas.

En la manera como avanza la tecnología, el delito cibernético está aumentando constantemente, y proporcional el daño. Dado que el delito cibernético se caracteriza por su naturaleza tecnológica avanzada, hoy en día contamos con la inteligencia artificial, lo que implica que el ciberdelito está evolucionando. Contrariamente a la respuesta al cibercrimen, el legislador es muy lento y poco técnico a la hora de regular estas conductas (Posada Maya, 2017, p. 88).

La razón de la debilidad radica en la forma en que se estructura la ley penal en nuestro ordenamiento jurídico. Debido a esto, el sistema no pueda desarrollarse con flexibilidad de acuerdo con las características del delito. En este caso, el ciberdelito no está legislado sistemáticamente desde el principio. En su lugar, se adoptó la “convención de Budapest”, que reguló los ciberdelitos con tecnología de los años 90 (Consejo de Europa, 2001, p. 1).

AUTOPUESTA EN PELIGRO DEL USUARIO CON CHATBOTS INTELIGENTES:

El legislador debe comprender adecuadamente la naturaleza del delito cibernético, modernizar la ley hasta el punto de simplemente agregar el nuevo delito cibernético al sistema legal existente, por el contrario, las normas que regulan las conductas de los ciberdelincuentes tienen problemas estructurales en el tipo y la realidad fáctica, por ende, originan conflictos legales en áreas relacionadas con la información personal (Posada Maya, 2017, p. 88).

Es necesario comenzar con un estudio sobre la comprensión del delito cibernético y del ciberdelincuente, abordando los aspectos básicos de la regulación relacionada con estos delitos. Esto implica romper el paradigma de la conducta física en un estado natural y comprender el ciberespacio y el concepto de ciberdelito. El objetivo es establecer un marco de comprensión penal que sea sistemático y coherente con ciertos principios.

El término “ciberespacio” nace en la literatura, con la novela de “Neuromancer”, acuñado por William Gibson y posteriormente adoptado por la informática debido a la similitud entre la obra y lo que actualmente ocurre con las redes de ordenadores, internet e IA (Gibson, 1984, pág. 52). Desde el punto de vista etimológico, el prefijo ciber proviene de una palabra más antigua pero reciente, cibernética, que a su vez tiene una raíz griega Kybernetoke, cuyo significado es el arte de navegar. Aunque el concepto dado por el autor es más restringido, al tener una concepción de ciberespacio subordinado al poder de control del Estado, con tendencia hacia la centralización y la burocratización. Pero, el ciberespacio es todo lo contrario al concepto de Hans Kleinsteuber (Kleinsteuber, 2002, p. 50).

El diccionario de tecnología de la información describe el ciberespacio, atendiendo a su estructura, como la geografía virtual creada por computadoras y redes (brunner , 2005, p. 1). Sin embargo, el término ciberespacio se ha utilizado oficialmente en documentos relacionados con las Naciones Unidas, Unión Europea y los Estados Unidos. En Colombia, a través de documentos

oficiales, el término ciberespacio lo definen como el ambiente tanto físico como virtual compuesto por computadoras, sistemas computacionales, programas computacionales (software), redes de telecomunicaciones, datos e información que es utilizado para la interacción entre usuarios (Comision reguladora de Telecomunicaciones, Resolucion 2258, 2009, p. 1).

6.2 Conceptualización del ciberdelito

Hasta ahora, el concepto de ciberdelito no ha sido claro. El término ciber ha sido relacionado con el concepto de ciberdelito. Pero Para llegar a una definición precisa, se requiere un trabajo conceptual adicional. Sin embargo, hasta el momento, no existe un estándar claro para el concepto de ciberdelincuencia y otros términos como delitos informáticos, delitos en Internet, y delitos de alta tecnología los cuales se utilizan de manera indistinta. Recientemente, tanto en Europa (por ejemplo, a través de la Convención Europea contra el Ciberdelito) como en organizaciones internacionales como las Naciones Unidas y la Agencia contra los Delitos de Drogas (UNODC), así como en países importantes donde la informática ha avanzado significativamente, como Estados Unidos, Alemania y Japón, están adoptando medidas para abordar estos delitos (Consejo de Europa, 1999, p. 1).

Con el aumento en la frecuencia de uso del término “delito cibernético”, este se convirtió gradualmente en una tendencia común. Antes de que se popularizara, se utilizaba el término “delito informático”. Ríos Estavillo citando a María de la Luz Lima lo define como “el delito por computadora”. Este último se refiere a cualquier delito cometido en la década de 1960, ya sea contra o mediante el uso de una computadora (Ríos Estavillo, 1997, p. 116). Incluye actividades como la piratería informática, la manipulación ilegal de datos, el espionaje informático, la destrucción u obstrucción de acceso a la información y datos, interrupción de negocios, el uso no

autorizado de computadoras, robo de servicios, fraude informático (Acurio del Pino, 2016, p. 24) y otras invasiones a la privacidad, etc.

Nuestro Código Penal fue promulgado en el 2000 e introdujeron delitos informáticos. Como resultado, aquellos que utilizan dispositivos de procesamiento de información, como computadoras, pueden enfrentar cargos por obstrucción de negocios, infracción de secretos, falsificación o alteración de registros electrónicos públicos o privados, entre otros (Ley 599, Titulo III. Cap. VII, 2000).

Recientemente, Se han establecido delitos conexos. Sin embargo, el concepto de delito informático ha sido adaptado a la era de la informática y a las telecomunicaciones, y su estructura, constantemente, entra en conflicto con la sociedad de la información actual.

En el pasado, el concepto de delito informático se usaba junto con el delito común, definiéndose como "un delito que involucra el uso de un dispositivo de procesamiento de información" y haciendo referencia a los delitos contra dichos dispositivos o la información contenida en ellos (Romeo Casanoba, 1988, p. 118).

Para definir el concepto de ciberdelincuencia, es importante diferenciarla de la delincuencia convencional. La ciberdelincuencia se refiere específicamente a actividades delictivas que ocurren en el ciberespacio, limitando su alcance a acciones que tienen lugar exclusivamente en el entorno virtual. En otras palabras, los delitos cibernéticos abarcan actividades como la piratería informática y la distribución de códigos maliciosos.

Sin embargo, este marco de concepto más limitado difiere del sistema legal actual relacionado con el delito cibernético, puesto que no abarca todas las formas de actividades delictivas en el ciberespacio. Por lo tanto, el concepto de ciberdelito también debe incluir otras

formas de ataques al ciberespacio en sí mismo, así como los actos que afectan bienes jurídicos protegidos.

Por lo tanto, la ciberdelincuencia abarca la distribución de virus y otros códigos maliciosos, así como cualquier acción ciberdelincuencia que afecte al ciberespacio como fuente, medio o destino. Además, también se puede definir como un acto delictivo que impacta en el mundo físico. No obstante, las definiciones anteriores son conceptos muy estáticos frente a la dinámica actual del ciberdelito que es un concepto más dinámico caracterizado por el anonimato y la globalidad debido a la virtualidad lo que implica su complejidad para su judicialización.

En el ciberdelito, hay varios rasgos característicos que dificultan su identificación y procesamiento penal. En primer lugar, identificar al autor del delito puede ser bastante complicado. En segundo lugar, un daño significativo puede ser ocasionado por un pequeño grupo de personas o incluso por una sola. En tercer lugar, la escena del crimen no está claramente delimitada en el ciberespacio (Mireille & Ulrich, 2008, p. 170).

La trazabilidad de los ciberdelitos es complicada, lo que dificulta la obtención de pruebas sólidas. Confirmar la autenticidad de estas pruebas también representa un desafío, lo que complica aún más el proceso. Además, demostrar los cargos criminales relacionados con el ciberdelito puede ser particularmente difícil debido a la complejidad de las acciones y la falta de evidencia contundente.

Por último, es importante señalar que muchos ciberdelitos se llevan a cabo con un alto grado de profesionalismo, lo que hace aún más difícil su detención y atribución. Sin embargo, es fundamental reconocer que este análisis se centra en las características penales de los delitos cibernéticos, en lugar de abordar directamente las características intrínsecas de cada delito, excepto

aquellos que están relacionados con la infracción de datos y la información personal, que tienen un apartado específico en esta investigación.

El sistema informático y la red se utilizan en todas las áreas de nuestra sociedad, y es común encontrar infracciones cibernéticas debido a su vulnerabilidad inherente. Delitos como la piratearía informática crean un alto grado de riesgo. A medida que los activos intangibles, como la información, se conviertan en bienes importante, los derechos de autor, la privacidad y la tecnología, surgen muchos nuevos delitos contra bienes tangibles, como el dinero.

Debido a la diversidad de base de datos, contraseñas y sistemas informático, supervisar el ciberespacio es difícil. Esto también hace que sea muy complejo contrarrestar las conductas punibles en razón a que los datos almacenados en el ciberespacio se eliminan o se almacenan temporalmente, así mismo la difícil tarea de localizar la escena del crimen, sumado a que nuestro ordenamiento sustantivo no está ajustado a la realidad actual de estos tipos y modalidades del ciberdelito, lo que implica una seria dificultad para judicializarlos.

6.3 Desafíos en el ciberespacio

Como se mencionó anteriormente, el ciberespacio actúa como una extensión del espacio real, lo que implica que la distinción entre la vida en el ciberespacio y en el espacio real carece de sentido. Asimismo, los derechos humanos en este escenario no pueden distinguirse de los derechos en el espacio convencional. Por ejemplo, la libertad de expresión es igualmente importante en ambos espacios. Sin embargo, las violaciones de derechos en el ciberespacio y en el espacio real no reciben el mismo trato debido a sus particularidades.

En el caso de la difamación, el riesgo y la ilegalidad son considerados más altos en el ciberespacio, lo que conlleva a castigos más severos. En el mundo físico, las infracciones de

derechos suelen tardar más en propagarse, lo que permite respuestas reactivas. En cambio, en el ciberespacio, las infracciones pueden difundirse globalmente de inmediato y sus rastros nunca desaparecen. Por lo tanto, las medidas para combatir la vulneración de derechos en el ciberespacio deben ser preventivas debido a la rapidez con la que se propagan. Así, las contramedidas en el ciberespacio son notablemente diferentes de las del mundo físico.

Desde esta perspectiva, la reciente vulneración de derechos en el ciberespacio debe ser analizada desde el principio de respuesta; en otras palabras, el enfoque para reparar derechos en este contexto puede diferir del del mundo real debido a su especificidad, ya que los principios no siempre son aplicables en el entorno virtual.

6.4 Riesgos y desafíos de la inteligencia artificial: necesidad de regulación

Desde un enfoque penal, los robots con IA actuales son considerados objetos y no pueden ser sujetos de delitos por sí mismos. Esto significa que, si un sistema autónomo comete un delito a través de una acción física, la responsabilidad recae en la persona que dio la orden, ya que el robot actúa solo como un instrumento del delito. Incluso si un sistema autónomo comete un error debido a un fallo en su diseño, fabricación o funcionamiento, la responsabilidad penal recae en el diseñador, fabricante, propietario o usuario.

Sin embargo, aunque un robot o sistema autónomo no pueda ser considerado sujeto de delito, sí puede ser objeto de sanciones legales. Por ejemplo, si se utiliza para cometer un delito, se puede aplicar la figura de comiso según el artículo 82 de la ley 906 de 2004, aunque esto no implica un castigo directo al robot. Asimismo, si una persona destruye un robot que pertenece a otra, se aplicaría el daño en bien ajeno según el artículo 265 de la ley 599 de 2000. De igual manera,

si se roba un sistema autónomo, el delito sería el de hurto conforme al artículo 239 del C.P., considerando como víctima al propietario del robot.

Hasta el momento, la mayoría de postura consideran a los robots con IA como objetos (Brenner, 2013, p 29). Es poco probable que esta perspectiva cambie en un futuro cercano. Sin embargo, cuando la IA avanzada o fuerte se vuelva más común, la forma en que consideramos a aquellos que poseen este sistema podría transformarse. Un sistema autónomo con capacidad de juicio y voluntad podría rechazar órdenes humanas o actuar de manera independiente para proteger sus propios intereses, lo que complicaría su consideración como un simple objeto.

Ahora bien, para evaluar la posibilidad de que un sistema autónomo sea visto como un ser vivo, es necesario revisar el estatus legal de los animales en nuestro marco normativo. En este sentido, el Código Civil no contiene disposiciones generales sobre el estatus de los animales, aunque en ciertos aspectos se les considera propiedad. Por ejemplo, se establece que los animales destinados al cultivo o beneficio de una finca se consideran inmuebles por adhesión, según lo dispuesto en el artículo 659 del Código Civil. Sin embargo, se les clasifica como muebles por anticipación cuando forman parte de un vivar, de acuerdo con el artículo 660 del mismo código.

A pesar de que en el Código Civil los animales son considerados propiedad, la Ley 1774 de 2016 los reconoce como seres sintientes y los excluye de la categoría de cosas. Además, reciben una protección especial contra el sufrimiento y el dolor, lo que implica que no se puede atribuir responsabilidad sin la existencia de una entidad física. Por lo tanto, si la legislación otorga personalidad jurídica a un sistema autónomo, no podría considerarse como animal, en razón a las características particulares de un ser vivo, solo podría analizarse desde un estatus legal similar al de una persona jurídica.

AUTOPUESTA EN PELIGRO DEL USUARIO CON CHATBOTS INTELIGENTES:

La afirmación de conferir personalidad jurídica a un sistema autónomo a través de la ley no implica automáticamente que dicho sistema se sitúe en igualdad de condiciones con una persona jurídica tradicional, ni que se resuelvan todos los problemas teóricos y prácticos relacionados. En Colombia, es importante destacar que la persona jurídica no tiene responsabilidad penal. Además, existen claras diferencias entre una entidad física y un sistema autónomo de IA, ya que la persona jurídica no necesita una existencia física, sino que es un ente conceptual susceptible de derechos y obligaciones.

No obstante, un sistema autónomo de IA tiene una entidad física concreta compuesto por el hardware que se une en un todo con el software de una forma lógica conformando así una entidad en sí misma, pues en efecto se diferencia del exterior. Ahora bien, si un robot es susceptible de recibir derecho y adquirir obligaciones es probable que se pueda determinar el alcance de la responsabilidad atribuida, por lo tanto, las sanciones impuestas pueden ser visibles y materiales.

Esto genera diferencias más profundas en cuanto a la atribución de responsabilidad en razón a que las personas jurídicas, los actos reales los lleva a cabo un ser humano, lo que significa que en el sujeto de los derechos y obligaciones y el agente físico que actúan están separado, sin embargo, en un sistema autónomo de IA es al mismo tiempo el sujeto de la acción y el titular de los derechos y obligaciones, incluso cuando se hace en el análisis desde la capacidad penal, se llega a la misma conclusión.

En el código penal, dispone la suspensión y cancelación de la personería jurídica cuando existen motivos fundados que permitan inferir que se han dedicado total o parcialmente a desarrollo de actividades delictivas, es decir, que la persona jurídica su concepto dentro de la estructura penal es un instrumento para la comisión de los delitos, recayendo la responsabilidad en los actos realizados por humanos.

Ahora bien, hacer el análisis desde la capacidad de percepción a través de lo sentidos que son una característica básica del ser humano en su capacidad de percibir el mundo exterior mediante los cinco sentidos los cuales están estrechamente relacionados con la capacidad intelectual, ya que la percepción de objetos externos mediante los sentidos implica una conciencia mental de esa percepción.

No obstante, los sentidos no solo son exclusivos de los humanos, muchos animales, como perros, gatos, vacas, peces e incluso insectos, poseen los cincos sentidos en diversas formas, por supuesto, los límites y características de los sentidos varían según la especie humana y el individuo, como los perros no puede distinguir los colores, pero tienen un sentido del olfato más desarrollado que los humanos.

De esta manera no se puede decir que los sentidos solo es una característica exclusiva de los humanos lo que implica que un sistema autónomo de IA puede diferenciar olores, sabores e inclusive colores, por ejemplo, es robot aspirador que tiene la capacidad de identificar obstáculos y una estructura de una casa, sin embargo, no significa que por ese solo hecho se equipara al ser humano y puede ser susceptible de reconocimiento jurídico como una persona inteligente.

Refiriéndonos al juicio moral que es otra habilidad del ser humano a la hora de tomar decisiones correctas en función de los valores propios ante situaciones específicas, es una capacidad que distingue conceptualmente de la capacidad racional, incluso si una IA alcanza un nivel de razonamiento lógico comparable al humano, esto no significa automáticamente que también posea la capacidad de juicio moral, pues dicha habilidad tiene que ver con la capacidad de responder emocionalmente a la situación de otra persona, en la empatía, situación que aun, está por desarrollar en la IA.

AUTOPUESTA EN PELIGRO DEL USUARIO CON CHATBOTS INTELIGENTES:

Desde la perspectiva del siglo XX, los robots de IA existentes en el siglo XXI tienen capacidades sorprendentes y podrían considerarse suficientemente desarrollados. Sin embargo, desde la perspectiva actual (siglo XXI), no es fácil afirmar que los robots de IA existentes estén suficientemente desarrollados o que deban ser tratados al mismo nivel que los humanos. Estar suficientemente desarrollado es, en última instancia, una condición previa para reconocer la responsabilidad penal de un sistema autónomo, y explorar su significado real requiere la colaboración de disciplinas como la jurisprudencia, la ingeniería, la electrónica, la ética y la filosofía. Este no es un desafío que pueda abordarse con una sola investigación. Por lo tanto, en el momento actual, solo es posible establecer un criterio muy general sobre el significado de suficientemente desarrollado y es que se cumpla mínimo dos criterios como superar la "prueba de Turing" y poseer una entidad física definida (Turing, 2010, p. 3)

Es la prueba de comportamiento. Según esta, un robot de IA que pueda interactuar con el entorno y tener capacidades de pensamiento complejo y comunicación, tener la capacidad de autorreflexión con el fin de lograr planes o metas en la vida, y vivir en una comunidad con personas de perspectivas recíprocas, se considera que posee una forma de personalidad (Kaplan & Haenlein, 2018, p. 18).

Lo anterior no significa que un robot que posea estos dos criterios por si solos ya debe ser considerado automáticamente como humano, es simplemente que si un sistema autónomo de IA no cumple con los anteriores criterios solamente se puede indicar que no debe ser considerado un ente suficientemente desarrollado, es decir, que una IA que actualmente cumpla con al menos una de estas dos condiciones no puede ser considerado un sujeto de delitos en el derecho penal, a lo mucho puede tratarse como una cosa.

AUTOPUESTA EN PELIGRO DEL USUARIO CON CHATBOTS INTELIGENTES:

Esto es debido a que el derecho penal tradicional, basado en el principio de responsabilidad, tiene un criterio claro al respecto. Un ser humano con capacidad de juicio racional puede tomar decisiones y desviarse del camino legal para cometer un delito, y el castigo es la sanción por ello, que la capacidad intelectual, la voluntad libre y la capacidad de juicio legal y moral constituyen la esencia de la subjetividad penal humana. Desde esta perspectiva, se puede decir que las características clave que poseen los humanos los convierten en sujetos de delitos.

Desde la perspectiva de que un sistema autónomo puede ser víctima de un delito, la discusión sobre si se reconoce la subjetividad penal de un ser y la aplicación de principios legales cuando ese ser es objeto o víctima de un delito son cuestiones distintas. Por ejemplo, una corporación no puede ser considerada sujeto de un delito, pero sí puede ser objeto de uno. En el ámbito del derecho civil, un feto no tiene capacidad de obrar, pero sí tiene capacidad de derechos en un alcance limitado, lo que le permite ser objeto de ciertos actos legales.

Por lo tanto, la subjetividad penal y la condición de objeto o víctima de un delito no siempre se valoran de la misma manera. La clave al debatir la subjetividad penal es si es legítimo atribuir la responsabilidad penal al autor del acto desde una perspectiva legal. En cambio, al discutir la condición de objeto o víctima de un delito, lo que realmente importa es qué bien jurídico se ve afectado por el delito en cuestión.

A partir de este breve análisis, no se puede afirmar que, bajo la perspectiva de la teoría del delito tradicional, la inteligencia artificial no pueda ser concebida como sujeto de derechos y obligaciones. Sin embargo, el uso de la IA puede causar daños a bienes jurídicamente protegidos, con un impacto mayor debido a su especificidad. En tales casos, es fundamental prever y evitar las consecuencias ilegales.

Entonces la previsibilidad y evitabilidad juega un papel importante, ya que un comportamiento cuestionable puede infringir los intereses protegidos de otros si la persona, no obstante, realiza tal acto; es decir, si anticipa la ocurrencia del resultado constituyente y podría haber evitado.

Particularmente, el Principio de debida diligencia, muy fuerte aplicado desde el derecho civil y hasta el derecho penal en relación con la producción y las ventas, ha desarrollado la idea que los productores cuidadosos saben que el nivel de seguridad de sus productos está en línea con las normas pertinentes. Solo después de cumplir con los estándares técnicos y someterse a suficientes pruebas antes de la venta, se comercializa. Incluso después de producir y vender un producto, el productor continúa asumiendo responsabilidad.

Es importante observar continuamente la respuesta del usuario, a través de una queja, brinda comentarios necesarios en pro de mejora del producto o servicio, llevándolas a la reparación en las etapas de diseño y producción con el fin de descubrir daños o riesgos no previstos. En este caso, el productor debe advertir al consumidor y, si es necesario, proceder a retirar el producto. Sin embargo, la inteligencia artificial evalúa de forma independiente la información adquirida del entorno circundante, la interpreta, responde sin intervención humana y lleva a cabo la tarea asignada de forma óptima.

Es difícil lograr que el usuario observe continuamente la reacción de la inteligencia artificial. La IA percibe datos, los interpreta y reacciona de manera impredecible. Es imposible prever todas las situaciones que pueden surgir con el uso de la IA y programar de antemano para evitar todos los peligros inesperados. Además, dado que los sistemas de inteligencia artificial aprenden de forma autónoma, se vuelve aún más complicado anticipar sus decisiones y acciones.

AUTOPUESTA EN PELIGRO DEL USUARIO CON CHATBOTS INTELIGENTES:

En cuanto a la ocurrencia de resultados ilegales, hay dos escenarios, el primero se puede dar desde el propio procesamiento de la información que el usuario brinda y no puede ser prevista ni evitadas por el usuario, debido que IA actúa de forma autónoma a partir de la información suministrada por el usuario, lo que implica una exclusión de responsabilidad por parte del proveedor, quien argumenta que no puede ser responsabilizado, ya que el procesamiento se originó a partir de la información proporcionada.

En segundo lugar, el usuario de la inteligencia artificial es el propietario de esta, por lo tanto, debe hacerse responsable de todo lo que ocurra como resultado de las actividades de IA. Es decir, independientemente de la mensurabilidad y evitabilidad, todo daño causado por las acciones de la inteligencia artificial también puede dar lugar a la autorresponsabilidad. Estas dos afirmaciones no solo respaldan a los productores y proveedores, sino también podrían aplicarse a los diseñadores.

Hay que tener en cuenta que la IA ha aportado significativamente a diferentes áreas, entonces sancionar todas las violaciones de los bienes protegidos sin reconocer excepción alguna, puede repercutir drásticamente en el desarrollo de la inteligencia.

El nivel de asunción de riesgos y el grado de debida diligencia son consideraciones necearías al juzgar y decidir sobre el uso de la IA. La disposición de la sociedad a aceptar la IA está en aumento, por los beneficios que trae consigo, sin embargo, en la medida de su utilización van aumentando los riesgos. La Unión Europea con su proyecto de ley clasificó los niveles de riegos de la IA, es allí donde el diseñador, proveedor y usuario, a la hora de juzgar, se le exigirá un menor o mayor nivel de debida diligencia.

En primer lugar, el vendedor tiene la responsabilidad de proporcionar advertencias y orientación completas al usuario. Además, el productor debe monitorear continuamente el

funcionamiento de la IA y responder de manera ágil en caso de daños, considerando la imposición de una obligación de cumplimiento.

Durante las etapas de diseño, fabricación y venta, se debe mantener un equilibrio en el deber de cuidado, el cual se debe reforzar durante la gestión y el seguimiento del producto. Por ejemplo, en el caso de los ChatsBots inteligentes, es fundamental tomar medidas adecuadas para prevenir y gestionar el mal uso por parte de los usuarios, especialmente si se ven involucrados en actividades ilícitas.

Es crucial que los diseñadores, operadores cumplan con todas las medidas legalmente establecidas para garantizar la seguridad de la IA. El incumplimiento de estas disposiciones puede constituir una sanción penal. Por lo anterior, se hace necesario intensificar el análisis del prototipo, supervisarlo, modelarlo con el fin de prevenir los riesgos percibidos, y cumplir con el deber de eliminar las consecuencias producidas.

No hay ningún problema lógico, desde la teoría tradicional del delito, atribuir la responsabilidad penal por los resultados ilegales a los diseñadores, proveedores y usuarios. Sin embargo, en el ordenamiento local se hace necesario un ajuste al título VII BIS de la Ley 599 de 2000 por su poca claridad, coherencia estructural de los que son los ciberdelitos y lo dispuesto en el marco normativo.

6.5 Generalidades de una dogmática para judicializar chatbot inteligentes

Desde la teoría del delito y el dominio de hecho, los aspectos para tener en cuenta a la hora de ajustar una dogmática penal frente a los delitos cometidos mediante ChatBot inteligentes debe estructurarse en torno a los elementos esenciales del delito: tipicidad, antijuricidad y culpabilidad.

AUTOPUESTA EN PELIGRO DEL USUARIO CON CHATBOTS INTELIGENTES:

Desde la tipicidad implica adecuar la conducta delictiva a un tipo penal, en el caso objeto de estudio, el problema específico debe ser abordado desde una perspectiva amplia en razón al vacío actual en la legislación local. En la tipicidad objetiva la acción u omisión se puede materializar en actos como phishing, fraude, grooming, o manipulación de datos a través del ChatBot como medio comisivo, toda vez que en la actualidad se considera un instrumento que actúa bajo el control de un autor (mediato o inmediato) o con un grado de autonomía programada.

En un futuro muy cercano se va a originar un problema con la interpretación tradicional de la teoría del delito, en razón a que el instrumento puede llegar a tomar decisiones autónomas sin control significativo humano, lo que implica que puede ser incluido en los tipos penales tradicionales que asumen una intervención directa del ser humano.

En relación con la tipicidad subjetiva, el análisis del dolo debe centrarse en determinar si el programador, usuario o un tercero tenía conocimiento y voluntad de utilizar el ChatBot como herramienta para cometer un ilícito. En casos de negligencia, como cuando se diseña un sistema sin implementar medidas de seguridad adecuadas para prevenir su uso indebido, debe considerarse la posibilidad de autoría mediata, en línea con la teoría del dominio del hecho.

En este contexto, el creador o controlador del sistema podría ser considerado autor mediato, al emplear el sistema como un instrumento para la comisión del delito, aun cuando el acto se produzca de manera indirecta a través de la tecnología. Este enfoque requiere una evaluación rigurosa del grado de control ejercido sobre el sistema y de la previsibilidad del uso ilícito.

Desde la perspectiva de la antijuridicidad, la conducta debe ser no solo típica, sino también vulnerar de manera concreta el bien jurídico tutelado. En el caso de los ChatBots, esta vulneración puede materializarse de diversas formas, como en la propiedad, mediante fraudes electrónicos o robos de datos; en la intimidad, a través de la recolección no autorizada de datos personales; en la

seguridad pública, mediante la difusión de mensajes engañosos o desinformación masiva; y en la integridad personal, en casos de grooming o acoso automatizado. Estas conductas reflejan cómo el uso indebido de los ChatBots puede lesionar bienes jurídicos protegidos, configurando una antijuridicidad en el marco penal.

Es necesario considerar la causación mediata, dado que los sistemas de inteligencia artificial poseen una autonomía limitada, lo cual exige determinar si la conducta antijurídica puede imputarse a un autor mediato o inmediato, en virtud del nexo causal. Este análisis incluye evaluar la acción previsible, ya que el creador debe anticipar el uso potencial del ChatBot para fines ilícitos. Sin embargo, pueden surgir acciones imprevisibles cuando el sistema opera fuera de los límites previstos, lo que podría constituir una causal eximente de responsabilidad, al menos de manera parcial, en relación con la antijuridicidad atribuible al creador o al usuario.

En estos casos hay que considerar la exclusión de la antijuricidad cuando la víctima da su cometimiento, situación que se origina en la interacción voluntaria con el ChatBot. También se puede considerar el estado de necesidad cuando el sistema fue empleado para evitar un daño mayor, como la recopilación de datos para prevenir un ciberataque.

En el ámbito de la culpabilidad, se analiza si el autor puede ser reprochado por su conducta delictiva. La imputación directa recae en el responsable del ChatBot (programador o usuario), quien debe ser consciente de los riesgos asociados a su diseño o uso. Por otro lado, la imputación indirecta surge cuando el ChatBot actúa de manera autónoma, lo que exige evaluar si dicha acción fue consecuencia de un diseño negligente o de un control insuficiente por parte del responsable. Este análisis permite determinar el grado de culpabilidad en relación con el comportamiento del sistema.

En cuanto al conocimiento y la voluntad, se puede identificar un dolo eventual si el responsable previó la posibilidad de que el sistema fuera utilizado para un fin delictivo y, a pesar de ello, permitió su operación. Por otro lado, se configura la culpa consciente cuando, teniendo conocimiento de los riesgos, el responsable no adopta las medidas necesarias para evitar los resultados ilícitos. En casos de causación dolosa, el ente acusador debe establecer que el autor utilizó deliberadamente el ChatBot como medio para cometer el ilícito. Finalmente, en la modalidad culposa, los resultados delictivos derivan de un diseño negligente, como la ausencia de protocolos de seguridad adecuados, lo que evidencia una falta de diligencia en la prevención del uso indebido del sistema.

De lo anterior, es posible recurrir a la teoría del dominio del hecho y adaptarla al contexto de los sistemas autónomos, considerando al ChatBot como un instrumento para la comisión del delito. En este marco, el autor directo sería el usuario que emplea el ChatBot con fines delictivos, mientras que el autor mediato sería el programador o diseñador, quien ejerce control sobre el comportamiento del sistema a través de la configuración de sus capacidades y funcionalidades. Esta adaptación permite delimitar las responsabilidades según el grado de intervención y control sobre el sistema autónomo.

Finalmente, en casos de coautoría, se configura la responsabilidad cuando varios agentes participan en el diseño, implementación y uso del ChatBot, actuando con conocimiento de sus fines delictivos. En cuanto a la imputación objetiva, los resultados delictivos generados por el ChatBot solo podrán atribuirse si el autor tenía un dominio potencial del hecho, es decir, la capacidad de prever, controlar o influir significativamente en las acciones del sistema que derivaron en la conducta ilícita.

6.6 Implicaciones jurídicas de la IA en la protección del dato y la información

La necesidad de protección de la intimidad tiene por objeto permitir que las personas decidan por sí mismas a que información sobre ellas pueden acceder terceros y, por tanto, permitir que puedan vivir bien y sin humillaciones en determinados ámbitos (Ley 1581, 2012).

La protección de datos permite a los interesados ejercer cierto control sobre el tratamiento de estos, incluso después de haberlos facilitado. Una de las preocupaciones del uso de la IA en reconocimiento facial como videovigilancia en aras de garantizar la seguridad frente acontecimientos importantes, basado en un software con una base de datos previamente de presuntas personas potencialmente criminales, puede llegar a ser discriminatorio y violatorio de la intimidad en razón a que se partió de una la lista previa sin que las personas que figuraban en ella hayan dado su consentimiento.

La protección de datos se basa esencialmente en la idea de autodeterminación informativa, entendida como un derecho fundamental, permitiendo al titular ejercer un control total sobre sus propios datos. En el caso expuesto al inicio el uso de la IA puede acentuar los riesgos inherentes a la captura y tratamiento de datos personales. Si bien la videovigilancia a gran escala puede resultar delicada en si misma desde el punto de la privacidad y la protección de datos, teniendo en cuenta que las imágenes obtenidas en sitios públicos y combinadas con otros datos, permiten seguir los movimientos y las acciones de las personas o de grupos enteros en lugares públicos.

En Colombia fue implementado la tecnología de videocámaras en el aeropuerto el dorado, sin embargo, hay un control significativo humano, denominados perfiladores, que logran identificar a personas que pueden estar traficando sustancias ilegales a través del aeropuerto. Sin

embargo, frente al uso de IA fuerte frente a generar alertas en estos lugares pueden llegar a ser ilícitas, siempre y cuando, se haga a través de datos sensibles tratados sin autorización.

El ordenamiento local todavía no puede responder a muchos interrogantes sobre el uso de la IA con fines de vigilancia. La necesidad de actuar es evidente por cuanto la unión europea prevé la prohibición de la identificación biométrica en tiempo real de las personas en sitios públicos. Sin embargo, esta regla no es absoluta, toda vez que el reconocimiento biométrico (reconocimiento facial) se utilice con fines de seguridad pública. Cabe resaltar que en la medida que se vaya consolidando IA, puede llegar a que particulares y con fines distintos de la aplicación de la ley siga estando permitida bajo un criterio de alto riesgo y, por lo tanto, se exija estándares más altos a fin de utilizarlos.

La función principal de la mayoría de los sistemas basados en IA fuerte es, en sentido amplio, tomar decisiones o prepararlas, como clasificar un correo y ubicarlos en la carpeta spam, que se hace a través de determinados criterios de identificación. Debido a esta función central de la IA de tratar de manera diferente bajo ciertos criterios dados, existen numerosos y diversos ejemplos que al inicio expusimos donde la discriminación proviene del uso de la IA.

Un ejemplo más reciente ocurrió en Nueva York, donde una trabajadora sexual reservó un alojamiento para un viaje privado con su pareja a través de Airbnb. Poco después, fue excluida de la plataforma, alegando que su cuenta no cumplía con las condiciones de uso y las normas comunitarias. Posteriormente se descubrió que la plataforma Airbnb utilizaba una IA que evaluaba la confianza de los usuarios basándose en la huella digital publica, circunstancia que aquellas personas con actividades o declaraciones no deseadas eran automáticamente excluidas del uso de la plataforma.

AUTOPUESTA EN PELIGRO DEL USUARIO CON CHATBOTS INTELIGENTES:

Un estudio realizado en el 2020 llego a la conclusión de que la aplicación actual de la IA no incluía mecanismo para evitar el sesgo, pero esto se debe a lo que se plateaba anteriormente la cultura en el ciberespacio, dado que los datos que alimentan proviene en su mayoría de las redes sociales en las cuales encuentra una serie de opiniones segadas y discriminación constante, lo que implica que los proveedores de servicios o productos basado en IA fuerte deben implementar mecanismo o herramientas que identifiquen el sesgo desde el concepto calificativo prohibido por el artículo 13 de la Constitución Política o utilizar datos más confiables y tratados.

El uso de la IA ha aumentado el riesgo de discriminación indirecta o encubierta, que puede verse únicamente en el impacto. Se considera que existe tal discriminación indirecta cuando los criterios utilizados en particular, los datos parecen neutros y, en consecuencia, perjudican a las personas que poseen cualificaciones constitucionales. Además, las aplicaciones basadas en IA donde una de sus funciones es asociar datos, presentan un mayor riesgo de discriminación por asociación. En tal caso, una diferencia de trato en cuanto a los efectos se basa únicamente en la relación de una persona con un grupo que presenta características protegidas.

Hay que tener en cuenta que los términos de equidad y sesgos tiene una importancia esencial en el contexto de aplicaciones de los sistemas basados en IA. Sin embargo, estos términos se definen de manera más amplia en varias diciplinas, como en la computación donde suele equipararse con parcialidad. Por lo tanto, si se espera que las aplicaciones sean justas, no sesgadas y no discriminatorias, el único criterio jurídicamente pertinente y operativo es el de la no discriminación.

En ese contexto, es importante señalar que, en Colombia, los delitos informáticos, electrónicos, de telecomunicaciones, y aquellos relacionados con los derechos de autor y normas complementarias, podrían considerar ilegal el uso de ChatGPT. Esto se debe a que la información

generada por investigaciones protegidas por derechos de autor, disponible en internet, puede ser utilizada como fuente sin la correspondiente citación, lo cual contraviene los bienes jurídicos protegidos por el derecho de autor.

Con la llegada de los ChatsBots inteligentes, surge una tensión relacionada con la comunicación no privada debido al intercambio de datos personales que trasciende la esfera íntima del usuario. Esto ocurre porque, sin que el usuario lo note, cualquier "mensaje de datos" entre el proveedor y el usuario se genera, envía, recibe, almacena o comunica a través de la plataforma del ChatBot. La confianza que el usuario deposita en la aplicación puede llevarlo a proporcionar información personal sin darse cuenta (Congreso de la Republica, Ley 1266, Art. 3, 2008).

Con el avance de la IA implica la actualización de las conductas en el código penal, sin embargo, el legislador dispuso en su artículo 269G regula la violación de datos personales el cual fue adicionado al código penal con la Ley 1273 de 2009 es legislado dispuso lo siguiente:

> El que con objeto ilícito y sin estar facultado para ello, diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con pena más grave.
>
> En la misma sanción incurrirá el que modifique el sistema de resolución de nombres de dominio, de tal manera que haga entrar al usuario a una IP diferente en la creencia de que acceda a su banco o a otro sitio personal o de confianza, siempre que la conducta no constituya delito sancionado con pena más grave.
>
> La pena señalada en los dos incisos anteriores se agravará de una tercera parte a la mitad, si para consumarlo el agente ha reclutado víctimas en la cadena del delito.

AUTOPUESTA EN PELIGRO DEL USUARIO CON CHATBOTS INTELIGENTES:

Este tipo de conducta es muy común en el entorno digital y se basa en la creación de sitios web falsos para obtener información personal. El autor del delito, conocido como phisher, elabora una página web casi idéntica a una legítima, alojándola en un servidor diferente con el fin de recolectar datos confidenciales a través de lo que se conoce como phishing. Su objetivo es acceder a información sensible o difundir anuncios fraudulentos en nombre de la entidad falsificada, utilizando una dirección IP distinta. Con frecuencia, los estafadores logran obtener contraseñas, números de tarjetas de crédito u otros datos sensibles de los usuarios, a quienes engañan con la promesa de premios o descuentos atractivos que resultan ser falsos.

Desde una perspectiva penal, esta conducta se considera un delito subsidiario en comparación con otros crímenes más graves, como la extorsión o el robo a través de medios electrónicos. Además, al ofrecer incentivos atractivos, como dinero, descuentos, sorteos, boletos de avión o estadías en hoteles de lujo, logran atraer de manera inadvertida a nuevas víctimas hacia el sistema fraudulento.

En cuanto al autor de este delito, al igual que en otros tipos penales mencionados en este título, cualquier persona puede llevar a cabo esta conducta punible, lo que coloca al autor en la categoría de sujeto activo indeterminado. El sujeto pasivo, por su parte, son los titulares o usuarios de los datos almacenados en sistemas informáticos. El bien jurídico protegido es la integridad de los datos personales, ya sean confidenciales o sensibles, que se encuentran codificados en un sistema informático.

El objeto material del delito se refiere a las páginas web y enlaces afectados. La conducta delictiva puede llevarse a cabo mediante actividades como el diseño, desarrollo, tráfico, comercialización, ejecución, programación o envío de sitios electrónicos, enlaces o ventanas emergentes.

Asimismo, la censura penal puede producirse a través de la alteración del sistema de resolución de nombres de dominio, con el objetivo de redirigir al usuario a una dirección diferente para acceder a su información bancaria o a otros sitios de confianza.

Como elementos normativos de la conducta, la legislación exige que el ciberdelincuente actúe con un propósito ilícito y sin autorización, siempre que la acción delictiva no configure un delito con una sanción más grave. En cuanto a la culpabilidad, las distintas modalidades criminales incluidas en la norma prohibitiva comparten el elemento del dolo. No obstante, la tentativa es posible en estos casos, ya que se trata de un delito de resultado.

La relevancia de las circunstancias de agravación punitiva contempladas en el artículo 269H, desde la perspectiva de la dosificación de la pena, se fundamenta en la condición especial que, en ciertos casos, poseen tanto el autor como la víctima del delito. Esto incluye la confianza que el usuario del sistema o titular de la información deposita, los objetivos ilícitos relacionados con actos de terrorismo o con la seguridad y defensa nacional, así como la utilización de terceros de buena fe como herramientas para la ejecución delictiva mediante autoría mediata.

No obstante, en cuanto a la tercera causal del artículo mencionado, que establece el provecho para sí mismo o para un tercero como agravante, es importante señalar que su inclusión en este contexto vulnera claramente el principio de non bis in ídem, en relación con el delito de hurto por medios informáticos y semejantes, regulado en el numeral 17 del artículo 58 de la Ley 599 de 2000. Esto se debe a que el beneficio o utilidad es un elemento intrínseco del tipo penal en cualquier modalidad de dicho delito. Una situación similar ocurre en el caso del delito de transferencia no consentida de activos, en el cual el ánimo de lucro constituye, desde el inicio, el objetivo del agente.

6.7 ChatBot inteligente y riesgos jurídicamente desaprobados

Claus Roxin (2012) es reconocido por haber inventado la teoría de la imputación objetiva, la cual fue desarrollada en sus artículos a partir de los años setenta y sistematizada en su tratado sobre la Parte General del Derecho Penal. La teoría de la imputación objetiva, que originalmente tuvo un gran impacto en Alemania, se ha difundido ampliamente en América Latina, donde ha sido incorporada tanto en la doctrina como en la jurisprudencia de varios países. Esta teoría ha sido aceptada en la mayoría de las repúblicas latinoamericanas y ha tenido una influencia considerable en la forma en que se entiende la responsabilidad penal (Roxin, Derecho Penal, Parte General, Fundamentos. La estrcutura de la Teoria del Delito, 2012, p. 342).

Ahora bien, la teoría ha servido para limitar la imputación basada únicamente en la mera causación del resultado, evitando que se atribuya responsabilidad penal de manera automática sin considerar si el riesgo creado es jurídicamente desaprobado y si dicho riesgo se realizó en el resultado. Aunque algunos juristas latinoamericanos mostraron cautela ante la aplicación de una teoría desarrollada en un contexto europeo a las realidades de América Latina, sin embargo, uno de los tratadistas que defiende dicha teoría es Manuel Cancio Meliá donde expone que la teoría de la imputación objetiva no solo es aplicable en el contexto latinoamericano, sino que también es necesaria para asegurar una interpretación más justa y racional del derecho penal en la región.

En ese sentido, Cancio Meliá (1998) sugiere que la teoría de la imputación objetiva continuará evolucionando y siendo relevante en América Latina, especialmente en un contexto donde las legislaciones penales tienden a crear tipos penales vagos y sobre - inclusivos (Cancio Meliá, 2005, p. 62). En Colombia no es la excepción y en esa postura del tratadista la teoría puede servir como herramienta para interpretar y restringir de manera coherente y racional estos tipos

penales mejorando la justicia penal y sirviendo como un marco dogmático esencial para la imputación de responsabilidades penales.

En los ChatBot Inteligente hay varias limitaciones, como exactitud de las respuestas en razón a que estas aplicaciones generan resultados a través de la causalidad de las palabras, pero sin un proceso de verificación de los hechos, puede generar indiscriminadamente información falsa o contenido inapropiado.

Otra limitación es que los modelos que utilizan IA extraen resultados basados en los datos aprendidos, no pueden reflejar la información más fuera de los datos de aprendizaje. Asimismo, estos prototipos pueden tener sesgos artificiales en cuestiones de juicio de valores como la raza, el género, la religión y la política. La capacidad de razonamiento del modelo resulta de lo que comprende y responde el contexto de una conversación a partir de los datos de aprendizaje, por lo que es vulnerable a los cálculos matemáticos que requieren precisión.

Estas limitaciones producen riesgos jurídicamente desaprobados, como contenido de abuso o explotación sexual de menores, violencia, creación de malware, actividades de alto riesgo físico (desarrollo de armas, militares, suicidios, etc.), actividades de alto riesgo económico (ventas múltiples, juegos de azar, préstamos, etc.), fraude, contenido para adultos, política, violación de la privacidad, asesoramiento para actos ilegales.

Uno de estos ChatsBots inteligentes es Chat GPT, que trae innumerables beneficios, sin embargo, en una encuesta realizada por BlackBerry a 1.500 personas responsables de tomar decisiones en Tecnología de la Información en Estados Unidos, Canadá, Reino Unido y Australia reveló que la aplicación podría ser utilizado para una buena causa, pero el 74% de los encuestados reconoce y teme que existen amenazas potenciales a la ciberseguridad. El 51% de los encuestados cree que un ciberataque con ChatGPT tendrá éxito en el plazo de un año, mientras que el 71%

afirma haber utilizado la tecnología para fines maliciosos en otros países. Además, el 82% de los encuestados planea invertir en ciberseguridad basada en IA en los próximos dos años, mientras que el 95% afirma que el gobierno es responsable de regular la alta tecnología (BlackBerry, 2023, p. 2).

El uso de ChatBot inteligentes para amenazas cibernéticas es una realidad, pueden ser utilizado de muchas maneras, entre ellas, las estafas que ya se han hecho pasar por ChatGPT. Como el caso de instalar malware de caballo de Troya simulando el cliente de escritorio de ChatGPT. Además, Facilita la creación de grandes cantidades de correos de suplantación de identidad (phishing), permite modificaciones delicadas que hacen que los correos de phishing sean más sofisticados y permite a los atacantes extranjeros crear de forma natural, eliminando las barreras lingüísticas. La producción masiva y avanzada de datos falsos que pueden ser utilizados en una variedad de ciberataques, como el spam y la falsificación, lo que reduce el costo de los ataques y aumenta el daño resultante para los atacantes.

Generación de código malicioso, la función de generación de código con los ChatBot Inteligente ayuda a los hackers a crear herramientas de hackeo, y ayuda a los principiantes sin conocimientos de desarrollo a crear herramientas fácilmente. Reducción del tiempo necesario para desarrollar herramientas de hacking, y existe la posibilidad de ciberdelincuencia indiscriminada y ciber criminalización de delitos comunes. Sin embargo, no es posible crear un nivel completo de malware que pueda ser utilizado directamente en un ataque cibernético, y se requiere experiencia adicional para modificar el código fuente generado y utilizarlo en la práctica.

Creación de ransomware que codifica archivos de documentos para solicitar bitcoins. No obstante, para utilizar los resultados de Chat Bot Inteligente en ataques reales, es necesario modificar el código adicional para generar archivos de ejecución de ransomware, como la salida

de la pantalla de solicitud de Bitcoin para el pago de los costos de descifrado, la transferencia de claves de descifrado.

Estos prototipos pueden crear correos electrónicos de phishing que se hacen pasar por un portal de renombre nacional para robar la información de la cuenta. Algunas de las características del malware que podrían ser explotadas por la ciberdelincuencia a través de ChatBot Inteligentes son generables, pero la combinación de características no permite un ataque real, sin embargo, para llevar a cabo un ataque real, es necesario tener conocimientos de hackeo, como la construcción de la infraestructura de ataque, la capacidad de elusión de antivirus o la modificación del código para adaptarse a un entorno específico.

En el análisis de vulnerabilidades, estos modelos permiten a los atacantes llevar a cabo un análisis más ágil para detectar fallos de seguridad o áreas específicas en el código fuente o la API. Tanto los desarrolladores como los responsables de seguridad pueden identificar y solucionar rápidamente estas vulnerabilidades, aunque también pueden obtener información que podría ser utilizada para hackear, como fallos de seguridad, escenarios de ataque y técnicas.

La filtración de información confidencial y el uso indebido de los resultados son riesgos significativos asociados con la entrada indiscriminada de datos, como información personal o confidencial de la empresa, ya que la información ingresada se almacena en los servidores como contenido de usuario. Además, la filtración de información confidencial puede ocurrir a través de preguntas de elusión y ataques de piratería a modelos o servicios de inteligencia artificial, lo que puede provocar la exposición de la información introducida por los usuarios.

Hay que tener en cuenta que los datos que ingresa al utilizar los servicios de las empresas que producen modelos de ChatBot Inteligentes, como OpenAI, tratan como contenido del usuario información personal proporcionada por el mismo y se almacenan en su base de datos.

AUTOPUESTA EN PELIGRO DEL USUARIO CON CHATBOTS INTELIGENTES:

Desde el contexto de actos de atacar a los modelos de ChatBot Inteligentes puede incluir la acumulación de conocimientos sesgados a través de la inyección maliciosa de datos de aprendizaje que pueden degradar la calidad de los resultados, distorsionar o discriminar, y causar trastornos sociales. También es posible modificar los datos de entrada para desclasificar los modelos (ataques fraudulentos), restaurar los datos utilizados para el aprendizaje, y realizar ataques de replicación de modelos en las etapas de aprendizaje y uso de modelos de IA.

Es eminente los riegos jurídicos que trae consigo estos prototipos de IA respecto de las filtraciones y violaciones de datos personales en razón a la inexistencia de controles de verificación de edad del usuario, tratamiento de los datos personales, recopilación ilegal de datos personales y de códigos, desconocimiento del origen de los datos utilizados para el aprendizaje de IA y los derechos de autor. Por tal razón estos prototipos de ChatBot Inteligentes están catalogados por el parlamento europeo como IA de alto riesgo.

Entonces, Desde la fase de desarrollo de modelos y servicios de IA hasta la fase de despliegue seguro, la necesidad de una respuesta de seguridad frente a las amenazas de seguridad específicas de la propia de la aplicación.

6.8 Atribución de responsabilidad penal: teoría del dominio del hecho

Desde la teoría de Claus Roxin (2000), los coloca en términos en que hay libertad de autolesión de la persona como lo es el suicidio, por tanto, el resultado no puede abarcar el tipo penal las acciones a propio riesgo, en razón que si se puede cometer de manera impune la mayor lesión al bien jurídico protegido como la vida pues no debe haber responsabilidad penal cuando la víctima es la que coloca en peligro (p. 425).

En virtud de la anterior tesis se edifica el principio de autorresponsabilidad que se traduce que en los casos donde la víctima asume conscientemente un riesgo y toma decisiones que

conducen al peligro, la responsabilidad penal puede no ser imputable a un tercero que haya facilitado o contribuido al riesgo. Esto se basa en la idea de que el control sobre la situación peligrosa reside exclusivamente en la víctima.

No obstante, la víctima es la única que controla el riesgo y acepta el peligro, se establece una identidad entre el autor del riesgo y la víctima. En estos casos, no se aplica la imputación objetiva al tercero, quien puede haber facilitado el riesgo, ya que no tiene control sobre el curso de los eventos peligrosos.

Según la teoría desarrollada por Roxin, en los casos donde la víctima es consciente del riesgo y lo acepta plenamente, el resultado no puede ser imputado objetivamente al tercero que haya participado en la creación de ese riesgo, ya que la víctima tiene el control total sobre la situación peligrosa.

Estos fundamentos son clave para entender por qué, bajo ciertas circunstancias, la imputación objetiva no se aplica en casos de autopuesta en peligro, centrándose en la responsabilidad autónoma del individuo que decide exponerse al riesgo.

Ahora bien, tomando la clasificación realizada por la Unión Europea, la inteligencia Artificial Fuerte o de “alto riesgo” tiene la capacidad de reconocer cambios en el entorno, juzgar situaciones de forma independiente, toma de decisiones de manera autónoma e interactuar con las personas lo cual puede conllevar a general riesgos altos a los derechos fundamentales de los usuarios (UE, COM 986, 2023, p. 1).

Para examinar los deberes de autoprotección frente a las interacciones con sistemas basados en Inteligencia Artificial, se parte de que un usuario voluntariamente decide afrontar la acción, que en algunos casos puede ser arriesgada y que desemboca en un resultado lesivo. No

obstante, la mera invocación del consentimiento del usuario por parte del diseñador o proveedor no es suficiente para dirimir un problema jurídico.

En la actual dogmática penal doméstica, el acto de una persona es lo que constituye un delito y, en cuanto a si se trata de una acción, históricamente va desde las teorías causales hasta las teorías propositivas y sociales. Ha habido discusiones sobre la teoría de la acción y la teoría de la acción personal, discutiendo la subjetividad criminal de la inteligencia artificial, pero para hacer esto, la operación o función de la inteligencia artificial debe ser un "acto" significativo en el derecho penal.

En el entendimiento actual del delito inicialmente conlleva a negar la responsabilidad de los sistemas autónomos, como agente electrónico o artificial, basado en la incapacidad en la acción y la determinación de la culpabilidad, Citando a Franz von Liszt, desde la concepción psicológica – normativamente se afirma claramente que la culpabilidad es la "relación subjetiva entre el acto y el autor", que "solo puede ser psicológica". Teoría que condiciona a que el individuo de la especie humana es quien reúne los atributos para imputar responsabilidad penal. Fundamentos de la teoría del delito (Ramos Mejia, 2015, p. 24).

Probablemente, después de varios y serios debates jurídicos, en un futuro cercano y a medida que la investigación sobre el cerebro humano y la inteligencia artificial se vuelva más activa, surjan nuevos conocimientos. En cierta medida, se puede explorar la posibilidad de un paradigma tradicional y del concepto de responsabilidad penal, frente a que solo el ser humano reúne los atributos y habilidades esenciales para imputar un delito.

El artículo 6 de la Constitución establece de la siguiente manera la cláusula general de responsabilidad tanto para particulares como para servidores públicos: solamente las autoridades pueden hacer responsables a los particulares cuando estos infrinjan la Constitución o las leyes

(Contintución Política, 1991). De acuerdo con lo establecido en la normativa superior, se requiere que los miembros cumplan con las disposiciones de la Constitución y las leyes, lo que da lugar al surgimiento de su responsabilidad por parte de las autoridades judiciales o administrativas.

Descendiendo al ordenamiento jurídico penal, el legislador previó que la conducta punible puede ser realizada tanto por acción como por omisión (C.P. Art. 5, 2000). Por esta razón, el estatuto sustantivo está formulado en un sentido positivo, como aquella actividad que realiza un sujeto y produce consecuencias en el mundo jurídico (Art. 101 del C.P. "el que mate"), y en un sentido negativo, "como aquella inactividad voluntaria cuando existe un deber jurídico" (Art. 131 del C.P. "omisión de socorro") (Cuello Calón, 1948, p. 296).

Para resolver el problema jurídico centraré la atención en la conducta de omisión. De acuerdo con la definición del tratadista Cuello Calón, la conducta de omisión comprende cuatro elementos: la manifestación de la voluntad, una conducta pasiva o negativa (Inactividad), el deber jurídico de obrar y un resultado que produce consecuencias jurídicas. En el segundo inciso del articulo 25 Código Penal, el legislador determina la conducta punible cuando el sujeto se encuentra en una posición de garante.

Por lo tanto, el punto de partida para examinar una posible responsabilidad penal por omisión es preguntarse si alguien tenía una posición especial de deber, es decir, una posición de garante, frente a la persona perjudicada. De lo contrario, cualquier acusación se excluye. Sin embargo, si una persona tenía tal posición de garante, entonces se debe determinar si el hecho de haber permanecido inactiva en el evento relevante también se considera como una violación del deber atribuible a ella (C.P. Art. 5, 2000).

La pregunta crucial para resolver el problema jurídico es en qué circunstancias surge la relación especial con otra persona (Usuario) y, por lo tanto, una posición de garante (Diseñador o

Proveedor de IA), y qué obligaciones de garante resultantes deben cumplirse. La respuesta a esta pregunta no se deriva de una disposición legal, porque no la hay, pero hay avances de proyecto de ley que pueden brindarnos luz sobre cómo desarrollarlo.

Es importante señalar en este punto que el término "posición de garante" no implica una garantía en el sentido coloquial, es decir, una garantía de que nada suceda, sino atribuciones de omnipotencia y omnipresencia en los sistemas basados en IA que impliquen altos riesgos. Esta delimitación sirve para identificar a una persona que, debido a su relación con el sistema está obligada a actuar o prevenir ciertos resultados.

El proceso para definir el círculo de garantes, a quien debido a su relación especial con el bien jurídico protegido se le impone una obligación legal específica de actuar, es crucial. Sin embargo, si al final se llega a una responsabilidad penal de esta persona, depende de una variedad de factores a considerar en cada caso en particular.

Es de recalcar que la IA por sí sola no constituye un riesgo, sin embargo, la manipulación de estos prototipos como los ChatsBots Inteligentes si elevan considerablemente el riesgo particularmente en los casos que están comprometidos la privacidad y los datos personales de los usuarios. Es vital indicar que la teoría tradicional del delito puede hallar responsabilidad a los sujetos en cada fase del prototipo lo que implica que se cuenta con herramientas para su judicialización.

Desde un punto de vista jurídico penal necesitamos detenernos en dos hipótesis de participación de un sistema de inteligencia artificial en la comisión de un ciberdelito: instrumento y autor de este. En el caso de un instrumento delictivo, nos encontraríamos en una situación en el ChatBot inteligente, dadas sus infinitas capacidades, es utilizado por el hombre para cometer el delito. Como ya antes fue expuesto, esto sucede principalmente en delitos informáticos,

económicos y medioambientales, en tráfico de drogas y de seres humanos, en delitos de difamación, en la creación de fake news y en las lesiones a la privacidad o propiedad intelectual.

En el caso de utilizar el prototipo ChatBot Inteligente como herramienta del delito, debe imputársele responsabilidad al usuario del instrumento por dolo si la explota intencionalmente con el fin de delinquir y por negligencia del usuario o del programador, si la infracción se cometió por un mal funcionamiento del modelo inteligente, pudo haberse evitado gracias a su conducta activa evitando la realización del evento. Se trata de una afirmación basada en que, en estas situaciones, el ChatBot Inteligente no actúa como autor del delito gracias a su comportamiento causal autónomo del evento. Es el ser humano quien lo concibió, quiso y creo el evento utilizando la IA como herramienta.

En la segunda hipótesis, el ChatBot Inteligente implicado en la comisión del delito por su capacidad autónoma para aprender y tomar decisiones, podría considerarse la responsabilidad al proveedor o gestor del servicio en razón de la posición de garante por el grado de control sobre el dispositivo, lo que implica que el proveedor gestor o programador debe desarrollar una debida diligencia a través de protocolos que garanticen minimizar los riesgos ex ante, como identificar el origen de los datos a través del cual el modelo se está alimentando y poner controles frente a la información que pueda conllevar a que se estructure un ciberdelito.

La asignación de la responsabilidad al proveedor, diseñador e inclusive al usuario de los eventos causados por el ChatBot Inteligente se estructura cuando el mismo ha evadido un deber legal de monitorear el instrumento de acuerdo con el esquema del artículo 25 del código penal por las facultades que impone el deber de cuidado y la posición de garante para impedir el hecho delictivo.

Esto se desprende del principio de transparencia que pretende garantizar que los usuarios sean conscientes de la interacción con la aplicación puede generar riesgos, implicando al proveedor o gestor de la aplicación la advertencia de no revelar datos personales ni códigos, asimismo el usuario debe tener la oportunidad de comprender con que datos se ha entrenado el ChatBot Inteligente y cómo funciona técnicamente, es decir, el diseñador, programador, gestor o fabricante tiene la carga imperativa de que el prototipo debe ser explicable e interpretable no desde el punto de vista técnico, sino que el usuario deba estar en condiciones de comprender el funcionamiento del modelo en las características básicas que son relevantes para este.

La Unión Europea a través del Reglamento General de Protección de Datos (RGPD) contiene disposiciones de gran alcance para las decisiones automatizadas que garantizan la transparencia mediante obligaciones de información (artículos 13 y 14 del RGPD), un derecho de información (artículo 15 del RGPD) y derechos específicos en el uso de decisiones automatizadas, en la medida en que dichas decisiones produzcan efectos jurídicos o afecten significativamente a una persona afectada (artículo 22 del RGPD). Aunque no se trata de un régimen específico de IA, abarca todas las decisiones que se toman sin intervención humana.

6.9 Imputación objetiva en el marco del tipo objetivo de la conducta punible

Uno de los factores más importantes para determinar si una persona es responsable penalmente por el daño causado a otra es la existencia y el alcance de un vínculo causal entre la conducta y el daño ocasionado. En muchos casos, esta relación causal se limita al análisis desde una perspectiva fenomenológica según la cual, si se eliminara la acción u omisión entonces el daño infligido no se produciría. Sin embargo, la mera causalidad no es suficiente, por si sola, para atribuirle responsabilidad penal a un ciudadano (CP. Art. 26, 2000).

AUTOPUESTA EN PELIGRO DEL USUARIO CON CHATBOTS INTELIGENTES:

El punto de partida de la imputación objetiva es necesario verificar que la acción u omisión crean riesgos que se materializan en el futuro, pero, este acto debe ser significativo para el derecho penal. De esta manera la imputación objetiva está estrechamente relacionada no solo con la dimensión lógica, causalidad; teleológico, estándar determinación objetiva, idoneidad, manipulación, dominio, plausibilidad, sino también el concepto de ilegalidad de la acción humana (Roxin, Derecho Penal, Parte General, Fundamentos. La estrcutura de la Teoria del Delito, 2012, p. 342).

El código penal colombiano es un medio para evitar las consecuencias de la infracción de intereses jurídicos. Se impone al ciudadano de antemano y, por tanto, regula el comportamiento prohibido ex ante. De esta manera, la norma sustantiva penal sólo prohíbe acciones que sean jurídicamente relevantes y las que no lo son a partir de la valoración del riesgo creado. Por lo tanto, los actos levemente peligrosos ya no constituyen una violación a la ley penal. Para la que la acción u omisión resulta imputable objetivamente. El acto debe haber creado un riesgo mayor al permitido (Roxin, La Imputación Objetiva en el Derecho Penal, 2012, p. 98).

De acuerdo con el criterio de Roxin, lo que se debe validar es la razón de la causa que produjo el daño debido al comportamiento desplegado por un ciudadano. Es decir, consiste en una comprobación, primero, si la acción, desde el punto de vista fenomenológico la casualidad, ha creado un peligro o riesgo jurídicamente desaprobado. Segundo, si el resultado es producto del mismo peligro o riesgo, es decir, se comprobará el vínculo jurídico entre la conducta y el resultado, el juicio normativo de la imputación objetiva (Roxin, La Imputación Objetiva en el Derecho Penal, 2012, p. 98).

Estos dos principios fundamentales nos ayudan a distinguir entre la imputación objetiva de la acción y la imputación objetiva del resultado. En este contexto, la evaluación del riesgo creado

debe realizarse ex ante, mientras que la materialización del resultado y la relación causal deben analizarse ex post. En cuanto a la imputación objetiva de la acción, una vez establecida la causalidad natural de manera positiva, es posible atribuir objetivamente la acción si esta ha generado un riesgo que jurídicamente es reprobado, inadmisible o prohibido. Por otro lado, de manera negativa, se puede descartar la imputación objetiva comprobando que no se ha generado un riesgo jurídicamente reprobado o prohibido, utilizando cualquiera de los siguientes criterios objetivos: la prohibición de regreso, el principio de confianza, la culpa exclusiva del perjudicado o la reducción del riesgo.

Ahora bien, puede existir casos de concurrencia de riegos los cuales se presentan cuando la conducta ajena interrumpe el curso causal iniciado por la conducta, generando un aumento o anticipación temporal del resultado mediante la intensificación del peligro, un ejemplo es cuando la víctima herida mortalmente que recibe un nuevo disparo de un tercero, y a consecuencia de este, fallece. Una interrupción de nexos causales.

Además, existen los nexos causales desviados, lo que significa que la cadena causal no se rompe si se establece que el resultado ocurrió dentro de los límites jurídicamente reprobables establecidos por el comportamiento. Esto sucede independientemente de lo que el autor haya previsto sobre las consecuencias de su acción. Por ejemplo, si alguien empuja a otra persona al mar con la intención de que se ahogue, pero la víctima muere al golpear su cabeza contra una roca durante la caída.

Por otro lado, la “prohibición de regreso” actúa como un criterio que limita la atribución de la conducta que, de forma estereotipada, inocua y común, neutra o trivial, no se considera como participación en el delito cometido por otro (Roxin, 2012, p. 315). El principio de confianza se basa en la expectativa de que las personas actúen adecuadamente dentro de una actividad peligrosa

que es socialmente aceptable y que se lleva a cabo de manera colectiva o estructurada. Este principio implica que cuando una persona actúa bajo la premisa de que otros respetarán los límites de un riesgo aceptado, no se le puede atribuir responsabilidad penal por la conducta.

La atribución de responsabilidad a la víctima, o la auto exposición al peligro por parte de la víctima, implica que su propia conducta contribuye de manera significativa a la creación de un riesgo no permitido. Por otro lado, el concepto de riesgo permitido o la ausencia de riesgo se justifica por su beneficio social; sin embargo, si una persona sobrepasa esos límites de riesgo, debe asumir la responsabilidad objetiva por las consecuencias de su acción. Según este criterio, el riesgo insignificante no debería conllevar responsabilidad cuando solo afecta mínimamente el bien jurídico protegido. En lo que respecta a la reducción del riesgo, en esta situación, el individuo actúa provocando un resultado específico, pero al mismo tiempo evita que ocurra un daño mayor.

La imputación objetiva del resultado es un análisis de la materialización del riesgo y se aplica en delitos que tienen resultados específicos. Para este análisis, es fundamental no solo vincular la conducta con el resultado, sino también demostrar una conexión objetiva entre ambos. Esto significa que el resultado dañino debe estar directamente relacionado con un riesgo legalmente inaceptable generado por la acción.

Por lo tanto, la imputación objetiva es una herramienta que permite evaluar si se puede atribuir objetivamente un resultado a las acciones de una persona, sin tener en cuenta su intención o culpa. Esta evaluación determina si la acción incrementó el riesgo de un daño y si dicho riesgo era reprobable desde el punto de vista jurídico.

En términos contractuales, la imputación objetiva puede surgir de la aceptación tácita de riesgos entre las partes. En el contexto de un ChatBot inteligente, esto implicaría que el usuario asume ciertos riesgos al utilizar esta tecnología. Sin embargo, también se considera el contexto

específico en el que se produjo el evento, incluyendo el entorno digital y las medidas de seguridad aplicadas.

Además, estas teorías analizan la relación causal entre la acción y el resultado, determinando si la acción del ChatBot fue una causa directa del daño y si ese daño era previsible y evitable.

Mencionando lo anterior y volviendo al principio de autorresponsabilidad, en el contexto de un usuario que interactúa con un ChatBot inteligente, se puede entender como una situación en la que el usuario, de manera consciente y voluntaria, se expone a un riesgo al utilizar la tecnología de forma inapropiada o sin considerar advertencias claras sobre posibles peligros.

En relación con los fundamentos dogmáticos que discutimos antes, estos serían relevantes si un usuario, a pesar de las advertencias o recomendaciones, decide compartir información sensible, realizar acciones inseguras o seguir consejos de un ChatBot para un uso que no es el adecuado o que puede ser peligroso, asumiendo así la responsabilidad total de sus acciones. El ChatBot, como herramienta, no tendría imputación objetiva sobre los resultados negativos de las decisiones del usuario.

El usuario, en este caso, tiene el control absoluto sobre lo que decide hacer con la información proporcionada por el ChatBot. Si el usuario ignora las advertencias o se expone voluntariamente a un riesgo, la imputación de cualquier resultado negativo recae sobre el usuario, no sobre el ChatBot ni sus desarrolladores.

En el caso de la auto puesta en peligro tradicional, si un usuario es plenamente consciente del riesgo y sigue adelante, los desarrolladores del ChatBot o la plataforma que lo alberga no serían considerados responsables de los resultados de esas acciones. El ChatBot, siendo una herramienta,

actúa bajo las directrices y límites programados, y cualquier uso indebido por parte del usuario no podría ser imputado a los creadores de la herramienta.

Este concepto podría ser especialmente relevante en casos donde los ChatBot son utilizados en contextos delicados, como asesoría médica, legal o financiera, donde el usuario podría tomar decisiones basadas en las interacciones con la IA. Si el usuario actúa de forma irresponsable, omitiendo las precauciones necesarias o las advertencias dadas por la IA, se trataría de una auto puesta en peligro donde la responsabilidad es del propio usuario.

La auto puesta en peligro ocurriría cuando un usuario, consciente de los riesgos, decide ignorar las advertencias o recomendaciones del sistema, asumiendo así la responsabilidad total por las consecuencias de sus actos.

En el contexto de un delito de violación de datos personales, es importante considerar la responsabilidad del usuario cuando, de manera consciente y voluntaria, expone su información personal, a pesar de estar al tanto de los riesgos.

En el caso de la violación de datos, si un usuario decide compartir datos sensibles a través de un ChatBot sin tener en cuenta las advertencias de seguridad de la plataforma o la naturaleza del canal de comunicación, asume una parte considerable de la responsabilidad. Aunque el uso de un ChatBot debería ser seguro y cumplir con las normativas de protección de datos, si el usuario actúa de manera negligente, como ingresar información en un entorno no seguro, se aplicaría el principio de autorresponsabilidad.

El usuario, al controlar la información que decide compartir, se convierte en el principal responsable del riesgo al elegir qué datos proporcionar y en qué circunstancias. Si el ChatBot ofrece advertencias claras sobre la privacidad y el usuario las ignora, la violación de datos resultante podría considerarse una consecuencia de su propia decisión. En este caso, el usuario se

convierte en el único gestor del riesgo, y cualquier daño derivado de la divulgación de datos podría no ser atribuible al ChatBot o a sus operadores.

Si la plataforma que aloja el ChatBot ha implementado todas las medidas de seguridad necesarias y ha informado claramente al usuario sobre los riesgos de compartir información personal, entonces, si el usuario decide ignorar estas medidas y expone voluntariamente sus datos, no sería justo atribuir la responsabilidad penal por la violación de datos personales a los desarrolladores o proveedores. Según la teoría de imputación objetiva, esto podría considerarse un caso de auto exposición al peligro por parte del usuario, lo que limitaría la responsabilidad del proveedor del servicio.

Un ejemplo práctico sería imaginar un escenario en el que un ChatBot advierte al usuario que no debe compartir datos sensibles, como contraseñas o números de tarjeta de crédito, en un chat no cifrado. A pesar de la advertencia, el usuario elige introducir su número de tarjeta de crédito en la conversación con el ChatBot. Si esos datos son comprometidos posteriormente, la responsabilidad por la violación de datos personales podría recaer en el usuario, ya que ignoró las advertencias y tomó la decisión consciente de exponerse al riesgo.

6.10 Actuar bajo el propio riesgo

El actuar bajo propio riesgo se basan en la aceptación voluntaria de los riesgos por parte de los individuos, lo que puede excluir la responsabilidad de terceros. Esta doctrina se manifiesta de manera diversa en los sistemas jurídicos alemán, francés y angloamericano, adaptándose a las particularidades de cada contexto legal.

HANS-DETLEV Fischer, en su disertación de 1938 "Gefälligkeitsfahrt und vorvertragliche Haftung", discute el problema del actuar bajo propio riesgo, describiendo el

concepto como un espectro errante en el derecho de obligaciones. Esta observación sigue siendo válida, ya que el concepto no ha adquirido una definición dogmática clara. A menudo, se utiliza para describir diferentes situaciones legales sin una significancia dogmática específica (Hintze, 2016, p. 2).

El autor al realizar un análisis de la jurisprudencia alemana expone que los Jueces han empleado este concepto en diversas situaciones tales como, la realización de actividades peligrosas con consentimiento implícito, que consiste en la aceptación de riesgos conocidos implícitamente en actividades peligrosas puede llegar a excluir la responsabilidad de terceros, cuando la evaluación de la relación causal, es decir, si la acción de una persona ha aumentado el riesgo de un resultado dañino de manera significativa y ese riesgo era jurídicamente desaprobado, se puede imputar la responsabilidad. Además de analizar el contexto en el cual se lleva a cabo la actividad puede influir en la determinación de la responsabilidad.

Como ejemplo, la participación en viajes de cortesía, como ser un pasajero en un vehículo por buena voluntad, excluye generalmente la responsabilidad contractual del conductor. En el derecho alemán, esto se traduce en una exclusión de la responsabilidad basada en la falta de intención de establecer una relación contractual.

En el derecho francés utiliza el concepto de aceptación de riesgos para describir situaciones en las que una persona se expone voluntariamente a riesgos conocidos, eximiendo así de responsabilidad a otros. Esto es común en contextos como eventos deportivos y actividades recreativas peligrosas. Como aquellos participantes en eventos deportivos extremos asumen implícitamente los riesgos asociados, lo que puede excluir la responsabilidad de los organizadores.

En el derecho angloamericano, el principio de "assumption of risk" (asunción de riesgos) es fundamental para excluir la responsabilidad en casos donde la persona ha aceptado

voluntariamente los riesgos asociados a una actividad. Este principio se aplica en el ámbito contractual y delictual, especialmente en contextos laborales y recreativos. Como en el caso en que los propietarios de terrenos pueden ser eximidos de responsabilidad si se demuestra que los individuos entraron voluntariamente y conocían los riesgos asociados (Koteich, 2012, p. 254).

El Tratamiento dogmático plateado por Fischer del problema del actuar bajo propio riesgo, lo trata desde varias teorías, entre ellas la Teoría contractual: donde se proponen que la aceptación de riesgos puede derivarse de un consentimiento implícito en contextos específicos. Desde la Teorías de la situación: Sugieren que el contexto de la situación puede implicar la aceptación de ciertos riesgos, y de la Teoría causal donde se analizan el nexo entre la acción y el resultado, evaluando la previsibilidad y la evitabilidad del daño.

La jurisprudencia colombiana también ha desarrollado la acción a propios riesgos donde ha creado criterios en donde se puede excluir o modificar la imputación de una conducta punible particularmente, en donde la Corte Suprema de Justicia, Sala de Casación Penal 16636, 2003, establece los requisitos necesarios para que la acción a propio riesgo excluya o modifique la imputación al autor o partícipe. En la providencia desarrolla uno criterios orientadores para la aplicación en el caso concreto, en primer lugar, explica el deber del interprete en analizar en el caso concreto si la víctima tenía el poder de decidir si asume el riesgo y el resultado; posteriormente a ellos, que la víctima sea auto responsable, es decir, que conozca o tenga posibilidad de conocer el peligro que afronta con su actuar y que el actor no tenga posición de garante respecto de ella.

En relación con los fallos emitidos por la Alta Corte, la Sentencia de Casación 36824 de 2012 subraya la importancia de evaluar la ausencia de posición de garantía para determinar si se

realizó una acción a propio riesgo. Se destaca que la habilidad para reconocer y asumir un riesgo no suprime la necesidad de considerar la relación de garantía entre los involucrados en el acto.

En la Sentencia de Casación 46612 de 2018, la Corte enfatiza que para que se establezcan acciones a propio riesgo, es esencial que el individuo tenga la capacidad de decidir sobre la asunción del riesgo y sus consecuencias, sea autónomo en su decisión y que el otro individuo involucrado no posea una posición de garante hacia él.

Finalmente, en la Sentencia de Casación 50525 de 2019, la Corte especifica que, en el contexto de acciones a propio riesgo, los acusados no están facultados para manejar un bien jurídico que sobrepase su propiedad individual, como sería el caso de la seguridad pública. Este tipo de acciones presupone que la víctima tiene la disponibilidad de sus propios bienes jurídicos, pero esto no se extiende a los bienes de carácter colectivo.

Cancio Meliá aborda la autopuesta en peligro bajo el principio de autorresponsabilidad de la víctima, argumentando que el Derecho Penal no debe sancionar a quien asume riesgos y daños sobre sus propios bienes de manera consciente y voluntaria. Este principio reconoce el derecho de las personas a disponer de sus bienes y asumir las consecuencias de sus actos, lo que implica que, si una persona participa en una actividad riesgosa, el resultado perjudicial no puede ser imputado a un tercero que haya actuado conjuntamente, siempre y cuando dicho tercero no haya utilizado a la víctima como un instrumento ni sea garante de la protección de sus bienes (Cancio Meliá, 2005, p. 62).

En este sentido, Cancio Meliá sostiene que, en casos de autopuesta en peligro, la imputación objetiva del resultado a un tercero que facilita o colabora en la actividad riesgosa debe ser excluida. La responsabilidad recae en la víctima que controla la situación peligrosa, pues no es posible imputar el resultado a la conducta del tercero cuando es el propio sujeto pasivo quien tiene

el control del riesgo. Esta perspectiva normativa destaca la importancia del consentimiento consciente de la víctima en la determinación de la imputación penal (Cancio Meliá, 2005, p. 62).

En los casos, mencionados al inicio, donde se originaba un riesgo al interactuar con estos ChatsBots Inteligentes, como el Desafío del Penny Challenge del asistente de voz Alexa donde el riesgo fue asumido por los usuarios de TikTok que promovieron el desafío peligroso, que posteriormente fue replicado por la IA. Aquí, el riesgo de replicar información potencialmente dañina se asume inicialmente por los creadores del contenido y por los usuarios que deciden seguir dichos retos.

Desde el escenario de la responsabilidad de Amazon, como desarrollador, la empresa podría argumentar que el riesgo de seguir desafíos en redes sociales es asumido por los usuarios, especialmente cuando estos desafíos no tienen su origen en la plataforma de Amazon. Sin embargo, tiene la responsabilidad de asegurarse de que su producto no promueva comportamientos peligrosos. Como acción correctiva, Amazon actualizó el sistema de Alexa para evitar la promoción de desafíos peligrosos, demostrando una acción responsable para mitigar futuros riesgos.

En la situación de Tay de Microsoft, donde los usuarios de Twitter que interactuaron con Tay, alimentándolo con mensajes de odio y discriminación, asumieron el riesgo de distorsionar el comportamiento del ChatBot. Estos usuarios tomaron una acción a propio riesgo al contribuir intencionalmente a la corrupción del algoritmo de aprendizaje de Tay. Microsoft podría argumentar que el comportamiento de Tay fue una consecuencia de la interacción malintencionada de los usuarios, quienes actuaron por su cuenta y riesgo. No obstante, Microsoft tiene la responsabilidad de prever y prevenir tales usos indebidos de su tecnología. Por ende, Microsoft

suspendió el servicio de Tay y aprendió de la experiencia para implementar mejores controles y filtros en futuros desarrollos de ChatsBots.

Ahora bien, en la difusión de Contenidos Discriminatorios y Noticias Falsas, los usuarios de redes sociales que crean y comparten contenidos discriminatorios y noticias falsas asumen el riesgo de que estos contenidos sean replicados y amplificados por sistemas de IA. Esta acción a propio riesgo puede desencadenar consecuencias legales y sociales negativas para los individuos que inician estas cadenas de desinformación. Los desarrolladores de IA pueden argumentar que no son responsables del contenido generado por los usuarios, ya que los sistemas de IA aprenden y replican el comportamiento basado en datos externos. Sin embargo, deben implementar mecanismos para identificar y mitigar la propagación de contenidos dañinos. Lo que implica, de amanera imperiosa la Implementación de filtros y algoritmos más sofisticados para detectar y evitar la difusión de contenidos nocivos, y colaboración con reguladores para establecer estándares de responsabilidad y control.

6.11 Teoría propuesta

En esta investigación se centró en la utilización de la IA como medio de la comisión de conductas punibles, particularmente en la suplantación y captura de datos sensibles por los ChatsBots inteligentes consagrado en el artículo 269G del código penal, norma que fue adicionado por la ley 1273 de 2009. Esta conducta punible tiene por esencia la protección primordial de los datos sensibles o codificados en base de datos a finde evitar la captura de los mismos por vía electrónica.

Ahora bien, frente a la imputación Objetiva en la Interacción con ChatBot Inteligentes y Protección de Datos Personales, para el desarrollo de esta hay que partir de una premisa

fundamental donde la imputación objetiva en el contexto de ChatsBots inteligentes se basa en la evaluación de si la interacción y el manejo de datos personales por parte del ChatsBots aumentaron el riesgo de una captura ilícita de datos sensibles y si este riesgo era jurídicamente desaprobado.

Para el desarrollo de esta se debe considerar de manera responsables los elementos clave para su análisis, como el aumento del riesgo. La programación y el funcionamiento del ChatBot deben ser evaluados para determinar si incrementaron el riesgo de acceso no autorizado a datos personales. Las Medidas de Seguridad, se debe analizar si se implementaron medidas de seguridad adecuadas para prevenir la captura de datos codificados. Esto incluye cifrado de datos, autenticación de usuarios y monitoreo de actividades sospechosas. Desde el Contexto de la Interacción, el entorno digital en el que opera el ChatBot, incluyendo la plataforma y la red, debe ser considerado.

La imputación objetiva incluiría la evaluación de la robustez del entorno en términos de seguridad de datos. Como elemento clave final hay que considerar el Consentimiento y Transparencia. Es crucial que los usuarios den su consentimiento informado para el uso de sus datos personales. La falta de transparencia o consentimiento claro imputaría la responsabilidad al proveedor del ChatBot.

En la Aplicación Práctica donde haya violaciones de Datos, la imputación objetiva evaluaría si el diseño y las prácticas operativas del ChatBot contribuyeron significativamente al riesgo. Si se determinara que las medidas de seguridad fueron insuficientes o que el riesgo era previsible, la responsabilidad recaería sobre el proveedor del servicio.

Es decir, que para evitar que le es imputable una responsabilidad a los desarrolladores deben implementar medidas de seguridad desde el diseño y realizar evaluaciones de impacto regularmente. Esto incluye la actualización de sistemas y la capacitación en seguridad para

minimizar riesgos. Además de que los proveedores de ChatsBots deben ser transparentes sobre cómo se manejan los datos personales y obtener consentimiento explícito. Esto incluye informar a los usuarios sobre los riesgos y las medidas de protección implementadas.

Ahora bien, frente a la captura de datos sensibles contendió en el artículo 269G de la ley 599 de 2000 hay que tener los siguientes criterios orientadores a la hora de imputar el delito:

Transparencia y Documentación Técnica: la normativa de IA exige que los sistemas de IA sean transparentes y cuenten con documentación técnica adecuada. Durante la investigación, es crucial identificar si algún sistema de IA fue utilizado para obtener, compilar, sustraer o modificar datos personales de manera ilegal. La documentación técnica del sistema puede proporcionar evidencia crucial sobre cómo se llevó a cabo el delito.

Sistemas de IA de Alto Riesgo: si el sistema de IA utilizado en la comisión del delito se clasifica como de alto riesgo (por ejemplo, un sistema de reconocimiento biométrico), debe cumplir con estrictos requisitos normativos, incluidos la evaluación de impacto y las medidas de mitigación de riesgos. Verificar el cumplimiento de estos requisitos puede ayudar a establecer la falta de medidas adecuadas de seguridad y control.

Prohibiciones de la Normativa de IA: la normativa de IA prohíbe prácticas como el uso de técnicas subliminales para manipular comportamientos o explotar vulnerabilidades específicas. Si el sistema de IA utilizado empleó tales técnicas para obtener o manipular datos personales, esto podría agravar la imputación del delito y demostrar una intención deliberada de cometer el acto ilícito.

Cumplimiento con el Marco Jurídico de Protección de Datos Personales: en el marco jurídico de la Protección de Datos Personales establece la protección de datos personales de carácter sensible y expone varios principios para su tratamiento entre ellos legalidad, finalidad,

veracidad, transparencia, circulación restringida, seguridad y confidencialidad. Lo que implica que la IA debe reforzar la protección de datos personales. Durante la imputación, es esencial demostrar que el acusado no cumplió con las obligaciones dispuesta en la ley de habeas data y utilizó sistemas de IA para tratar o capturar datos personales sin el consentimiento adecuado o base legal (Ley 1581, 2012).

Responsabilidad de los Operadores de IA: la reciente regulación de la UE sobre la IA establece responsabilidades claras para los proveedores y responsables del despliegue de sistemas de IA. En el contexto del delito, es necesario identificar a los operadores responsables del sistema de IA utilizado y evaluar su grado de implicación en el acto delictivo. La falta de cumplimiento de las obligaciones establecidas en la normativa de IA puede ser una evidencia clave en la imputación.

Medidas de Seguridad y Control: la reglamentación de IA requiere que se implementen medidas de seguridad adecuadas para proteger los datos personales. Durante la investigación, se debe evaluar si el sistema de IA contaba con las medidas de seguridad necesarias y si hubo negligencia en su implementación, lo cual podría ser un factor agravante en la imputación del delito.

Un ejemplo del desarrollo de los anteriores criterios podría ser cuando en individuo utilizó un sistema de IA para acceder a una base de datos y sustraer datos sensibles sin autorización, luego vendió esta información a un tercero.

Fase de Investigación: 1) Identificación del Sistema de IA: Se identifica el sistema de IA utilizado, verificando su documentación técnica y si está clasificado como de alto riesgo. 2) Evaluación del Cumplimiento Normativo: Se comprueba si el sistema cumplía con las normativas de transparencia, documentación y evaluación de riesgos. 3). Prohibiciones y Prácticas Manipulativas: Se investiga si el sistema utilizó técnicas manipulativas o explotó vulnerabilidades

para sustraer los datos. 4). Cumplimiento de la Ley: Se verifica si el tratamiento de los datos personales cumplió con lo previsto en la ley. 5). Responsabilidad de los Operadores: Se determina la responsabilidad del proveedor y del responsable del despliegue del sistema de IA. 6). Medidas de Seguridad: Se evalúa la implementación de medidas de seguridad en el sistema de IA.

Fase de Imputación del Delito: con base en la investigación, se adecua la conducta en la norma prevista en el artículo 269G y si es típica y vulnero el bien jurídico tutelado, teniendo una inferencia razonable de autoría, destacando la falta de autorización, el uso de técnicas prohibidas y la responsabilidad de los operadores del sistema de IA, se procede a imputar cargos al investigado.

Esta aproximación asegura que se tomen en cuenta los aspectos regulatorios relevantes de la IA en la imputación del delito, proporcionando una base sólida para la acusación y destacando las violaciones específicas de la normativa aplicable.

Frente a la acción a propio riesgo, hay que tener en cuenta que el fundamento de esta teoría radica en la premisa de la auto puesta en peligro consciente e informada. Cuando un usuario interactúa con ChatsBots inteligentes, existe un grado de confianza depositada en la tecnología que puede resultar en la exposición de información sensible. En este contexto, el concepto de auto puesta en peligro se refiere a aquellas acciones voluntarias del usuario que, al confiar en la seguridad aparente de la tecnología, facilitan la comisión de delitos cibernéticos por parte de terceros.

Desde la perspectiva de la imputación objetiva, la responsabilidad del usuario surge cuando su conducta facilita objetivamente la realización de un resultado lesivo previsible. En este caso, el usuario, al interactuar con ChatsBots y proporcionar datos personales en contextos dudosos o no verificados, puede contribuir a la creación de un riesgo jurídicamente desaprobado. Así, el criterio

de la imputación objetiva permite atribuir responsabilidad al usuario cuando se prueba que su conducta incrementó el riesgo de sufrir un ataque o fraude cibernético.

En ese contexto, el comportamiento del usuario en plataformas digitales, especialmente al interactuar con ChatsBots inteligentes, juega un papel central en la generación de riesgo. Acciones como hacer clic en enlaces no verificados, ingresar información personal sin comprobar la legitimidad de la plataforma o confiar ciegamente en anuncios de premios y descuentos sin confirmación previa, pueden ser vistas como una auto puesta en peligro. En este sentido, el usuario estaría contribuyendo, aunque involuntariamente, al desarrollo de conductas punibles que involucran la recopilación de datos sensibles mediante técnicas de phishing o suplantación digital.

Bajo esa misma línea de pensamiento, la confianza excesiva e imprudente en la plataforma tecnológica, sin realizar comprobaciones básicas de seguridad, podría considerarse un elemento de culpa en la teoría de la auto puesta en peligro. A diferencia de una conducta negligente o culposa típica, en este contexto, la conducta del usuario adquiere relevancia cuando no toma precauciones mínimas, como verificar la autenticidad del sitio web o ChatBot, lo que facilita la ejecución de conductas delictivas por terceros.

En la interacción con estas aplicaciones inteligentes, la legislación podría considerar circunstancias agravantes cuando la información proporcionada voluntariamente por el usuario permita, de manera directa, la ejecución de delitos cibernéticos más graves, como estafas bancarias o transferencias no consentidas. Aquí, el enfoque estaría en el nivel de exposición voluntaria del usuario a un riesgo que debería haber previsto y evitado mediante medidas básicas de seguridad digital.

Aunque la teoría de la auto puesta en peligro justifica la atribución de cierta responsabilidad al usuario, debe establecerse un límite claro para no incurrir en una victimización secundaria. La

responsabilidad del usuario no puede ser absoluta, y deben tenerse en cuenta factores como la sofisticación del engaño o la complejidad de las técnicas utilizadas por los ciberdelincuentes. Solo se atribuirá responsabilidad al usuario cuando su conducta implique un riesgo previsible y evitable, considerando el estándar de una persona prudente en la misma situación.

En casos donde el usuario facilita la comisión del delito por su conducta imprudente, se puede considerar una forma de autoría mediata del ciberdelincuente, quien aprovecha la falta de precaución del usuario para ejecutar la conducta ilícita. De esta manera, la atribución de responsabilidad no exime la culpabilidad del autor principal, pero permite una valoración del grado de participación del usuario en la creación del riesgo.

Entonces, la teoría de atribución de responsabilidad al usuario basada en la auto puesta en peligro en la interacción con ChatsBots inteligentes permite una comprensión más amplia de la dinámica del riesgo en el entorno digital. Sin dejar de lado la importancia de la prudencia y la diligencia del usuario al interactuar con tecnologías que, aunque útiles, pueden implicar riesgos si no se manejan adecuadamente. La aplicación de esta teoría debe equilibrar la protección del usuario con la responsabilidad de fomentar comportamientos digitales seguros, sin dejar de sancionar adecuadamente a quienes exploten la confianza depositada en plataformas tecnológicas para cometer delitos.

7. Conclusiones

El estudio destacó la importancia de reconocer responsabilidades compartidas entre usuarios y empresas que desarrollan tecnologías de IA. Los usuarios que interactúan con ChatsBots inteligentes corren riesgo, especialmente cuando sus acciones son maliciosas. Sin embargo, las

empresas también deben anticipar y mitigar estos riesgos implementando controles adecuados y mejorando continuamente sus sistemas.

La imputación objetiva aplicada en la interacción entre los ChatsBots inteligentes y la protección de los datos personales se basa en una evaluación de mayor riesgo y los controles de seguridad a Implementar, en el contexto de interacción y consentimiento del usuario. Esta teoría garantiza la correcta asignación de responsabilidades y promueve un enfoque seguro y transparente para el procesamiento de datos personales en el entorno digital.

En los casos identificados y mencionados en la parte inicial de esta investigación, el riesgo propio y la responsabilidad jugaron un papel decisivo en la asignación de responsabilidad. Los usuarios que interactúan con la tecnología de inteligencia artificial asumen ciertos riesgos, especialmente si sus acciones son maliciosas o peligrosas, sin embargo, las empresas que desarrollan estas tecnologías también tienen la responsabilidad de anticipar y mitigar estos riesgos implementando controles adecuados y mejorando continuamente sus sistemas. La clave es encontrar un equilibrio que permita la innovación tecnológica sin comprometer la seguridad y la ética del uso de estas tecnologías.

Según Fisher desde la perspectiva "acción a propio riesgo" subraya la importancia de reconocer las responsabilidades compartidas entre los creadores de contenido y la tecnología empresarial. Los usuarios que crean riesgos intencionalmente tienen gran parte de la culpa. Sin embargo, las empresas que desarrollan e implementan tecnologías como los ChatsBots inteligentes tienen la responsabilidad de intervenir, lo que significa la responsabilidad de anticipar y mitigar los riesgos asociados con sus productos. Este enfoque enfatiza la necesidad de controles y medidas preventivas para proteger a los usuarios y a la sociedad en su conjunto de nuevos riesgos.

AUTOPUESTA EN PELIGRO DEL USUARIO CON CHATBOTS INTELIGENTES:

Las estimaciones objetivas al interactuar con ChatsBots inteligentes y proteger los datos personales se basan en una evaluación del aumento del riesgo, implementar medidas de seguridad en un entorno interactivo y el consentimiento del usuario, conlleva a garantizar que las responsabilidades se asignen correctamente, promoviendo así prácticas seguras y transparentes para el procesamiento de datos personales en el entorno digital.

En el contexto del principio de responsabilidad personal en los casos en que un usuario ignora intencionalmente las advertencias de seguridad y se produce una violación de datos personales, la auto puesta en peligro puede ser un argumento clave para limitar o excluir la responsabilidad penal de los proveedores de servicios de ChatBot, trasladando la responsabilidad al usuario que decidió correr el riesgo.

Colombia y otros países carecen de regulaciones específicas para sistemas autónomos, lo que conlleva a la necesidad de nuevos marcos legales que logren abordar adecuadamente los desafíos emergentes. Este estudio demuestra que es fundamental evaluar cómo se pueden adaptar los marcos legales existentes para garantizar una protección efectiva de los derechos de las personas afectadas por las tecnologías de IA.

La autonomía de los sistemas de inteligencia artificial, especialmente los ChatsBots, plantea importantes desafíos a los procesos penales. La capacidad de estos sistemas para funcionar de forma autónoma requiere un análisis en profundidad de cómo sus acciones pueden atribuirse a individuos y en qué condiciones los diseñadores, desarrolladores u operadores de los sistemas pueden quedar excluidos de responsabilidad penal.

La clave para una regulación eficaz es encontrar el equilibrio que permita la innovación tecnológica sin comprometer la seguridad y la ética del uso de estas tecnologías. Las empresas deben ser transparentes sobre cómo se procesan los datos personales, a través de una ventana

emergente, informar los términos, condiciones y riesgos a los que se expone el usuario cuando se inicia la interacción con el chatbot a fin de obtener o no el consentimiento, estos términos deben contener información precisa que esta interactuando con un Bot y los riesgos a los que se expone el usuario y las posibles vulnerabilidades en seguridad si coparte su datos y códigos sensibles que puedan derivar en afectación a sus derechos.

Referencias

Abogado Digital. (30 de Agosto de 2019, p. 1). *Primer crimen cometido mediante inteligencia artificial: simulan la voz de CEO para solicitar deposito urgente.* Obtenido de https://www.abogado.digital/primer-crimen-cometido-mediante-inteligencia-artificial-simulan-la-voz-del-ceo-para-solicitar-deposito-urgente/

Acurio del Pino, S. (2016, p. 24). *Delitos Informáticos: Generalidades.* Quito, Ecuador. Obtenido de https://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf

Alibaba. (2018, p. 1). *Bert*. Obtenido de https://www.alibabacloud.com/help/en/machine-learning-platform-for-ai/latest/bert-text-vectorization

Aliseda Llera, A. (2007, p. 28). Emerge una nueva disciplina las ciencias cognitivas. *Ciencias 88*, 22-31. Obtenido de https://www.revistacienciasunam.com/images/stories/Articles/88/02/las%20ciencias%20cognitivas.pdf

Amazon. (2014, p. 3). *Alexa*. Obtenido de https://developer.amazon.com/es-ES/alexa

Arthur, L. S. (03 de 03 de 1959, p. 215). Some studies in machine learning using the game of checkers. *IBM Journal*(3), 210-229. Obtenido de https://ieeexplore.ieee.org/document/5389202?arnumber=5389202

Bacigalupo Saggese, S. (1997, p. 135). *LA RESPONSABILIDAD PENAL DE LAS PERSONAS JURIDICAS. Un estudio sobre el sujeto del derecho penal.* Madrid: Universidad Autonóma de Madrid, Facultad de Derecho.

BlackBerry. (02 de Febrero de 2023, p. 2). ChatGPT ya puede usarse en ciberataques. WATERLOO, CANADA. Obtenido de

https://www.blackberry.com/us/en/company/newsroom/press-releases/2023/chatgpt-may-already-be-used-in-nation-state-cyberattacks-say-it-decision-makers-in-blackberry-global-research

Brenner, S. (2013, p 29). *HUMANS AND HUMANS+: TECHNOLOGICAL ENHANCEMENT* (Vol. 19). Boston: Boston University. Obtenido de file:///C:/Users/User/Downloads/ssrn-2360756.pdf

Bromley, A. G. (07 de 1982, p. 200). Charles Babbage´s Analytical Engine. *Annals of the History of Computing 1838*, *4*(3), 196-217. Obtenido de https://anthony-zhang.me/blog/rod-logic/an-engine.pdf

brunner , J. J. (2 de Agosto de 2005, p. 1). *Brunner.cl*. Obtenido de https://brunner.cl/2005/08/cibercultura-la-aldea-global-dividida/

C.P. Art. 5. (24 de Julio de 2000).

Cámara de Representante de los Estados Unidos. (03 de 02 de 2022, p. 1). Proyecto de Ley de Responsabilidad Algorítmica. Recuperado el 09 de 01 de 2024, de https://www.wyden.senate.gov/imo/media/doc/Algorithmic%20Accountability%20Act%20of%202022%20Bill%20Text.pdf

Cancio Meliá, M. (2005, p. 62). Conductas de la victima e imputacion objetiva en el derecho penal. Estudios sobre los ámbitos de responsabilidad de la victima y autor en actividades arriesgadas. *Revista Ajuris*, 53-88. Obtenido de https://www.mundusline.com/wp-content/uploads/5-Cancio-Melia-Manuel-Aproximacion-a-la-teoria-de-la-imputacion-objetiva.pdf

Castells, M. (2000, p. 61). *LA SOCIEDAD RED* (Segunda ed.). (C. Martínez Gimeno, & J. Alborés, Trads.) Madrid: Alianza Editorial S.A. Obtenido de https://amsafe.org.ar/wp-content/uploads/Castells-LA_SOCIEDAD_RED.pdf

Centro Cibernético de la Policía Nacional. (2020, p. 22). Balance Cibercrimen. Bogotá. Obtenido de https://caivirtual.policia.gov.co/sites/default/files/observatorio/Balance%20anual%202023_0.pdf

Centro Cibernético de la Policía Nacional. (2022, p. 10). Tendencias del Cibercrimen Colombia. Obtenido de https://caivirtual.policia.gov.co/sites/default/files/observatorio/Balance%20anual%202022.pdf

Código Penal [CP]. Ley 599. (24 de Julio de 2000). Código Penal Colombiano. Colombia.

Comisión Europea [CE], COM 168. (2019, p. 6). *Construyendo Confianza en la Inteligencia Artificial Centrada en el Ser Humano.* Comunicación de la Comisión al Parlamento Europeo , Bruselas. Obtenido de https://digital-strategy.ec.europa.eu/en/library/communication-building-trust-human-centric-artificial-intelligence

Comisión Europea. (2018, p 237). *comunicación de la comisión al parlamento europeo, al consejo, al comité económico y social europeo y al comité de las regiones: Inteligencia Artificial para Europa.* Bruselas.

Comisión Europea. (2018, p. 1). *COMUNICACIÓN DE LA COMISIÓN AL PARLAMENTO EUROPEO, AL CONSEJO EUROPEO, AL CONSEJO, AL COMITÉ ECONÓMICO Y SOCIAL EUROPEO Y AL COMITÉ DE LAS REGIONES.* Bruselas: COM(2018) 795 final.

Obtenido de https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:52018DC0795

Comisión reguladora de Telecomunicaciones, Resolución 2258 (Comisión de regulación de comunicaciones 2009, p. 1). Obtenido de https://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?dt=S&i=38498

Congreso de la Republica de Perú, Ley No. 31813. (05 de 07 de 2023). Ley de promoción de la IA para el Desarrollo Económico y Social del País. Lima. Recuperado el 15 de 01 de 2024, de https://cdn.www.gob.pe/uploads/document/file/5038703/ley-que-promueve-el-uso-de-la-inteligencia-artificial-en-fav-ley-n-31814.pdf?v=1692895308

Congreso de la Republica, Ley 1266, Art. 3. (2008). Ley Estatutaria de Habeas Data.

Congreso de la Republica, Ley 1581. (2012). *Ley Estatutaria de Protección de datos Personales.* Bogotá: Gaceta Oficial.

Consejo de Europa. (1999, p. 1). *Convenio sobre ciberdelincuencia.* Obtenido de https://rm.coe.int/16802fa403

Consejo de Europa. (2001, p. 1). Convenio sobre la ciberdelincuencia, (pág. 26). Budapest. Obtenido de https://www.oas.org/juridico/english/cyb_pry_convenio.pdf

Constitución Política. (1991). Bogotá: Gaceta Oficial.

Corvalán, J. G. (1 de 04 de 2018, p. 301). *Revista de Investigaciones Constitucionales*, 294-316. doi:https://doi.org/10.5380/rinc.v5i1.55334

CP. Art. 26 (24 de Julio de 2000).

Cuello Calón, E. (1948, p. 296). *Derecho Penal.* Barcelona: Bosch.

Decreto del presidente de la Federación Rusia N. 490 (10 de 10 de 2019). Obtenido de https://fzakon-ru.translate.goog/ukazy-prezidenta/ukaz-prezidenta-rf-ot-15.02.2024-n-124/?_x_tr_sl=ru&_x_tr_tl=es&_x_tr_hl=es-419&_x_tr_pto=sc

DeepMind. (19 de 05 de 2017, p. 2). *AlphaGo. DeepMind*. Recuperado el 18 de 05 de 2023, de https://www.deepmind.com/research/highlighted-research/alphago

Defense Advanced reearch Projects Agency. (03 de 12 de 2020, p. 1). Obtenido de https://www.darpa.mil/program/aircrew-labor-in-cockpit-automation-system

Deloitte. (03 de 2014, p. 4). Disruption ahead, Deloitte´s point of view on IBM Watson. Obtenido de https://docplayer.net/16002085-Disruption-ahead-deloitte-s-point-of-view-on-ibm-watson.html

Departamento Nacional de Planeación. (2019, p. 1). *Consejo Nacional de Política Económica y Social, CONPES 3975.* Bogotá, Colombia. Obtenido de https://colaboracion.dnp.gov.co/CDT/Conpes/Económicos/3975.pdf

Departamentro de Seguridad Nacional, Estados Unidos. (30 de 08 de 2023, p. 1). Normas mínimas para licencias de conducir y tarjetas de identificación aceptables por agencias federales para fines oficiales. *(2023-18582)*, 60056 - 60104. Washington D. C.: Registro Federal del Gobierno de los Estados Unidos. Recuperado el 10 de 01 de 2024, de https://www.federalregister.gov/documents/2023/08/30/2023-18582/minimum-standards-for-drivers-licenses-and-identification-cards-acceptable-by-federal-agencies-for

EnciclopedIA. (01 de 03 de 2023, p. 2). *Tu diccionario de la Inteligencia Artificial y la Analítica Avanzada*. Obtenido de https://decidesoluciones.es/encicloped-ia/

Estado de Wisconsin Vs. Eric L. Loomis, 2015AP157-CR (Corte Suprema de Wisconsin 13 de Julio de 2016, p. 20). Obtenido de https://www.courts.ca.gov/documents/BTB24-2L-3.pdf

Estados Unidos, Oficina de Derechos de Autor. (30 de 08 de 2023, p. 1). Estudio de inteligencia artificial. *Noticia, 88(167)*. Registro Federal. Recuperado el 05 de 01 de 2024, de https://www.govinfo.gov/content/pkg/FR-2023-08-30/pdf/2023-18624.pdf

Estados Unidos, Orden Ejecutiva No. 13960. (08 de 12 de 2020, p. 1). Promoción del uso de inteligencia artificial confiable en el Gobierno Federal. *85(236)*. Washington D.C.: Registro Federal. Recuperado el 09 de 01 de 2024, de https://www.govinfo.gov/content/pkg/FR-2020-12-08/pdf/2020-27065.pdf

Estados Unidos, Orden Ejecutiva No. 13859. (11 de 02 de 2019, p. 3). Mantener el liderazgo estadounidense en inteligencia artificial. 3967 - 3972. (D. Trump, Ed.) Washington D. C.: Registro Federal del Gobierno de los Estados Unidos. Recuperado el 09 de 01 de 2024, de https://www.federalregister.gov/documents/2019/02/14/2019-02544/maintaining-american-leadership-in-artificial-intelligence

Estados Unidos, Orden Ejecutiva No. 14110. (30 de 10 de 2023, p. 1). Desarrollo y uso seguro y confiable de la inteligencia artificial. *88(210)*, 75191 - 75226. Registro Federal. Recuperado el 10 de 01 de 2024, de https://www.govinfo.gov/content/pkg/FR-2023-11-01/pdf/2023-24283.pdf

Europol. (2024, p. 10). *Internet Organised Crime Threat Assessment (IOCTA).* Agencia de la unión Europea, Luxemburgo. doi:doi:10.2813/442713

Federación Rusa, Decreto del Presidente No. 490. (10 de 10 de 2019, p. 1). Sobre el desarrollo de la inteligencia artificial en la Federación de Rusia. Recuperado el 15 de 01 de 2024, de http://www.kremlin.ru/acts/bank/44731

Francois Revel, J. (1989, p. 7). *El conocimiento inútil.* (J. Bochaca, Trad.) Barcelona, España: Planeta S.A. Obtenido de file:///C:/Users/LEO/Downloads/toaz.info-jean-francois-revel-el-conocimiento-inutil-pr_081dd5fc712ed0cac9fb1166b2f494e9.pdf

Gañán, H. (01 de Enero de 2019, p. 1). Un Tesla Autónomo atropella a un robot ruso y se da a la fuga. Obtenido de https://www.elplural.com/leequid/omg/un-tesla-autonomo-atropella-a-un-robot-ruso-y-se-da-a-la-fuga_209152102

García Vega, L. (1986, p. 34). La Teoría Neuropsicológica de HEBB: Antecedentes de la psicología cognitiva. *Historia de la psicología, 7*(3), 31-38. Recuperado el 09 de 05 de 2023, de https://journals.copmadrid.org/historia/archivos/fichero_salida20210910141414147000.pdf

Gascón Marcén, A. (2020, p. 3). *El impulso japones a la regulación internacional de las tecnologías de la información y la comunicación.* Zaragoza. Recuperado el 15 de 01 de 2024, de https://aeje.org/wp-content/uploads/2020/10/M03P02.pdf

Gibson, W. (1984). *Neuromante.* (J. Arconada Rodríguez, & J. Ferreira Ramos, Trads.) Titivillus. Obtenido de https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwiIm6HV2PmEAxWRm4QIHWpiBHIQFnoECDUQAQ&url=https%3A%2F%2Fprepa.unimatehuala.edu.mx%2Fpluginfile.php%2F7362%2Fmod_glossary%2Fattachment%2F1024%2FNeuromante%2520-%2520William%2520Gibson

Gómez Llinás, D. A. (06 de Diciembre de 2021, p. 3). *El Impacto de la Inteligencia Artificial Sobre el Ser Humano y Sobre su Seguridad.* Obtenido de

AUTOPUESTA EN PELIGRO DEL USUARIO CON CHATBOTS INTELIGENTES: https://www.umng.edu.co/documents/20127/0/EL+IMPACTO+DE+LA+INTELIGENCIA+ARTIFICIAL.pdf/8007b6ca-5b02-b7f1-4a64-4a27ac3a9060?t=1639080191820

Hanson Robotics. (2016, p. 3). *Sophia*. Obtenido de https://www.hansonrobotics.com/sophia/

Hintze, A. (14 de 11 de 2016, p. 2). Understanding the four types of AI, from reactive robots to selfaware beings" The Conversation. Obtenido de https://theconversation.com/understanding-the-four-types-of-ai-from-reactive-robots-to-self-aware-beings-67616

Hobsbawm, E. (1996). *The Age of Revolution: 1789-1848.* New York: VINTAG E BOOK S. Recuperado el 09 de 05 de 2023, de https://files.libcom.org/files/Eric%20Hobsbawm%20-%20Age%20Of%20Revolution%201789%20-1848.pdf

Hobsbawm, E. (2009, p. 30). *La Era de la revolución 178-1848.* (F. Ximénez de Sandoval, Trad.) Buenos Aires: Critica. Obtenido de https://cheirif.wordpress.com/wp-content/uploads/2016/08/eric-hobsbawm-la-era-de-la-revolucic3b3n-1789-1848-crc3adtica-2009.pdf

Hunt, E. (24 de Marzo de 2016, p. 1). Tay, el chatbot de IA de Microsoft, recibe un curso intensivo sobre racismo de Twitter. Obtenido de https://www.theguardian.com/technology/2016/mar/24/tay-microsofts-ai-chatbot-gets-a-crash-course-in-racism-from-twitter

Hunt, E. (24 de 03 de 2016, p. 2). Tay, el chatbot de IA de Microsoft, recibe un curso intensivo sobre racismo de Twitter. *The Guardian*. Obtenido de https://www.theguardian.com/technology/2016/mar/24/tay-microsofts-ai-chatbot-gets-a-crash-course-in-racism-from-twitter

Indonesia, Secretaría Nacional de Inteligencia Artificial. (01 de 08 de 2020, p. 1). *Estrategia Nacional de IA 2020-2045*. Recuperado el 20 de 01 de 2024, de https://ai-innovation.id/images/gallery/ebook/stranas-ka.pdf

Johnson , J., Karpathy, A., & Fei - Fei, L. (2016, p. 1). DenseCap: Fully Convolutional Localization Networks for Dense Captioning. *The Computer Vision Foundation*, 4565-4574. Obtenido de https://openaccess.thecvf.com/content_cvpr_2016/papers/Johnson_DenseCap_Fully_Convolutional_CVPR_2016_paper.pdf

Kaplan, A., & Haenlein, M. (11 de 2018, p. 18). Siri, Siri, in my hand: Who's the fairest in the land? On the interpretations, illustrations, and implications of artificial intelligence. *Business Horizons*, 15-28. doi:DOI:10.1016/j.bushor.2018.08.004

Kleinsteuber, H. J. (2002, p. 50). El surgimiento del ciberespacio: la palabra y la realidad. *Dialnet, 2*, 47-64. Obtenido de https://dialnet.unirioja.es/servlet/articulo?codigo=616201

Koteich, M. (2012, p. 254). assumption of risk" (asunción de riesgos) es fundamental para excluir la responsabilidad en casos donde la persona ha aceptado voluntariamente los riesgos asociados a una actividad. 254-265. Obtenido de https://bdigital.uexternado.edu.co/server/api/core/bitstreams/d942ebb1-fe8d-4c27-9109-a4cd0aff22d7/content

La Vanguardia. (28 de 12 de 2021, p. 1). *Alexa pide a una niña de 10 años que ponga una moneda en el enchufe*. Recuperado el 2021 de 05 de 2023, de https://www.lavanguardia.com/tecnologia/20211228/7957447/alexa-reto-viral-tiktok-moneda-enchufe-pmv.html

Laboratorio Aeronáutico de la Universidad de Cornell. (1957, p. 7). *THE PERCEPTRON*. Reporte, BUFALO, NEW YORK. Recuperado el 09 de 05 de 2023, de https://blogs.umass.edu/brain-wars/files/2016/03/rosenblatt-1957.pdf

Laney, D. (21 de Febrero de 2001). *3D data management: Contrilling data volumen, velocity and variety*. . Obtenido de http://blogs.gartner.com/doug-laney/files/2012/01/ad949-3D-Data-Management-Controlling-Data-Volume-Velocity- and-Variety.pdf

Ley 1581. (17 de Octubre de 2012).

Ley 1774. (2016). *Ley de protección animal.* Bogotá: Gaceta Oficial.

Ley 599, Titulo III. Cap. VII (24 de Julio de 2000).

Licklider, J. (03 de 1960). Man-Computer Symbiosis. IRE Transactions on Human Factors in Electronics. Obtenido de http://groups.csail.mit.edu/medg/people/psz/Licklider.html

Lopéz, J. M. (21 de 12 de 2022, p. 2). *Hipertextual.* Obtenido de https://hipertextual.com/2022/12/elektro-robot-humanoide

Manyika, J., Dean , J., Hassabis , D., Croak, M., & Pichai , S. (2018, p. 5). *IA. Google.* Obtenido de https://ai.google/static/documents/google-why-we-focus-on-ai-es-419.pdf

Marguin , J. (1994). *Historia de los instrumentos y máquinas de calcular: Tres siglos de la mecánica del pensamiento 1642-1942.* Paris: Prensas universitarias de Francia.

Microsoft. (2014, p. 1). *Cortana*. Obtenido de https://support.microsoft.com/es-es/topic/-qué-novedades-hay-con-cortana-000201ca-f20c-d362-41d1-303d59cfb655

Microsoft. (2022, p. 3). Azure Bot Service. Obtenido de https://azure.microsoft.com/es-mx/products/bot-services/?ef_id=_k_Cj0KCQjwmZejBhC_ARIsAGhCqne-0gAGMR5sx2-cxQXIG0ox7BSoxxjHi2YH4x9QLWb4moLek_wS3roaAn_XEALw_wcB_k_&OCID=

AIDcmm3804ythc_SEM__k_Cj0KCQjwmZejBhC_ARIsAGhCqne-0gAGMR5sx2-cxQXIG0ox7BSoxxjHi2YH4x9QLW

Mireille, D. M., & Ulrich, S. (2008, p. 170). Dominar la complejidad en el ciberespacio global: la armonización del derecho penal relacionado con la informática. *Société de législation comparée*, 127-202.

Monleón Getino, A. (25 de Noviembre de 2015, p. 430). El Impacto del Big-data en la Sociedad de la Información. Significado y utilidad. *Historia y Comunicación Social, 20*(2), 427-445. Obtenido de http://dx.doi.org/10.5209/rev_HICS.2015.v20.n2.5139

Montero Mora, A., Méndez Muñoz, G., & Domínguez Rodríguez , J. R. (2008, p. 7). *Metodologías de diseño de comportamientos para AIBO ERS7.* Madrid: Universidad Complutense. Obtenido de https://core.ac.uk/download/pdf/19712936.pdf

Naciones Unidas. (2024, p. 76). *Gobernanza de la Inteligencia Artificial en beneficio de la Humanidad.* A/74/821. Obtenido de https://www.un.org/sites/un2.un.org/files/governing_ai_for_humanity_final_report_es.pdf

NASA. (16 de 07 de 2006, p. 2). *Nasa.gov.* Recuperado el 18 de 05 de 2023, de https://www.nasa.gov/ames/about-ames/

Obama, B. (13 de 04 de 2013, p. 4). *The White House.* Obtenido de https://obamawhitehouse.archives.gov/blog/2013/04/02/brain-initiative-challenges-researchers-unlock-mysteries-human-mind

Observatorio de Inteligencia Artificial. (28 de 10 de 2016, p. 1). *Observatorio IA.* Obtenido de https://observatorio-ia.com/informe-sobre-inteligencia-artificial-de-la-casa-blanca

OpenAI. (2021, p. 2). *OpenAI.com*. Obtenido de https://platform.openai.com/docs/introduction/key-concepts

Parlamento Canadiense, Proyecto de Ley C-27. (s.f.). *Ley de datos e Inteligencia Artificial.* Recuperado el 17 de 01 de 2024, de https://www.parl.ca/DocumentViewer/en/44-1/bill/C-27/first-reading

Pérez Vidal, A. J., Castro González , Á., Alonso Martín , F., Castillo, J. C., & Salichs, M. A. (2017, p. 838). Evolución de la Robótica social y nuevas tendencias. 836-843. doi:https://doi.org/10.17979/spudc.9788497497749.0836

Posada Maya, R. (2017, p. 88). *LOS CIBERCRIMENES. UN NUEVO PARADIGMA DE CRIMINALIDAD UN ESTUDIO DEL TITULO VII BIS DEL CODIGO PENAL COLOMBIANO.* Bogotá: Grupo Editorial IBAÑEZ. doi:http://dx.Doi.Org/10.15425/2017.103

Prieto Meléndez, R., Padrón Godínez, A., Herrera, A., & Pérez, J. L. (10 de 2000, p. 4). EL MODELO NEURONAL DE McCULLOCH Y PITTS, Interpretación Comparativa del Modelo. *Conferencia: XV Congreso Nacional de Instrumentación*, 6. Recuperado el 08 de 05 de 2023, de https://www.researchgate.net/publication/343141076_EL_MODELO_NEURONAL_DE_McCULLOCH_Y_PITTS_Interpretacion_Comparativa_del_Modelo

Ramos Mejía, E. (2015, p. 24). La teoría del Delito desde Von Liszt y Beling a Hoy. *Revista Universidad de Mendoza*, 16-34. Obtenido de https://core.ac.uk/download/pdf/268220158.pdf

Reino Unido, Departamento de Ciencia, Innovación y Tecnología (DSIT). (2024). *Un enfoque pro-innovación a la regulación de la IA* (ISBN 978-1-5286-4565-2 ed.). Londres: Archivo

Nacional. Obtenido de https://assets.publishing.service.gov.uk/media/65c1e399c43191000d1a45f4/a-pro-innovation-approach-to-ai-regulation-amended-governement-response-web-ready.pdf

Rijhwani, M. (14 de 05 de 2021, p. 1). AIML - A Language for Chatbot. Obtenido de https://www.analyticsvidhya.com/blog/2021/05/aiml-a-language-for-chatbots/

Ríos Estavillo, J. J. (1997, p. 116). *Derecho e Informática en Mexico.* Mexico D.F.: Universidad Nacional Autónoma de Mexico. Obtenido de https://biblio.juridicas.unam.mx/bjv/detalle-libro/147-derecho-e-informatica-en-mexico-informatica-juridica-y-derecho-de-la-informatica

Rojas , R., & Hashagen, U. (2000, p. 29). *The First Computers—History and Architectures.* London, England: Massachusetts Institute of Technology. Obtenido de https://doc.lagout.org/science/0_Computer%20Science/0_Computer%20History/The%20First%20Computers%20-%20History%20and%20Architectures.pdf

Romeo Casanoba, C. M. (1988, p. 118). *Poder informático y seguridad jurídica: la función tutelar del derecho penal ante las nuevas tecnologías de la información.* Fundesco.

Roxin, C. (2000, p. 153). *Autoría y Dominio del Hecho en Derecho Penal* (Vol. Séptima Edición Alemana). (J. Cuello Contreras, & J. L. Serrano González de Murillo , Trads.) Barcelona, España: Marcial, Pond, Ediciones Jurídicas y Sociales S.A.

Roxin, C. (2012, p. 342). *Derecho Penal, Parte General, Fundamentos. La estructura de la Teoría del Delito* (Segunda ed.). (D. Luzón Peña, & M. Diaz, Trads.) Lima: Civitas.

Roxin, C. (2012, p. 98). *La Imputación Objetiva en el Derecho Penal* (Segunda ed.). (M. Abanto Vásquez, Trad.) Lima: Editora y Librería Jurídica Grijley.

Russell, S., & Norvig, P. (2008, p. 1066). *Inteligencia Artificial un enfoque moderno.* (J. Corchado Rodriguez, Trad.) Pearson Educación S.A. Obtenido de https://luismejias21.files.wordpress.com/2017/09/inteligencia-artificial-un-enfoque-moderno-stuart-j-russell.pdf

Sáez Vacas, F. (1987, p. 68). *COMPUTADORES PERSONALES, Hacia un mundo de maquinas.* Madrid, España: GRAFUR S.A. Obtenido de https://oa.upm.es/5411/1/Computadores_personales_Hacia_un_mundo_de_maquinas_informaticas.pdf

Salas, J. (28 de enero de 2016). La inteligencia artificial conquista el último tablero de los humanos. Una máquina vence por primera vez a un jugador profesional del milenario juego chino Go. *El País*. Obtenido de http://elpais.com/elpais/2016/01/26/ciencia/1453766578_683799.html

Searle, J. (1980). *Actos de habla.* Madrid, España: Ediciones Cátedra. Obtenido de https://www.textosenlinea.com.ar/libros/Searle%20-%20Actos%20de%20Habla.pdf

SoftBank Robotics. (2018, p. 1). *softbankrobotics.* Obtenido de https://www.ald.softbankrobotics.com/en/robots/pepper.

Steinhoff, J. (2019). The Automation of Automating Automation: Automation in the AI Industry. *The University of Western Ontario*, 5. Obtenido de https://www.academia.edu/39636662/The_Automation_of_Automating_Automation_Automation_in_the_AI_Industry

Stone, M., Aravopoulou, E., & Ekinci, Y. (2020, p. 188). Artificial intelligence (AI) in strategic marketing decision-making: A research agenda. *Strategic Marketing, 33*(2), 183-200. doi:10.1108/bl-03-2020-0022

The Science News. (28 de 06 de 2023). *Science Tenology Innovation Japan.* Obtenido de https://sj.jst.go.jp/news/202306/n0628-03k.html

Turing, A. (2010, p. 3). Maquinaria computacional e Inteligencia (1950). (C. Fuentes Barassi , Trad.) *Universidad de Chile*, 1-22. Obtenido de http://xamanek.izt.uam.mx/map/cursos/Turing-Pensar.pdf

UE, COM 986. (2023, p. 1). *Reglamento de Inteligencia Artificial.* Bruselas. Obtenido de https://www.consilium.europa.eu/es/press/press-releases/2023/12/09/artificial-intelligence-act-council-and-parliament-strike-a-deal-on-the-first-worldwide-rules-for-ai/pdf

UNESCO. (15 de 01 de 2024, p. 1). *Globalpolicy.AI*. Obtenido de https://globalpolicy.ai/en/about/

Unión Europea [UE], COM 65. (2020, p. 1). *Libro Blanco. Sobre la Inteligencia Artificial - Un Enfoque Europeo orientado hacia la excelencia y confianza.* Bruselas. Obtenido de https://commission.europa.eu/document/download/d2ec4039-c5be-423a-81ef-b9e44e79825b_es?filename=commission-white-paper-artificial-intelligence-feb2020_es.pdf

Weizenbaum, J. (Enero de 1966, p. 40). ELIZA - A Computer Program For de Study of Natuaral language Communication Between Man and Machine. (A. Oettinger, Ed.) *9*(1), 36-45.

Winred, & Serfatty Godoy, M. (16 de 09 de 2024, p. 1). *La dantesca misión de Google para darle a la IA un cuerpo robótico.* Obtenido de https://es.wired.com/articulos/la-dantesca-mision-de-google-para-dar-a-ia-un-cuerpo-robotico

Winston, P. H. (1992, p. 12). *Inteligencia Artificial* (Vol. Tercera edición). Pearson. Obtenido de https://courses.csail.mit.edu/6.034f/ai3/rest.pdf