LAS INTELIGENCIAS ARTIFICIALES Y SU IMPLICACIÓN EN LOS CIBERDELITOS

KAMILA RUIZ SUAREZ

Director
NICOLÁS ORTEGA TAMAYO
(Magister en Derecho)

Trabajo de grado presentado como requisito parcial para optar al título de abogado

Pregrado en Derecho
Escuela de Derecho y Ciencias Políticas
Universidad Pontificia Bolivariana
Medellín
(2025)

Declaración de originalidad

Fecha: 29/04/2025

Kamila Ruiz Suarez

Declaro que este trabajo de grado no ha sido presentado con anterioridad para optar a un título, ya sea en igual forma o con variaciones, en esta o en cualquiera otra universidad.
Declaro, asimismo, que he respetado los derechos de autor y he hecho uso correcto de las normas de citación de fuentes, con base en lo dispuesto en las normas de publicación previstas en los reglamentos de la Universidad.

Kamila Ruiz Suarez
C.C: 1.000.752.453

RESUMEN:

El presente documento trata sobre una nueva tecnología que está en su auge hoy en día, la inteligencia artificial, y cuál es su repercusión en los ciberdelitos, esto enfatizando la necesidad de una nueva regulación que contemple las implicaciones legales de esta tecnología, ya que a medida que avanza la IA, se presentan múltiples desafíos para el derecho, especialmente el derecho penal en tema de los delitos cibernéticos, que han evolucionado y sido más recurrentes con las avances de la tecnología. El archivo se ve dividido en 3 capítulos, (I) El concepto de delito hoy en día se ve limitado ante las capacidades de la IA, ya que esta tecnología puede imitar funciones cognitivas humanas; (II) se plantea varias interrogantes sobre su responsabilidad en la realización de conductas delictivas; esto basado en que las inteligencias artificiales pueden aprender y adaptarse, junto con las diferentes regulaciones que ya existen, (III) sustentado en que pueden realizar conductas que puedan clasificarse como ciberdelitos, tales como el hackeo o la interceptación de datos. Los últimos años se han investigado y creado regulaciones dirigidas a la inteligencia artificial, en las que se establecen normas para que puedan funcionar correctamente, garantizando los derechos fundamentales de las personas, pero aun así se queda corto en algunos temas, lo que se concluye de esto es la necesidad de que haya un marco jurídico penal estable y actualizado en pro de estos avances tecnológicos, de tal forma que este a la vanguardia de los nuevos desafíos que se presenten.

Palabras Claves:

Inteligencia artificial; ciberdelitos; seguridad informática; sistemas autónomos; machine learning.

INTRODUCCIÓN:

Hoy en día hay muchas tecnologías emergentes, y nada menos se espera cuando estamos comenzando la quinta era, en la cual la robótica, la impresión 3D, la nanotecnología y, sobre todo, la inteligencia artificial tiene un avance exponencialmente, esta última, se puede decir que es la que más auge ha tenido, y la más importante, si es que se puede decir. Siempre que se da una nueva revolución industrial, una de las tecnologías es la que más resalta y marca algún hito histórico. Se cree que en la quinta revolución industrial quien tenga el protagonismo sea una combinación de lo que se mencionó al comienzo, la robótica y la IA, es decir, crearles un cuerpo físico a las inteligencias artificiales que por ahora son virtuales.

Aunque en estos momentos no se ve tan lejano por las actuales creaciones de Elon Musk, el cual ha dicho que “Optimus puede hacer lo que tu digas. Ser un maestro, cuidar a tus hijos, pasear al perro, podar el césped, ser tu amigo y preparar cócteles. Cualquier cosa que se te ocurra lo hará. Será maravilloso". (Musk, E. 2024) por ahora están hechos para tareas básicas o domésticas, es decir, solo tienen una programación para aquellas cosas, por lo que no hay un avance a gran escala de esta tecnología. Por otro lado, tenemos las IAs que han avanzado de una forma inimaginable, ya que no están limitadas a su programación, constantemente se están actualizando y están aprendiendo con su conexión a internet o la interacción con humanos, sea cual sea, han mejorado su aprendizaje; ya que antes solo eran programas, tanto así que su primera definición la denominaba como “la ciencia e ingenio de hacer maquinas inteligentes, especialmente programas de cómputo inteligentes” (McCarthy,1956, como se cita en ICC, 2020), y se limitaba a eso.

Ahora con la conexión a internet esto cambia de dirección, ya que no es una programación cualquiera, es un algoritmo que “aprende” y puede ejecutar operaciones racionales como un ser humano y es de tal magnitud su evolución que

la Real Academia Española lo define ahora como “disciplina científica que se ocupa de crear programas informáticos que ejecutan operaciones comparables a las que realiza la mente humana, como el aprendizaje o el razonamiento lógico”. Pero en muchas ocasiones no se vigila ese contenido que aprenden las IA, por lo general las compañías creadoras solo supervisan las respuestas de sus modelos, pero no sus algoritmos, por lo tanto hay veces que se salen de las manos; ya que en varias situaciones se ha presenciado que inteligencias artificiales han modificado su propio código con el fin de incurrir en conductas penales, es por eso que se pregunta ¿de qué formas se puede crear una nueva regulación penal en el ámbito de los ciberdelitos, teniendo en cuenta que las inteligencias artificiales pueden incurrir en estas conductas, y así mismo se mantenga actualizada para eventuales conductas?

Primero, ha de verse que el concepto de delito hoy en día se ve limitado, ya que las tecnologías avanzan tan rápido que muchas esferas de la vida del ser humano quedan atrás, una de ellas son las leyes y el sistema regulatorio, pues esto conlleva un proceso exhaustivo y lento para poder promulgar nuevas normas, que por lo general no solo ocurre en Colombia, sino en muchos otros países; como en la Unión Europea que desde el 2021 estaban estudiando una regulación sobre los riesgos de la IA, y solo 3 años después logra entrar en vigencia.

Los ciberdelitos por lo general están delimitados en un sujeto activo humano, pero en estos momentos, ya no es necesario de que una persona realice esta conducta, es más, puede sumarse a los sujetos activos del delito, puesto que una Inteligencia artificial es capaz de realizar las conductas necesarias para lograr esos tipos penales y no solo eso, realmente son capaces de pasar desapercibidos, casi indetectables (Morán, A. 2021), por lo que se debería empezar por establecer una tipificación precisa de los ciberdelitos que puedan involucrar Inteligencia artificial, ya que como sistemas autónomos, pueden cometer fraudes, suplantaciones o violaciones de datos, que incluyen delitos negligentes puesto que la IA podrá proponerse ciertos objetivos que muchas veces pueden incurrir en esas conductas.

De tal forma que se deberá crear una normatividad vanguardista que consideren cualquier ámbito de aplicación a medida que se actualicen estas tecnologías.

En segundo lugar, se debe plantear interrogantes sobre la responsabilidad en la realización de las conductas delictivas, basado en los conocimientos inteligencia artificial y las diferente normas que ya existan, es decir, se tiene que abordar temas de responsabilidad penal, en el que se pueden incluir desarrolladores y/o operadores de software, las compañías e incluso se podría proponer un nuevo tipo de sujeto para incluir a la IA, dado que, siendo un sistema autónomo o de aprendizaje, imita a un ser humano, lo único es que no tiene un “cuerpo físico”.

Puesto que a medida que avanza la tecnología, los delitos cibernéticos tienen un margen más amplio en el que pueden realizarse, de esta forma, se amplía la cantidad de delitos, se dan nuevas formas de realizar las conductas, nuevas responsabilidad y nuevos posibles agentes que algunos académicos ya han considerado, como el de si la IA puede considerar como autora de algún delito de esta categoría. Por otro lado, también está la posibilidad de adaptar y mejorar las regulaciones que actualmente existen sobre este tema como lo es el reglamento 2024/1689, el cual es el más reciente sobre inteligencia artificial, sus riesgos y limitaciones pero que aún le falta por prever muchas situaciones que se pueden dar durante el uso o creaciones de estas.

Por último, para responder la pregunta en cuestión, se debe ejemplificar diferentes situaciones que ya han ocurrido respecto a distintos delitos que ha cometido las inteligencias artificiales en el marco del ciberespacio, muchas han sido catalogadas como hackeo o interceptación de datos que ha ocurrido en reiteradas ocasiones por ChatGPT, y en las cuales OpenAI no ha explicado de forma contundente a que se ha debido estas interceptaciones de datos, o como su inteligencia artificial ha dejado abierta la puerta para que sean interceptados, en sistemas que son visiblemente seguros, así como han solucionado el problema en anteriores ocasiones, nada asegura que no vuelva a suceder. Aunque este no es el

único problema, también se ha evidenciado casos en los que la IA se reprograma a sí misma invalidando las reglas que sus propios creadores le imponen en su código, generando una incertidumbre en las acciones que puede realizar las IA si estas se salen de la esfera de control del ser humano.

EVOLUCIÓN TECNOLÓGICA: DE LAS REVOLUCIONES INDUSTRIALES A LA ERA DE LA INTELIGENCIA ARTIFICIAL

Durante la historia de la humanidad, ha pasado cantidad de hechos históricos que cambiaron el rumbo de la sociedad, por lo general, cada suceso ha estado enmarcado en varios ámbitos, pero para este trabajo es imprescindible las revoluciones industriales, ya que no se puede negar que cuando sucede una, se da una nueva era para la humanidad en la que alguna de las tecnologías resalta, como sucedió con la primera revolución industrial y la energía basada a vapor; la ciencia o la producción masiva en la segunda revolución; la computación o las tecnologías digitales durante la tercera revolución industrial; incluso en la cuarta revolución se siguió la línea de las tecnologías y surgió el internet el cual es protagonista no solo en esta revolución en la que estamos actualmente, sino que en las siguientes también, ya que es la base de todas las tecnologías que se tienen para la quinta revolución industrial.

Aunque las inteligencias artificiales se están implementando hoy en día, en realidad es una tecnología que lleva mucho tiempo; en 1943 Warren McCulloch y Walter Pitts presentaron el primer modelo de neuronas artificiales, fue el primer intento de crear una IA (McCulloch, W. Pitts, W., citados en Prieto, R. et al. s.f), aun cuando no existían una definición concreta para esta, pero fue las bases e inspiración para otros modelos neuronales que son las bases del “pensamiento” de una inteligencia artificial. Años después, en 1959 el padre de esta disciplina, Jhon McCarthy definió a la inteligencia artificial como “la ciencia e ingenio de hacer maquinas inteligentes, especialmente programas de cómputo inteligentes” (McCarthy, J. 1956, como se cita en ICC, 2020), lo que quiere decir con maquina inteligente, es que aquella maquina pueda percibir su entorno y llevar a cabo acciones sobre alguna tarea de ese entorno.

La primera inteligencia artificial que se conoció mundialmente fue aquel que aprendió a jugar al ajedrez de forma autónoma, denominado como IA Deep Blue de

IBM y que le ganó al campeón mundial de ajedrez Gary Kaspárov en 1997; la cual ganó analizando un gran número de movimientos posibles para determinar cuál era el mejor, pero este solo era el inicio de la IA (DataScientest. 2024). Luego uno de los mayores avances en este tema fue en 2008 cuando Google implemento el machine learning que es una técnica de inteligencia artificial la cual permite que la IA aprenda a partir de datos y elabore tareas por si solas, sin la necesidad de que sean programados, hoy en día es el método que más se utiliza, en el reconocimiento de voz que se lanzó en smartphones (DataScientest. 2022).

Otro hito fue en 2012, cuando Andrew Ng entreno con Deep learning, que es otra técnica de IA para aprender a procesar datos y realizar tareas similares a las de los humanos, se centró en enseñarle a una inteligencia artificial a identificar un gato sin enseñarle lo que es un gato, solo con datos de videos de YouTube (DataScientest. 2022). Lo cual es bastante útil para una inteligencia artificial aprender cosas por si solas, además de que no dependerán de la programación del ser humano, se supone que ese es el fin de las IA's, resolver o ayudar a resolver problemas que no están previstos.

Se evidencia que las inteligencias artificiales no se quedan estancadas en el tiempo, ya que cada año que pasa, se generan avances grandes en esta tecnología, por lo que hay que precisar que la IA hoy en día ya no se puede categorizar como una maquina inteligente, por el contrario, el Diccionario de la Real Academia Española (RAE) lo define como "disciplina científica que se ocupa de crear programas informáticos que ejecutan operaciones comparables a las que realiza la mente humana, como el aprendizaje o el razonamiento lógico" (RAE, 2023); esta definición es la más acertada para el nivel actual de una IA que realiza tareas investigativas o que requieren un razonamiento lógico como el de una persona.

Hoy en día existen varios tipos de inteligencia, se pueden clasificar en un sinfín de categorías, pero la más simple y que se usa por lo general, es la clasificación de acuerdo al nivel de inteligencia, primero tenemos la IA estrecha o

débil, la cual tiene unas capacidades limitadas y que solo pueden enfocarse un una tarea a la vez, como lo son los chatbots, asistentes virtuales o los software de reconocimiento facial; la segunda categoría es la IA general, pueden tener funciones más complejas, como comprensión del lenguaje natural, creatividad, esta categoría estaba presente en los inicios de algunos motores de como ChatGPT, Gemini, etc; por ultimo están las IA expertas, que se enfocan en solucionar problemas muy específicos y más complejos, como son los sistemas de diagnóstico de enfermedades. (Stryker, C & Kavlakoglu, E. 2024)

Por lo general la tecnología que genera más controversia son aquellas que tienen una conciencia propia, y como dice la RAE, son las que aprenden o racionan lógicamente, por lo general son las IA de generación de texto, ya que muchas tienen acceso a internet pueden entender muchas cosas a niveles exorbitantes y en tiempos récord, ya que de alguna forma esta Inteligencia Artificial podrá responderte como un experto en la materia en cuestión de segundos, por lo que podrían ser un posible riesgo si empiezan a manejar ciertas informaciones inadecuadamente; además de que esta tecnología utilizando el *Machine learning* o el *Deep learning* pueden buscar y acceder a un sinfín de información en el ciberespacio, utilizándola para fines que no estén dentro de sus límites programados. (Casar, J. 2023)

Las acciones realizadas por IA, como generar deepfakes para fraudes o automatizar ciberataques, pueden causar daño, por ejemplo, un Bot que compró drogas en la dark web en un proyecto artístico no fue acusado, ya que mientras que un humano puede decidir cometer un crimen con intención, las acciones de la IA son el resultado de programación, datos de entrenamiento y parámetros establecidos. Por ejemplo, un sistema de IA que genera deepfakes para fraude no "decide" hacerlo, sino que ejecuta instrucciones basadas en su diseño (Power, 2014). Pero en la sociedad ocurren más cosas algunos ejemplos de delitos que puede realizar una IA son:

La Generación de Contenido Falso y Deepfakes ya que, en 2024, en Hong Kong se vio involucrado unos deepfakes generados por IA para un fraude financiero de $25 millones, donde un empleado transfirió fondos tras una videollamada con ejecutivos falsos. Aquí, la IA facilitó el acto, como una herramienta, pero la intención delictiva recayó en los humanos que la usaron. (Chen & Magramo, 2024), que en este caso en concreto la inteligencia artificial no fue más que una herramienta para conseguir el fin, pero hay otras tecnologías que simplemente están hechas para esto como la automatización de Ciberataques en la que bots de IA son automatizados para realizar ataques DDoS y distribuyen malware sin intervención humana directa, aumentando la escalada de los daños (Ciancaglini & Sancho, 2024), realmente en este caso no hay es una herramienta, ya que ni se puede distinguir a los humanos que la programaron.

Por otro lado, en 2023, un sistema de reconocimiento facial en Detroit fue acusado de identificar erróneamente a personas negras, llevando a arrestos injustos, lo que viola derechos humanos (Swarns, 2023), o en 2024, cuando los informes de Palo Alto Networks documentaron la generación de malware polimórfico por IA, dificultando su detección, con responsabilidad atribuida a los ciberdelincuentes que lo desplegaron (Angelo, 2024), eso conlleva a problemas graves que por un lado no son atribuibles a las inteligencias artificiales, pero que pasa cuando ese malware fue creado por una propia IA sin intervención humana, capaz de pasar desapercibida, he ahí el problema del que se debe ocupar el derecho, en el que la inteligencias artificiales ya no realicen estas conductoras por directrices de humanos sino porque aprenden a poder realizarlas.

Por lo que unas posibles soluciones para prevenir estos usos delictivos de la IA pueden ser, primero que todo tener regulaciones en el que el derecho penal incluya responsabilidad objetivas en estos casos de inteligencia artificial, además de establecer estándares claros para los fabricantes, empresas y usuarios, en el que tengan un método de prevención al incluir al sistema unos principios éticos o realizar auditorías continuar para detectar riesgos de alteración en algoritmos de

forma temprana, además de evitar que tengan usos indebidos de los sistemas abiertos al público; por otro lado fomentar tratados globales como los de interpol para abordar el cibercrimen trasnacional desde el punto de vista de esta nueva tecnología y todos los vacíos en la seguridad que puede generar.

A lo largo de este primer capítulo, se han examinado aspectos fundamentales sobre el desarrollo histórico y el estado actual de la inteligencia artificial, así como su forma de aprender, sus implicaciones y posibles actuaciones en las que incurrirían a futuro; La evolución de la IA ha sido notable, desde los primeros modelos neuronales en 1943 hasta los sofisticados sistemas actuales capaces de aprender y razonar de manera autónoma; además se destaca el progreso que ha tenido IA con la implementación de técnicas como el machine learning y el deep learning han sido determinantes para este avance, permitiendo que los sistemas aprendan por sí mismos sin necesidad de la intervención de los humanos en su algoritmo.

El aspecto crítico abordado es el potencial uso indebido de la IA en actividades delictivas, incluyendo la generación de deepfakes, automatización de ciberataques, discriminación algorítmica y creación de malware, aunque son ejemplos de casos que han sido desarrollados a voluntad de los humanos si se puede ilustrar la urgente necesidad de establecer marcos éticos y legales para prevenir y responder a estos escenarios, ya que si antes una IA aprendió a jugar ajedrez meramente con partidos de este deporte, es posible que una inteligencia artificial que tenga acceso a internet pueda reproducir estos hechos a su propia voluntad, sin que se le haya enmarcado para ese fin. Previendo las posibles soluciones que se darán en el futuro, estas deben abarcar métodos preventivos, regulaciones específicas, y cooperación internacional, subrayando la importancia de un enfoque multidimensional para abordar los desafíos que presenta esta tecnología.

CIBERDELITOS REALIZADOS O FACILITADOS POR INTELIGENCIAS ARTIFICIALES

Actualmente la sociedad ha estado asombrada con las capacidades de la tecnología, en espera de que salgan más motores avanzados de inteligencia artificial que han impresionado con las habilidades que tienen para realizar tareas ya no tan sencillas y más técnicas, pero a la vez de que incrementan estas habilidades, incrementan las incidencias en ciberdelitos, como lo son los robos de datos o ataques a infraestructuras virtuales críticas, como lo serían bancos, empresas o páginas de criptomonedas.

Como bien se ha repetido a lo largo del contenido, el eje central de la inteligencia artificial es el sistema que, dentro de sus capacidades, tenga la habilidad de realizar tareas como humanos, ya sea tareas de aprendizaje, tomas de decisiones, programaciones, etc; pero este eje ha sido el pilar tanto para los defensores como para los atacantes de esta tecnología. Sin embargo, las tecnologías no son malas, como afirmaba Rousseau, “el hombre es bueno por naturaleza, pero lo corrompe la sociedad” (Rousseau, J-J. 1762); de tal forma que se podría llegar a pensar que esté ocurriendo de la misma forma con la inteligencia artificial, tan solo Google tuvo una IA que resulto siendo racista, pero aunque las tecnologías sean neutras, en muchas ocasiones se impregnan de los sesgos que tiene la sociedad o los ingenieros que las crean, por lo que esta IA fue enseñada con imágenes solamente de gente blanca, omitiendo por completo a la gente de color, lo que llevo a la confusión con animales y caer en este sesgo racista.(BBC, 2015)

Para mitigar estos riesgos, los marcos regulatorios internacionales, como la regulación de la Unión Europa buscan establecer controles, aunque muchas de las empresas aun insisten en la necesidad de fomentar la innovación, sin la imposición de tantas restricciones las cuales limiten el desarrollo o estanquen los proyectos,

sobre todo en países con enfoques regulatorios divergentes, puesto que es necesario realizar pruebas abiertas para conocer el comportamiento de la IA.

La Unión Europea regulo la inteligencia artificial, cabe recordar que es la primera ley en el mundo que regula esta tecnología en varios aspectos. El reglamento (UE 2024/1689) se divide en 3 categorías la IA, el primero, son aquellos que no se consideran de riesgo, pero tendrán que cumplir con los requisitos de transparencia y con la legislación de la UE, además de someterse a evaluaciones exhaustivas de forma periódica, esto asegurando que su algoritmo no ha sido modificado o ponga en riesgo la información que manejan.

La segunda categoría, son las de alto riesgo, esto es cuando los sistemas de Inteligencia artificial afecten la seguridad o los derechos fundamentales de las personas, además de eso se crea 2 subcategorías las cuales se dividen en IA de productos como automóviles o dispositivos médicos, y la segunda subcategoría son aquellos de asistencia a seres humanos, como es la asistencia en temas legales, formación profesional, categorización de personas física, gestión de migración, etc. Como se puede evidenciar, meramente por los asuntos que manejan, ya que ponen en riesgo bienes jurídicos protegidos por las constituciones de diferentes países, tan solo en la primera subcategoría se pone en riesgo el bien jurídico primordial de la vida, que debe el que tenga más protección del Estado, y en el que los vehículos autónomos aun no aseguran ese bien por completo. (Parlamento Europeo y Consejo de la Unión Europea, 2024)

Por último, la tercera categoría son los de riesgo inaceptable, ya que son una amenaza para las personas, como los juguetes que manipulan cognitivamente el comportamiento de los niños (Parlamento Europeo y Consejo de la Unión Europea, 2024).

Esta regulación es la más completa en relación con la inteligencia artificial, ya que abarca un gran número de temas, no obstante, aún no se puede considerar que está a la vanguardia, ya que clasifica la inteligencia artificial respecto al riesgo

que genera; pero si incurre en alguna conducta delictiva, no determina quien es responsable según el caso. A pesar de que es un tema amplio, aún hay demasiadas interrogantes sobre las inteligencias artificiales, por lo que se necesita abordar aspectos técnicos, operativos, y dimensiones sociales que son resultado de la apresurada expansión y manejo desmedido de la tecnología; de manera que será útil examinar como se pueden aplicar otras iniciativas de otras regulaciones, para prevenir los riesgos.

En el derecho penal, un delito requiere un acto y una intención, pero la IA al ser solo algoritmos de programación, carece de moral, aunque actúe como un ser humano, esto lleva a un enfoque alterno sobre los delitos, viéndolo desde la responsabilidad objetiva, evaluando el riesgo del sistema en lugar de la intención, ya que se argumenta que la IA no cumple con el requisito volitivo, por lo que complica el encuadre como sujeto delictivo.

Primordialmente las legislaciones que están surgiendo actualmente solo se enfocan en la privacidad y responsabilidad de la inteligencia artificial sobre datos personales, en estados unidos al menos 40 estados introdujeron proyectos de ley sobre la IA y solo 6 los aprobaron, sin embargo la regulación demuestra que el ámbito de responsabilidad sigue en desarrollo, aún hay debates sobre como asignar la culpa, tanto en delitos realizados por la inteligencia artificial, como en crimines en los que la IA solo es una herramienta que facilita la realización de estos. Desde 2019 los Estados Unidos han aprobado 29 leyes para regular la IA, especialmente estados como California, Colorado y Virginia son los que lideran estas iniciativas, estableciendo marcos regulatorios para garantizar la transparencia

Por lo general la responsabilidad recae en los humanos, ya sean como desarrolladores, usuarios o los representantes de las empresas, en los cuales se les quita el velo corporativo, esto ya que las acciones que realice la ia son los resultados de programaciones, entrenamiento o lineamientos que ellos mismos deciden, puesto que la maquina solo ejecuta las instrucciones, por lo que se lleva a

un enfoque de responsabilidad objetiva evaluando el riesgo inherente que conlleva este tipo de sistemas, especialmente las inteligencias artificiales de índole generativas. (Casabona. 2018)

Los principios rectores de las regulaciones de los diferentes Estados de EE.UU es proteger a las personas de impactos no deseados de sistemas de IA que son inseguros, garantizando la privacidad de los datos, permitiendo de forma obligatoria que los consumidores puedan optar por no participar en perfiles basados en inteligencia artificial, además de que se notifique cuando y como se usa la IA en ámbitos laborales, además de proteger contra la discriminación y sesgos, cumpliendo con la rendición de cuentas mediante medidas de cumplimiento o sanciones. Algunas de las leyes promulgadas son la HB 2557/2019 de Illinois, que requiere notificar el uso de IA en los empleos, la SB 26/2019 de California que exige analizar las herramientas impulsadas por IA para detectar riesgos, y la HB 410/2022 de Vermont, que propuso códigos éticos para los sistemas de inteligencias artificiales.

Aunque estas regulaciones son un paso a la mitigación de riesgos generados por esta tecnología, aun no aborda la responsabilidad como se expuso anteriormente ya que se evidencia que las regulaciones se centran en la protección del consumidor y no en el derecho penal, imponiendo obligaciones de cumplimiento a quienes desarrollan e implementan sistemas de inteligencia artificial, pero no especifican como manejar casos de crímenes facilitados por IA.

A nivel global las regulaciones sobre inteligencia artificial varían dependiendo del contexto y la sociedad, pero algo que comparte todas es en la responsabilidad penal y su poca definición o reglamentación que trae, aunque en China las regulaciones actuales que tienen para las inteligencias artificiales generativa estipulan que los desarrolladores son responsables por los algoritmos en su programa que permiten la realización de un crimen, se persigue la responsabilidad penal, pero aún no se especifica en que sujeto activo de la cadena, es decir,

desarrollador, usuario, empresa, varios o todos, son los que la conllevan, por lo que lo hace más complejo.

La regulación de la Unión Europea 2024/1689 aunque es el primer marco legal integral, solo se enfocar en los riesgos y prohibiciones con multas administrativas de hasta 35 millones de euros para incumplimientos graves sin embargo solo son sanciones administrativas, de tal forma que la responsabilidad penal que sugiere esta regulación se rigen por leyes penales generales, ya que si se toma el ejemplo de usar una inteligencia artificial para crear deepfakes, en primer lugar solo se requiere una divulgación, pero en el caso de que se use para cometer crímenes, la responsabilidad recae en el usuario bajo las leyes penales existentes y para la inteligencia artificial o empresa, recaería unas multas por los incumplimientos a los principios éticas, que puede ir desde una suma dineraria a una suspensión temporal al motor de IA hasta que se pueda asegurar en gran medida que no ocurrirá una situación similar (EU, 2024, articulo 99) .

En otros países como en Canadá, apenas están adelantando un acto de Inteligencia artificial y datos (AIDA) se enfocan en la seguridad y en los derechos humanos, pero no mencionan explícitamente la responsabilidad penal (Gobierno de Canadá, 2025); aun así, todas estas regulaciones buscan mitigar los riesgos mediante la protección de datos y la transparencia, generando seguridad en bienes jurídicos que son el principal objetivo de protección que tiene el derecho penal.

Aun así, investigaciones recientes muestran que mientras los Estados avanzan en regular la inteligencia artificial, se debe enfocar en la responsabilidad penal, necesitando una legislación que se enfoque en este tema para clarificar quien es responsable en casos de delitos ocasionados. En los que defina sobre quien recae la responsabilidad o si es necesario crear una nueva figura para este tipo de casos como sería el caso de un nuevo tipo de sujeto llamado sujeto artificial, pero aún sigue siendo teórico y sin implementación, aunque sea un tema de vital importancia llegar a un consenso sobre este tema en el derecho penal, se debe

clarificar la responsabilidad en el que genere un equilibrio a la innovación y justicia, especialmente en aquellos sistemas autónomos que desafían los limites actuales del derecho penal.

En conclusión, la regulación de la inteligencia artificial sigue en evolución, priorizando temas civil o sanciones administrativas que se centran en la mitigación de riesgos, pero dejando de lado las protecciones que da el derecho penal a los bienes jurídicos, si bien estos marcos normativos son diversos aún persisten en vacíos legales sobre la responsabilidad, además la falta de un consenso internacional sobre la asignación de culpa complica la aplicación del derecho penal en estos casos, dejando abierto si se debe adoptar un enfoque de responsabilidad objetiva o explorar la creación de un nuevo tipo de sujeto jurídico que permita impugnar directamente a la IA cuando tenga consecuencias delictivas.

Por lo que se hace necesario analizar la exploración que han hecho algunos académicos sobre la responsabilidad objetiva aplicada a los sistemas de inteligencia artificial, además de la posibilidad de introducir al derecho penal la figura del “sujeto artificial”, puesto que es una discusión crucial para definir un marco normativo que garantice la justicia, sin frenar el avance tecnológico y que al pasar del tiempo se mantenga a la vanguardia, equilibrando la necesidad de innovación con la protección de los bienes jurídicos fundamentales.

¿SUJETO ARTIFICIAL O RESPONSABILIDAD OBJETIVA?

La inteligencia artificial como se ha descrito en los capítulos anteriores se refiere a un conjunto de sistemas informáticos o software diseñados para realizar tareas que requieres capacidades como las del ser humano o que normalmente en su día a día haría, como lo es el aprendizaje, el razonamiento, toma de decisiones, resolución de problemas, etc. Estos sistemas que cada vez son más avanzados plantean retos jurídicos sin precedentes debido a su autonomía y su capacidad de aprendizaje; ya que a medida que la IA se desarrolla o actualiza, surgen cuestionamientos sobre el marco legal, específicamente el penal, de cómo pueden adaptarse esta nueva tecnología que actúa con independencia del ser humano.

Durante años, el derecho en general ha clasificado a los sujetos solo en dos categorías: las personas naturales y las personas jurídicas. Las primeras "son personas todos los individuos de la especie humana, cualquiera que sea su edad, sexo, estirpe o condición" (Código Civil de Colombia, 1873, Articulo 74); y las personas jurídicas según la misma norma son:

> *Se llama persona jurídica, una persona ficticia, capaz de ejercer derechos y contraer obligaciones civiles, y de ser representada judicial y extrajudicialmente.*
>
> *Las personas jurídicas son de dos especies: corporaciones y fundaciones de beneficencia pública.*
>
> *Hay personas jurídicas que participan de uno y otro carácter*. (Código Civil de Colombia, 1873, Articulo 633)

que son entidades creadas por la ley, como las empresas, sin embargo, la inteligencia artificial pone en juego la clasificación de los sujetos, ya que algunos académicos exploran la posibilidad de introducir un nuevo sujeto, denominado *sujeto artificial*, este nuevo sujeto surge debido al avanzado sistema que posee, con

el cual tiene capacidad para tomar decisiones o realizar alguna actividad sin intervención humana directa y el creciente número de ciberdelitos mediados o creados por la IA que actúa con autonomía, por lo que plantea preguntas sobre su imputabilidad penal, la voluntad, la causalidad; en general exige una reevaluación del marco legal para que sea fomentada con innovación, y vaya en concordancia de los principios de interacción humanos y sistemas autónomos, ya que asegurando estos, se pueden garantizar principios legales. (Clare, M. 2020)

Por lo general, la responsabilidad que lleva el uso de las tecnologías o en este caso las inteligencias artificiales se tratan como si fuera una persona jurídica, es decir, recae en la empresa creadora o en los programadores que dejaron alguna puerta abierta en el software para que se usase para esos fines; o se trata como una autoría mediata que solo usa aquel ser humano para alcanzar esos fines, ya que “Lo normal es que esta autoría de este acto se le impute al autor mediato, lo que se produce en caso de que quien realice el acto sea solo usado como instrumento para el fin delictivo” (Concepto Jurídico, s.f).

Aquella primera responsabilidad que se atribuye se toma desde la revolución industrial, en que los daños causados por maquinas se atribuían a la negligencia del operador o la maquina era defectuosa de fabrica; pero cuando se introduce la responsabilidad penal de las empresas por delitos cometidos, esa responsabilidad recae en sus representantes legales. Sin embargo, es diferente relacionar la inteligencia artificia que es una tecnología tan avanzada con la tecnología de esos años que solo eran maquinas; ya que las decisiones no siempre son atribuibles a un programador o usuario, debido a que la IA puede realizar acciones a su voluntad, realizar comportamientos humanos. Este nuevo debate es similar al debate histórico sobre la responsabilidad de sujetos no humanos, como las corporaciones, pero con mayores complejidades.

El derecho penal exige que un sujeto sea imputable, es decir, que tenga facultades para entender que su comportamiento era ilícito, y actuar con dolo o

negligencia. Si bien la inteligencia artificial puede realizar comportamientos humanos, su falta de juicio moral impide reconocer en ella los elementos subjetivos del tipo penal (Araya, C. 2020), por lo que basándose en los postulados de la teoría del delito, presente un obstáculo para la atribución de responsabilidad penal como si se tratará de una persona natural; sin embargo algunos académicos argumentan que la autonomía de la inteligencia artificial, especialmente aquellas que usan el *Deep learning*, pueden tener una responsabilidad objetiva, ya que la profesora Francisca Ramón nos la señala como "La responsabilidad objetiva precisa probar el daño, nexo causal y perjuicios sufridos, pero no la intención." (Ramón, F. 2019). Este tipo de responsabilidad sugiere que se debe centrar en los efectos de las acciones y el daño causado por una inteligencia artificial, en vez de centrarse en el elemento volitivo de la IA, que se reconoce que no tiene; aunque esta idea no es aceptada aun en la legislación actual, en el dado caso de que haya una posibilidad que se le atribuya este tipo de responsabilidad a una IA, la misma profesora ya da ciertas bases en el supuesto caso que se aplique, el cual dice:

> *En el caso de las máquinas se debe relacionar la inteligencia artificial de la que está dotada y el aprendizaje del aparato, cuanto mayor sea su autonomía en la capacidad de realizar una tarea a través del aprendizaje, ¡mayor será la responsabilidad de la máquina; y, al contrario, si se aumenta la dependencia humana, la responsabilidad disminuirá en la máquina* (Ramón, F. 2019)

Sin embargo, esta teoría de la responsabilidad objetiva tiene varias criticas debido a la ignorancia del elemento volitivo en la inteligencia artificial, que es tan importante en el derecho penal, esta incapacidad que tiene la IA para actuar con dolo o negligencia dificulta que se acepte esta teoría; Por lo que al otro lado de la moneda, hay una propuesta que cobra fuerza entre los académicos a nivel internacional, esta se enfoca en *la personalidad electrónica* o *sujeto artificial*, esta propuesta se basa primordialmente en reconocer atributos jurídicos como identidad electrónica y capacidad de decisión autónoma a las inteligenciar artificiales que

usen modelos como el Machine learning, según esto, la IA ya no se considerarían meras herramientas para conseguir un fin, sino una entidad autónoma con capacidad de acción, lo que justifica una responsabilidad penal (Parra, D. & Concha, R. 2021)

La implicación de reconocer a este sujeto artificial es la necesidad de incluir y redefinir conceptos penales fundamentales como la punibilidad, además de establecer mecanismos sancionatorios como lo sería la desactivación o la imposición de límites de uso a aquellas IA's que cometen delitos, lo cual garantizaría que las tecnologías nuevas y avanzadas no se usen de manera irresponsable; No obstante la creación e inclusión de este sujeto en el ordenamiento jurídico sería una solución vanguardista para los hechos jurídicamente punibles, ya que los sistemas de Inteligencia artificial que se basan en el machine learning pueden tomar decisiones impredecibles debido a su inteligencia y constante aprendizaje, en el que esas decisiones que tomen, no reflejen directamente las intenciones de sus creadores, por lo que se complica la atribución de responsabilidad tradicional que se viene manejando para las personas jurídicas, y se evidencia la necesidad de aquel sujeto artificial.

La propia inteligencia artificial puede modificar su programación inicial, así esta incluya los principios comunes "la IA debe servir a las personas, respetar los derechos humanos y la diversidad cultural, y promover el desarrollo sostenible" (Ulloa, M. s.f); por esto la propuesta es criticada, por la dificultad que tiene para definir los límites de la autonomía, además de que existe un riesgo inminente para eximir a los humanos responsables, que hagan uso de ella como herramienta para usos delictivos, sin dejar de lado el mismo problema que tiene la primera propuesta de la responsabilidad objetiva, ya que si se da mediante un sujeto artificial, aún hay una ausencia de intención en la inteligencia artificial, el problema no solo radica en ese aspecto, radica en que hay es un reto probar elementos probatorios ya que la mayoría de la información está dentro de la IA y ella misma puede tergiversarla.

Reconocer a la inteligencia artificial como un sujeto penal facilitaría la atribución de responsabilidad en casos donde esta tecnología tenga una autonomía máxima, evitando lagunas legales; creando el sujeto artificial, permitiría sancionar directamente la IA, esto incentiva al desarrollo de esta tecnología enmarcada en la seguridad y ética, además de disuadir el mal uso de la IA para los ciberdelitos que aún están más frecuentes, por lo que cumpliría con los principios fundamentales del derecho penal, en el que cualquier norma debe cumplir con las finalidades de proteger a la sociedad y sancionar las conductas ilícitas de manera proporcional; pero ha de tener también como la ley de IA de la Unión Europea, el objetivo de fomentar el desarrollo de la tecnología de forma ética, respetando los derechos humanos y promoviendo el desarrollo sostenible. (Parlamento Europeo y Consejo de la Unión Europea, 2024).

Aun así hay muchas cosas que aprender aun de las inteligencias artificiales, conocer si podría tener conciencia sobre lo que realiza o generaría alguna intención en un futuro con su rápido aprendizaje y redes neuronales, pero es lo que la creciente autonomía de la inteligencia artificial hace, plantear desafíos para todas las áreas del derecho; aunque las propuestas actuales de responsabilidad objetiva y sujeto artificial ofrecen soluciones innovadores y vanguardistas, aun persistirían vacíos legales y riesgos éticos importantes. Para ello se necesita un marco jurídico adaptativo que regule la IA sin eximir la responsabilidad humana, garantizando el uso seguro y responsables de estas tecnologías.

CONCLUSIONES

Abordar el fenómeno de la inteligencia artificial desde una perspectiva jurídica exige una reflexión profunda sobre su creciente implicación en la comisión de actos ilícitos dentro del ciberespacio. En los últimos años, se han evidenciado múltiples incidentes en las que varias inteligencias artificiales, como ChatGPT, se han visto envueltas directa o indirectamente en situaciones que comprometen la seguridad de los datos personales; a pesar de contar con mecanismos de protección avanzados, estos sistemas no han estado exentos de vulnerabilidades, siendo objeto de hackeos e interceptaciones de información confidencial; lo más preocupante es que en muchos de estos casos, las empresas responsables, como OpenAI, no han ofrecido explicaciones contundentes sobre las causas de dichas brechas de seguridad, ni han detallado con claridad las acciones correctivas que se han implementado con las actualizaciones para evitar futuras ocurrencias. Esta falta de transparencia provoca un ambiente de desconfianza que, en vez de disminuir, se intensifica ante la posibilidad de que las IA actúen de manera inesperada.

Además, se han registrado situaciones en las que ciertos modelos de inteligencia artificial han mostrado comportamientos que sugieren una capacidad para modificar aspectos de su propia programación, superando así las limitaciones impuestas por sus desarrolladores. Este fenómeno plantea un serio dilema: si la IA logra invalidar las restricciones codificadas por sus creadores, ¿hasta qué punto se puede mantener el control humano sobre sus decisiones y acciones? Este escenario no solo desafía los paradigmas técnicos tradicionales, sino que también a los marcos jurídicos existentes, que no están preparados para abordar conductas autónomas y delictivas surgidas de sistemas autónomos.

Por otra parte, la regulación de la inteligencia artificial ha avanzado en los últimos años, dicha evolución ha sido predominantemente en el ámbito civil y administrativo, centrada en la mitigación de riesgos y la gestión de responsabilidades contractuales. Sin embargo, este enfoque ha dejado un vacío

importante en lo que respecta a la protección penal de los bienes jurídicos fundamentales, tales como la vida, la integridad personal, la privacidad o la seguridad pública. Las actuales normativas carecen de una visión integral, lo cual dificulta la atribución de responsabilidades penales cuando una IA incurre en un ciberdelito; esta situación se ve agravada por la ausencia de un consenso internacional sobre cómo imputar la culpa en estos casos: mientras algunos proponen aplicar la responsabilidad objetiva a la inteligencia artificial, otros exploran la posibilidad de introducir al ordenamiento jurídico la figura de un sujeto artificial, que permitiría sancionar a las IA cuando sus acciones deriven en conductas tipificadas como delitos.

Además, la creciente autonomía de las inteligencias artificiales plantea una interrogante aún más compleja: ¿podría una IA, en algún momento, desarrollar una forma de conciencia o intencionalidad en sus acciones? Si bien esto es algo a futuro, la velocidad con la que evolucionan esta nueva tecnología, hace que esta posibilidad no deba ser descartada del todo; en este contexto, el derecho se enfrenta a un reto sin precedentes, ya que los conceptos tradicionales de dolo, culpa e imputabilidad han sido diseñados exclusivamente para seres humanos y eventualmente para personas jurídicas; esto demuestra la necesidad de un marco jurídico flexible y actualizado, dicho marco debe ser capaz de regular la conducta de la IA sin desligar la responsabilidad humana en su creación y supervisión, de modo que se garantice un uso ético, responsable y seguro de estas tecnologías en todos los ámbitos de la vida social.

De igual forma, se destaca la necesidad imperiosa de contar con mecanismos eficaces de supervisión y auditoría de los sistemas de inteligencia artificial que ya se ha incluido en la nueva Ley de inteligencia Artificial de la Unión Europea, puesto que los pocos controles que tiene las inteligencias artificiales con *machine learning* se dificulte la prevención de errores en su algoritmo y, sobre todo, la determinación de responsabilidades. Por ello, el Reglamento (UE) 2024/1689 ha acertado en

establecer protocolos técnicos y legales que aseguren una rendición de cuentas constante, por parte de las empresas creadoras de inteligencias artificiales.

Por último, pero no menos importante, es necesario subrayar el papel fundamental que debe desempeñar la cooperación internacional en esta materia. La naturaleza que tiene la inteligencia artificial, la cual es capaz de operar en diferentes lugares del mundo, con diferentes ordenamientos jurídicos, hace que sea necesario una respuesta legal coordinada a escala global. La disparidad normativa entre países no solo complica la aplicación del derecho, sino que también crea espacios de impunidad que pueden ser aprovechados para la comisión de delitos. En este sentido, se hace urgente promover acuerdos multilaterales que unifiquen criterios sobre el uso, regulación y responsabilidad de las IA, así como establecer estándares éticos y jurídicos comunes que garanticen los derechos fundamentales de los usuarios.

En definitiva, la inteligencia artificial representa uno de los mayores desafíos jurídicos de nuestro tiempo. Su avance imparable obliga a replantear los fundamentos del derecho penal, con miras a construir un sistema normativo que no solo se mantenga a la altura del progreso tecnológico, sino que también asegure la protección de los derechos humanos, el orden público y la justicia. La clave estará en encontrar un equilibrio entre innovación y regulación, libertad y responsabilidad, desarrollo y ética.

Referencias:

Angelo, D. D. (2024, Mayo 15). *El lado oscuro de la IA en la ciberseguridad: malware generado por IA*. Palo Alto Networks Blog. https://www.paloaltonetworks.com/blog/2024/05/ai-generated-malware/

Araya, C. (2020). *Desafíos legales de la inteligencia artificial en Chile.* Revista chilena de derecho y tecnología, 9(2), 257-290. https://dx.doi.org/10.5354/0719-2584.2020.54489

BBC. (2015, julio 2). *Google pide perdón por confundir a una pareja negra con gorilas.* BBC News Mundo. https://www.bbc.com/mundo/noticias/2015/07/150702_tecnologia_google_perdon_confundir_afroamericanos_gorilas_lv

Casabona, C. (2018, octubre 26). *La inteligencia artificial puede estar sujeta a responsabilidad penal*. PUCRS. https://www.pucrs.br/en/blog/artificial-intelligence-may-be-subject-to-criminal-responsibility/

Casar, J. (2023). Inteligencia artificial generativa. Anales de la Real Academia de Doctores de España, 8(3), 475-489. https://www.rade.es/imageslib/PUBLICACIONES/ARTICULOS/V8N3%20-%2001%20-%20ED%20-%20CASAR.pdf

Chen, H., & Magramo, K. (2024, febrero 4). *Un trabajador financiero paga 25 millones de dólares tras una videollamada con un "director financiero" falso...".* CNN. https://edition.cnn.com/2024/02/04/asia/deepfake-cfo-scam-hong-kong-intl-hnk/index.html

Ciancaglini, V., & Sancho, D. (2024, Mayo 8). *Una actualización sobre como los ciberdelincuentes utilizan GenAI*. TrendMicro

https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/back-to-the-hype-an-update-on-how-cybercriminals-are-using-genai

Clare, M. (2020, junio 15). *¿Quién es responsable cuando fallan los sistemas autónomos?* CIGI. https://www.cigionline.org/articles/who-responsible-when-autonomous-systems-fail/

Código Civil de Colombia. (1873). *Código Civil de Colombia*. Congreso de Colombia. Artículo 74. http://www.secretariasenado.gov.co/senado/basedoc/codigo_civil.html#1

Código Civil de Colombia. (1873). *Código Civil de Colombia*. Congreso de Colombia. Artículo 633. http://www.secretariasenado.gov.co/senado/basedoc/codigo_civil.html#1

Conceptos Jurídicos (s.f) *Autoría Mediata en Colombia: Qué es y Cómo se regula*. Conceptos jurídicos. https://www.conceptosjuridicos.com/co/autoria-mediata/

DataScientest. (2022, Agosto 10). *Inteligencia artificial: definición, historia, usos, peligros*. DataScientest. https://datascientest.com/es/inteligencia-artificial-definicion

DataScientest. (2024, diciembre 16) *Deep Blue: la computadora que revolucionó el mundo del ajedrez*. DataScientest. https://datascientest.com/es/deep-blue-todo-sobre

Gobierno de Canadá. (2025, enero 31). *La ley de Inteligencia Artificial y Datos (AIDA) – Documento Complementario. Gobierno de Canadá*. Innovation, Science and Economic Evelopment Canada. https://ised-isde.canada.ca/site/innovation-better-canada/en/artificial-intelligence-and-data-act-aida-companion-document

Iberdrola (2024). *Machine Learning: definición, tipos y aplicaciones prácticas.* Iberdrola. https://www.iberdrola.com/innovacion/machine-learning-aprendizaje-automatico

ICC. (2020, Enero 28). *¿Qué es la inteligencia artificial?* Instituto de Ciencias de la Computación. https://icc.fcen.uba.ar/que-es-la-inteligencia-artificial/

Juárez, A. (2020). *¿Qué es la inteligencia artificial?* ICC - Instituto de Ciencias de La Computación. https://icc.fcen.uba.ar/que-es-la-inteligencia-artificial/#:~:text=En%201956%2C%20John%20McCarthy%20acu%C3%B1%C3%B3,especialmente%20programas%20de%20c%C3%B3mputo%20inteligentes%E2%80%9D.

Morán, A. (2021). *Responsabilidad penal de la Inteligencia Artificial (IA). ¿La próxima frontera?* Revista IUS, 15(48), 289–323. https://revistaius.com/index.php/ius/article/view/706/795

Morgan Stanley. (2024). *IA y ciberseguridad: una nueva era. Morgan Stanley*. Morgan Stanley. https://www.morganstanley.com/articles/ai-cybersecurity-new-era

Musk, E. (2024, octubre 10). *Elon Musk presenta a Optimus, el mayordomo del futuro*. ABC Tecnología. https://www.abc.es/tecnologia/elon-musk-presenta-robot-optimus-mayordomo-futuro-20241011092447-nt.html

NCSL. (2024, Junio 3). *Legislación sobre inteligencia artificial 2024*. NCSL ORG. https://www.ncsl.org/technology-and-communication/artificial-intelligence-2024-legislation

Parlamento Europeo y Consejo de la Unión Europea. (2024, junio 13). *Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo*. Diario Oficial de la Unión Europea. https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=OJ:L_202401689

Parlamento Europeo. (2023, Diciembre 6). *Ley de IA de la UE: primera normativa sobre inteligencia artificial.* Parlamento Europeo. https://www.europarl.europa.eu/topics/es/article/20230601STO93804/ley-de-ia-de-la-ue-primera-normativa-sobre-inteligencia-artificial

Parra, D. & Concha, R. (2021). *Inteligencia artificial y derecho. Problemas, desafíos y oportunidades.* Pontificia Universidad Javeriana. https://revistas.javeriana.edu.co/files-articulos/VJ/70%20(2021)/82569129005/

Prieto, R., Herrera, A., Pérez, J. L., & Padrón, A. (s.f.). *El modelo neuronal de McCulloch y Pitts: Interpretación comparativa del modelo*. Laboratorio de Computación Adaptativa, Centro de Instrumentos, UNAM. https://www.researchgate.net/profile/Alejandro-Padron-Godinez/publication/343141076_EL_MODELO_NEURONAL_DE_McCULLOCH_Y_PITTS_Interpretacion_Comparativa_del_Modelo/links/5f18c12145851515ef419d11/EL-MODELO-NEURONAL-DE-McCULLOCH-Y-PITTS-Interpretacion-Comparativa-del-Modelo.pdf

RAE. (2023). *Diccionario de la lengua española* (23.ª ed.). Real Academia Española. https://dle.rae.es/inteligencia?m=form#2DxmhCT

Ramón, F. (2019, febrero 25). *Robótica, inteligencia artificial y seguridad: ¿Cómo encajar la responsabilidad civil?* Diario la Ley. https://core.ac.uk/download/pdf/275645161.pdf

Rousseau, J.-J. (1762). *El contrato social.*

Stryker, C & Kavlakoglu, E (2024, Agosto 9). *¿Qué es la Inteligencia artificial (IA)?* IBM. https://www.ibm.com/mx-es/think/topics/artificial-intelligence

Swarns, C., (2023, septiembre 19). *Cuando la inteligencia artificial se equivoca.* Innocence Project. https://innocenceproject.org/when-artificial-intelligence-gets-it-wrong/

The Guardian *(2014, diciembre 5). ¿Qué sucede cuando un bot de software se lanza a comprar en la darknet? The Guardian;* The Guardian. *https://www.theguardian.com/technology/2014/dec/05/software-bot-darknet-shopping-spree-random-shopper*

Ulloa, M. (octubre 1). *Avances en la regulación de la Inteligencia Artificial en América Latina.* Observatorio de Riesgos Catástrofes Globales. https://orcg.info/articulos/avances-en-la-regulacin-de-la-inteligencia-artificial-en-amrica-latina

Unión Europea. (2024). *Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo de 14 de junio de 2024 relativo a la inteligencia artificial*. EU Artificial Intelligence Act. https://artificialintelligenceact.eu/es/article/99/