Problemas jurídicos ocasionados por los errores en la inteligencia artificial

Brahian Arroyave Hincapié

Tomás Rozo Acevedo

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

ASESOR: José Alberto Toro Valencia

ESCUELA DE DERECHO

UNIVERSIDAD EAFIT

MEDELLÍN

JUNIO TRECE DE DOS MIL VEINTICINCO

Tabla de contenido

Resumen

Esta investigación tiene como objetivo principal analizar las complicaciones generadas por las inteligencias artificiales en el campo del derecho privado, así como cuales son los errores más comunes en el campo de la implementación y creación de estos sistemas. Se explorará distintos tipos de desarrollo, el sistema de aprendizaje de estas herramientas, trasfondo histórico, derecho comparado y dar soluciones de cara a la legislación colombiana que permita llenar los agujeros normativos existentes.

Palabras clave: *Deep learning*, derecho comparado, *design error*, inteligencia artificial, responsabilidad civil,

Abstract

The main objective of this research is to analyze the complications generated by artificial intelligence in the field of private law, as well as what are the most common mistakes in the field of implementation and creation of these systems. It will explore different types of development, the learning system of these tools, historical background, comparative law and provide solutions to Colombian legislation to fill existing normative gaps.

Key words: Artificial intelligence, civil liability, comparative law, deep Learning, design error,

Glosario

Aplicación o Programa: programa informático diseñado como una herramienta para realizar operaciones o resolver funciones específicas.

Back End: parte del desarrollo web que se encarga de que toda la lógica de una página web funcione correctamente. Es decir; es la parte en donde está comprendido todo lo relacionado con el algoritmo y el lenguaje de programación.

Bug: son los errores dentro de la programación. Estos podrían estar asociados con un mal funcionamiento, cierre abrupto del programa o sencillamente interferencias visuales que no deberían de presentarse

Ciber acoso o *Cyber Bullying*: arista de la Ciber violencia, se basa en el uso de medios digitales para molestar o acosar a una persona mediante ataques personales, divulgación de información personal, sea real o no, entre otros medios.

Ciber violencia: es el acoso, amenazas, intimidación o cualquier método de violencia personal ejercida a través de imágenes o datos digitales que pueda tener mensajes sexuales, agresivos, hostigadores en cualquier forma del entorno digital.

Deep Fake: son imágenes o videos editados a través de las herramientas de inteligencia artificial en donde se superponen rostros de personas reales o inexistentes en cuerpos de personas diferentes al del rostro

Deep Learning: arista del *machine learning*, el cual utiliza redes neuronales para simular la toma de decisiones del cerebro humano en las inteligencias artificiales.

Errores de programación: Errores en el código fuente creados por incumplimiento en el diseño lógico en el programa. Dichos errores se pueden generar por expresiones incompletas o erróneas; variables no declaradas; palabras mal escritas, Bugs, entre otras

Front End: parte de las páginas webs o de las aplicaciones con la cual los usuarios ven e interactúan. Esta sección comprende temas como el diseño, la interfaz del usuario, elementos visuales, colores entre otros.

Inteligencia artificial: red neuronal artificial mediante la cual los ordenadores pueden ejecutar actividades y tomar decisiones de manera independiente al operador humano.

Machine learning: tipo de aprendizaje para las inteligencias artificiales, mediante el análisis de datos previamente ingresados.

Programador o desarrollador: profesional que se encarga de diseñar y crear software mediante el uso de lenguajes de programación.

Spam: mensajes no solicitados o deseados

Testers: personas encargadas encontrar problemas de programación que se generen en la aplicación previo a su lanzamiento al mercado.

Introducción

A lo largo de la historia, la humanidad siempre se ha encontrado en una perpetua cadena de desarrollo de ideas en aras de materializarlas en el entorno productivo. Esta estructura se inicia desde la filosofía y se concreta en todas las áreas del saber humano. De allí que se identifiquen distintas eras, tales como la época clásica, el medioevo, renacimiento, la ilustración y la modernidad y así dar paso a la revolución industrial e innovaciones en la automatización del trabajo y del pensamiento.

Así pues, las revoluciones industriales se destacan por tratarse de cambios de paradigma en cuanto nuestra interacción con el mundo. La primera revolución industrial introdujo la maquinaria de vapor y la mecanización de los procesos productivos, transformando las sociedades rurales en urbanas e industriales. Posteriormente, la segunda revolución industrial trajo consigo la electricidad, además de la producción en masa y el desarrollo de las telecomunicaciones, aspectos que intensificaron la urbanización y reformaron profundamente la organización empresarial.

Ya a partir de la tercera revolución industrial, el enfoque paso de la mecanización a la digitalización, esto gracias a la invención y desarrollo de los sistemas computacionales, la digitalización y el surgimiento del internet,

transformando de forma radical la comunicación a escala global. Finalmente, en la época actual, nos encontramos en lo que se ha categorizado como la cuarta revolución industrial la cual, a diferencia de la tercera, se encuentra en la convergencia entre la realidad física y digital mediante el acaparamiento y análisis de datos, siendo esto representado en tres aspectos: el Big Data, el Internet de las Cosas (IoT) y a la Inteligencia Artificial (IA).

El IoT se refiere a la interconexión de objetos físicos al internet, creando ambientes digitales con interacciones en el mundo físico, tales como el uso de relojes inteligentes o vehículos de movimiento automático. Esta tecnología ha permitido el aumento exponencial de la automatización de procesos.El Big Data se refiere a la estructuración de información y del conocimiento para poder reconocer una serie de patrones y predecir conductas para tomar decisiones acertadas en tiempo real.

Finalmente, la IA emerge como uno de los desarrollos más disruptivos. Los sistemas de IA tienen la capacidad de aprender, razonar, identificar patrones, tomar decisiones y ejecutar acciones de forma autónoma, replicando funciones propias de la inteligencia humana, casi como si se tratase de la creación de una nueva vida inteligente. Desde asistentes virtuales hasta diagnósticos médicos, pasando por sistemas de recomendación o plataformas de justicia predictiva, la IA se ha insertado en numerosas dimensiones de la vida contemporánea.

Sin embargo, toda innovación acarrea múltiples discusiones respecto al impacto, no solo positivo, sino negativo que tendrá en la sociedad, cómo lo es en el marco de la seguridad digital, la privacidad y uso de datos sensibles, la desigualdad de datos e información, los sesgos que podrían llegar a generarse mediante el uso de estas nuevas tecnologías y la responsabilidad frente a los posibles fallos y errores de funcionamiento que genere esta tecnología.

En la actualidad, nos encontramos en un alza de desarrollo y creación de aplicaciones computacionales con inteligencia artificial, desde los teléfonos celulares hasta aplicaciones web o centros de asistencia inteligente usan y aprovechan estas herramientas para hacer simplificar la vida cotidiana. Sin embargo, esta creación masiva de programas avanza rápidamente dificultando el estudio de los problemas y daños colaterales que podrían causar. Hace apenas una década, se inició el estudio e implementación de políticas y normas que buscan llenar los vacíos normativos que dejan estas herramientas. Sin embargo, estas políticas y normas no suelen ajustarse en todos los casos o directamente no tienen contingencias para frenar los daños y problemas ocasionados por estos aplicativos.

> La normatividad colombiana no ha podido actualizarse dentro de la problemática contemporánea que el boom de las inteligencias artificiales (II. AA) ha creado, existiendo así un vacío legal que es necesario ser resuelto; la responsabilidad extracontractual, las problemáticas éticas y jurídicas dilemas que generan los errores de malfuncionamiento relativo al uso de las

inteligencias artificiales, esta situación no es sorprendente, ya que el derecho es una problemática social que se ajusta a las necesidades de cada sociedad, por lo tanto, es una respuesta al comportamiento que tenga cada población.

Sin embargo, en la actualidad, algunos Estados y organizaciones han abordado ciertos proyectos regulatorios sobre el tema, por ejemplo, la Unión Europea, EE. UU., Canadá y China ya han iniciado con la creación de sistemas normativos que permiten subsanar los daños causados por las IA. Siendo la normativa más extensa y sólida la europea, la cual se utiliza como referencia en este texto.

Empero, la normatividad a veces se queda corta para poder definir y trazar soluciones para estos problemas, siendo necesario fijar un marco ético que permita subsanar los vacíos legales o que permita fijar las reglas para la creación de los sistemas legales. A través del estudio del trasfondo ético y principialista que existe sobre la IA.

En este contexto, surge la pregunta de investigación: ¿cómo se logra determinar los problemas jurídicos en los errores o fallos causados por las Inteligencias Artificiales en Colombia? Es relevante determinar dichas problemáticas, especialmente en los países que carecen de un marco normativo robusto sobre la IA; tales como Colombia, cuya falta de regulación en el tema obliga a los operadores jurídicos a recurrir al derecho comparado, analogías o inclusive

forzar interpretaciones de un Código Civil de 1887, el cual no tiene aplicaciones fácticas referente a las II. AA

El objetivo general de este trabajo es el de analizar los problemas jurídicos y los errores de diseño en las IA por medio de un estudio sobre la doctrina y normatividad tanto nacional como extranjera, con el fin de encontrar una solución a las contingencias originadas en estas situaciones. Para lo anterior, es menester tener en cuenta los siguientes pasos

El primero es el de identificar aquellas situaciones comunes en las que se suele presentar coyunturas jurídicas causadas por las II. AA mediante la estructuración de un marco de errores realizado por estas.

El segundo paso consta de la definición de un perfil de impacto ético de los dilemas jurídicos causados por el mal funcionamiento y/o errores que pueda presentar la IA en su aplicación

El tercer paso sería identificar los esquemas normativos para la regulación de la IA, realizando un especial énfasis en los marcos éticos de estos IA

Finalmente, y teniendo en consideración lo expuesto, se deberá de proponer un panorama de posibles soluciones a la disyuntiva planteada basado en la implementación de principios éticos de la IA.

Así pues, la metodología a realizar para el presente trabajo será basada en el rastreo normativo y doctrinal de la Inteligencia Artificial tanto a nivel local como internacional.

De igual manera, el trabajo se presentará mediante una estructura capitular divida en cuatro partes. El primer capítulo servirá como un contexto general limitado a la historia de la IA y sus aplicaciones en la sociedad, siendo una de estas en el ámbito jurídico mediante el uso de los “sistemas jurídicos expertos”. De igual manera, se abordará el componente de programación de las II. AA; de su creación, lenguaje y finiquitará con los tipos de aprendizaje de las II. AA. El segundo capítulo retomará el enfoque programático al centrarse en las fallas y errores en los que se puede incurrir al diseñar aplicaciones; para ello se destacan dos errores comunes, siendo estos los errores de sintaxis, diseño y mala praxis; cada uno de estos con su respectivo análisis de cómo se provoca y de las consecuencias que llegase a generar.

El tercer capítulo, toma un eje diferente, ya que se enfoca en el trasfondo ético y principialista de las inteligencias artificiales; sugiriendo esquemas de creación de marcos éticos generales, creados principalmente por la doctrina y la filosofía, mediante la implementación de siete principios de aspecto universal. Finalmente, en el cuarto capítulo se retoma la esquematización de las II. AA mediante la aplicación de marcos éticos para el desarrollo de diversos modelos de

regulación, realizados tanto por países como por bloques regionales, siendo estos representados por dos bloques: la regulación general y la regulación atómica.

Finalmente, se identifican ciertas problemáticas actuales respecto al uso de II. AA en el derecho y cómo, bajo este amplio margen normativo, es preferible no enfocarse en la regulación normativa como tal sino en el establecimiento de principios reglamentarios concentrados en un marco ético sólido y delimitante.

Capítulo I. Inteligencia artificial: Historia, creación y aprendizaje

Historia de la Inteligencia Artificial

Para poder hablar mejor sobre este tema es menester primero responder a la pregunta: ¿qué se entiende como inteligencia artificial? Múltiples doctrinantes han realizado definiciones de estas, un ejemplo de estas fue la dada por Marvin Misk, referenciado en el artículo de John Tassiolas *"First stop towards an ethics of robots and artificial intelligence*" (2019, p. 52) quien la define como "*La ciencia de hacer que las maquinas hagan cosas que requerían inteligencia si fuesen hechas por humanos"* (Rozo, 2025, p. 52, traducción propia)[1]". Por otro lado, Goretty Carolina Martínez Baena en su artículo *La Inteligencia artificial y su aplicación al campo del derecho*, la define como "*Una rama de la informática que trata de realizar con máquinas, tareas que puede realizar el ser humano aplicando cualquier tipo de razonamiento*" (2012, p. 828). Así pues, teniendo estas definiciones en consideración, es plausible considerar a la inteligencia artificial como aquella habilidad que tienen los ordenadores para realizar algún tipo de actividad que requiera, en alguna medida, interferencia humana de forma autónoma sin necesitar de agentes externos, esta actividad requiere de la toma de decisión, la cual debe

[1] Frase original del texto: "*the science of making machines do things that would require intelligence if done by men', such as face recognition or language translation*"

ser ejecutada de forma completamente independiente, sin necesidad alguna de un operador. Para poder realizar este procedimiento se requiere del uso de los lenguajes de programación, para habilitar algoritmos y códigos que puedan cumplir con la tarea deseada (Rouhiainen, L., 2018) La primera mención sobre la IA fue en 1943, en el artículo *"A Logical calculus of ideas immanent in nervous activity",* escrito por Warren McCollugh y Walter Pitts, presentando en este trabajo el primer modelo matemático que fuese capaz de crear una red neuronal artificial.

Sin embargo, la primera aplicación y desarrollo en cuestión se presentó en 1956 con el artículo "Máquina de teoría lógica" escrito por Allen Newell y Herbert A. Simon, quienes desarrollaron un ordenador que fuese capaz de realizar y resolver teoremas matemáticos. Así pues, la IA se convierte en una herramienta que no se limita únicamente en la automatización de procesos, sino que se extiende a la ejecución de tareas, análisis y procesamiento de datos, lo cual permite su implementación en actividades de uso cotidiano y con ello transformado de manera exponencial la productividad y el trabajo de las personas.

Existe una gran variedad de inteligencias artificiales, cada una diseñada para un propósito distinto. Estas pueden clasificarse acorde al tipo de aprendizaje que tienen, como lo es el caso de las inteligencias que usan el aprendizaje automático, las cuales recolectan datos por medio de una red neuronal que las instruye para generar y dar respuestas a sus usuarios (Rouhiainen, L., 2018). Otra clasificación

de aprendizaje se basa en aquellas que requieren del ingreso de datos o preparación por parte de los desarrolladores, esto tiene el nombre de *Machine Learning*. También se pueden diferenciar o reconocer por sus funciones y o aplicaciones, como lo es el caso de los Sistemas Expertos Jurídicos, que son herramientas creadas para facilitar el trabajo de los abogados, despachos judiciales, jueces y peritos. La primera ocasión rastreable de la implementación de sistemas Expertos jurídicos data del año 1981, siendo una incursión realizada en Inglaterra, usando como base las preposiciones lógicas del tipo “sí… No… Entonces... Sí y sólo sí…”. (Martínez, 2012).

Sistemas jurídicos expertos

En el apartado anterior, se esbozó de forma breve algunos antepasados importantes de la inteligencia artificial dentro de la órbita del derecho y a pesar de la novedad que suponen las IA en el mapa de la actualidad, existen bastantes ejemplos antiguos de estas herramientas.

Los expertos jurídicos o también llamados, sistemas jurídicos basados en conocimiento (Martínez, 2012) son el primer nombre dado a este utensilio, son IA enfocadas para resolver o ayudar en casos y controversias jurídicas; algunas veces para la toma de decisiones por medio de la información previamente insertada dentro de las bases de datos del Experto, claramente la idea de todo tipo de IA es

la de emular de alguna forma imitar ciertas acciones dentro del comportamiento humano, en este caso, los Expertos tienen como principal objetivo tratar de mitigar algunas labores poco relevantes que tienen los despachos de esta manera facilitando el trabajo dentro de juzgados o despachos, es muy común que exista una gran acumulación de procesos para los jueces y estas herramientas ayudan a dar un rápido tramite a algunos de estos problemas. Ciertamente no se puede permitir que estos asistentes puedan conocer de todos los temas dentro de una legislación, o al menos no sin supervisión de un abogado o dependiente judicial, pero la idea de asociar a los Expertos jurídicos con el derecho penal, siendo este una rama del derecho de suma importancia, sin ningún tipo de supervisión es poco probable en los años siguientes, al igual que en casos que puedan impactar de forma relevante la vida de alguna de las partes.

Los sistemas expertos jurídicos tienen a su vez a estar clasificados en modos, los cuales dependerán de la estructura en su construcción y método de aprendizaje.

Estas clasificaciones se pueden resumir en dos tipos de modos: modelos de procesamiento simbólico y modelo conexionista (redes neuronales**).** El primer modo hace mención del aprendizaje a partir de la inferencia, análisis y estudio de símbolos previamente insertados y traducidos por parte del programador. El segundo modelo, tratan de solucionar problemas no algorítmicos en experiencias almacenada dentro de su conocimiento, este tipo necesita de un entrenamiento y es el tipo de

racionamiento más cercano al cerebro humano (Martínez, 2012) Algunos de los ejemplos más notables de este tipo de tecnología son:

Lex Machina: esta es una herramienta de análisis de casos y litigios. Generalmente buscan un patrón de acciones o identificar tendencias que puedan ayudar a los juristas dentro del caso.

COMPAS (Correctional Offender Management Profiling for Alternative Sanctions): es una aplicación que funciona como soporte para las sentencias en EE. UU., los jueces la usan para comprobar el porcentaje de reincidencia de una persona basada en algunos factores tales como el estatus socioeconómico, raza, edad, sexo, entre otras variables. Este programa no es perfecto y de algún modo viola el principio de la transparencia al incluir sesgos dentro del comportamiento de esta herramienta (Mattu, 2023). Sin embargo, podría existir otra razón por la efectiva predilección del COMPAS al momento de aumentar la probabilidad de reincidencia de los afrodescendientes y es que, en efecto exista una gran cantidad de afrodescendientes que terminen en las rejas múltiples veces una vez hayan cometido un delito, es complejo determinar hasta qué punto, es algo estrictamente objetivo por parte de la aplicación, o si realmente existe algún tipo de grado de falta de parcialidad dentro de la configuración del Sistema Experto.

PretorIA: este sistema ayuda a analizar y categorizar las tutelas reduciendo los tiempos para estas labores. Generalmente, una persona al día puede leer unos 30 de estos procesos, este sistema puede hacerlo en tan sólo 2 minutos (Corte Constitucional, 2020)

Prometea: al igual que PretorIA, Prometea analiza tutelas, pero esta vez no para categorizar, sino para ayudar al juez a tomar una decisión, es decir. esta herramienta estudia las circunstancias y puede darle al juez un panorama del caso, pero en sí misma no decide en ningún momento por el juez.

Fiscal Watson: sistema de inteligencia artificial basado en tecnología de IBM, adquirido por la Fiscalía General de la Nación Colombiana como parte de un plan para mejorar la eficiencia en la investigación penal. Dicho sistema utiliza la analítica de datos, procesamiento de lenguaje natural (NLP) y aprendizaje automático, con la finalidad de asociar casos registrados en el sistema penal acusatorio (SPA), analizando grandes volúmenes de información estructurada y no estructurada para identificar patrones y relaciones entre casos, principalmente en la etapa de indagación. (Palacios et al, 2024)

De la creación y el lenguaje

Todo tipo de programas computacionales o aplicaciones tanto de ordenadores como de teléfonos móviles están construidos de formas similares a

través de los lenguajes propios de la programación. A su vez, existe una cantidad considerable de lenguajes[2] y utilidades diversas para estos mismos. La estructura dentro de estos se divide en dos tipos: *Front End* y *Back End*; El *Front End* se encargará de la primera interacción de la aplicación con el usuario final, es decir, el cliente, la interfaz de usuario y todo lo relacionado con la utilización y gestión de la aplicación. El *Back End*, por otro lado, se refiere al trasfondo de lo creado por los desarrolladores, es decir; la implementación de los lenguajes de programación a través de algoritmos y fórmulas para el correcto funcionamiento de la aplicación o del programa computacional. (Ibarra et al, 2021). La estructura clave de cada algoritmo y aplicación será entonces los códigos que, dependiendo del lenguaje utilizado, cambiaran completamente o podrían ser similares.

Para la construcción de una aplicación, es necesario fijar estándares y parámetros a partir de la lógica, seguimiento de reglas y la solución de problemas matemáticos a través de los algoritmos usados según el lenguaje de programación que se desee usar, esto se realiza siguiendo determinadas secuencias lógicas, siendo necesario entonces una carga pre establecida de datos para la formulación y contestación de los problemas que se planteen dentro de la aplicación, por lo cual, si se pretende realizar, por ejemplo, una página web; será necesario incluir dentro del algoritmo todas las posibilidades previstas que pudiesen ocurrir al momento de

[2]No se abordará este tema porque no es competente de este estudio.

correr la aplicación, paso a paso, desde el título, hasta la finalización de algún bucle o dotar de características propias a un botón.

Los lenguajes de programación tienen como función desarrollar un paradigma el cual fijará las reglas de juego por las cuales se regirá la solución del problema concreto, creando una estructura que recoja todas las bases establecidas y permita la formulación de problemas coherentes y su solución. Dicho de otro modo, los lenguajes de programación son un instructivo de ordenes secuenciales como si se tratase de una especie de receta de cocina: Si quiero hacer una taza de café, necesito una taza, verter el agua en la taza, luego verter el café en la taza, revolverlo y así obtendré como resultado una taza de café (Si A, B y C entonces D).

Tipos de aprendizaje

Para poder configurar de forma óptima una Inteligencia Artificial es necesario realizar un entrenamiento a la misma y dotarla de toda la capacidad para responder o satisfacer las necesidades de sus usuarios, para hacer esto, es necesario otorgarle métodos de aprendizaje a la aplicación, que sean consecuentes para su correcto funcionamiento. Existen dos métodos de aprendizaje, el *Machine Learning* y el *Deep Learning* y dependerá del propósito de la aplicación para tomar la decisión al momento de la creación de la IA para la asignación de este aprendizaje. Es posible que estos tipos de aprendizaje tengan subcategorías y también apéndices

que permitan realizar una mayor ramificación del tema, pero sólo se tocarán los temas que puedan ser competentes para esta investigación. Es necesario recordarle al lector, que en este inciso sólo se mencionará y se explicarán de forma bastante breve los distintos tipos de aprendizaje que se estudiarán a lo largo de la presente investigación y sólo se centrará en el tema de investigación pertinente.

- ***Machine learning***

Su principal característica es el aprendizaje automático a partir de patrones dentro de datos, mejorando su desempeño y eficiencia cuantos más datos puedan analizar. Para que se pueda dotar de este aprendizaje, hay algunas técnicas que diferencian la forma de la obtención y análisis de datos dentro de la IA. (Bobadilla, 2020). Existe una gran cantidad de aplicaciones que se usan a diario que están realizadas con este tipo de aprendizaje, desde la función de reconocimiento de la cara para poder desbloquear un móvil (o detección del rostro), pasando por extensiones para los navegadores que impiden la aparición de Spam, bloqueadores de publicidad, hasta comprensión de textos. No obstante, lo relevante de este tipo de aprendizaje es la Big Data y sus implicaciones, tanto en el campo de la mercadotecnia o del consumo en general.

La Big Data, por decirlo de un modo simple; corresponde a un gran pozo de información, generalmente, se entiende como una combinación de “las tres V”: Volumen, Velocidad y Variedad (Wall, 2014).

Volumen: es la enorme cantidad de datos, puede tratarse de cualquier tipo de datos, desde búsquedas en sitios webs, frecuencia en la búsqueda de algún *item* en la red, hasta responder historias en alguna red social, el tiempo que se está dentro de un sitio web.

Velocidad: es el ritmo en el que se entregan los datos.

Variedad: diversidad de la información y rastro de las búsquedas. Lo cual genera datos que son administrados por los titulares del sitio correspondiente. Existen, datos estructurados que serían los correspondientes a las búsquedas, pero también existen datos semi estructurados o no estructurados que corresponden a audios, videos o textos.

- **Aprendizaje supervisado**

En este apéndice del *Machine Learning* se usarán etiquetas, las cuales estarán cargadas de datos, por ejemplo, si se planea realizar una IA que realice reconocimiento de imágenes, se deberá de crear etiquetas que permitan la clasificación del objeto o imagen en cuestión (img0001.bmp, “libro”), (img0002.bmp, “cuaderno”), dotando al código de información se permitirá un entrenamiento que

permita a la aplicación realizar la distinción y categorización de las distintas imágenes usando la base de datos preestablecida que se cargó. (Bobadilla, 2020)

- **Aprendizaje no supervisado**

Para el aprendizaje supervisado, era necesario realizar la creación de etiquetas que permitieran la diferenciación y categorización de los ítems, en el aprendizaje no supervisado, no es necesaria la realización de las etiquetas, pero sigue siendo necesaria la carga de datos. Para el análisis de estos datos, se realizarán agrupamientos de los datos en una práctica conocida como *clustering* la cual pretende realizar grupos a través de los datos, siendo la misma aplicación la que realice las colocaciones pertinentes con base en los comportamientos o parámetros deseados. (Bobadilla, 2020)

- ***Deep learning***

Este tipo de aprendizaje tiene como principal característica la automatización a partir de un modelo neuronal de entrenamiento, esto se hace a través de la creación de decenas o hasta cientos de “neuronas” creadas a través de etiquetas o pesos dentro de la estructura de la aplicación, dotando a la inteligencia artificial de la capacidad de aprender por sí misma y de su interacción con los usuarios. (Bobadilla, 2020). Es decir, este tipo de aprendizaje es parcialmente automático, necesita de algún tipo de desarrollador que pueda revisar y analizar el progreso del aprendizaje

a través de los datos que le arrojan a la aplicación, esto se logra entrando en un programa de entrenamiento para la aplicación en donde se le da retroalimentación constante a su escalado de aprendizaje, así como una inyección de datos y propósitos para que pueda desempeñarse de la forma adecuada. Una vez esté entrenada la aplicación y se encuentre disponible para el público, serán los usuarios quienes decidan si el resultado arrojado por la aplicación es correcto o no, es por esto por lo que este tipo de aplicaciones se sustentan y mejoran únicamente a través de la retroalimentación de sus usuarios. Este tipo de aprendizaje tiene infinidad de funciones y aplicaciones, sin embargo, si existe un patrón de uso para este aprendizaje y estos son los más populares: Programas de traducción de textos o de imágenes, detección de fraude, los asistentes virtuales, como Siri, Cortana, Google assistant.

Síntesis

A pesar de que pueda sonar novedoso el tema de la Inteligencia artificial, es bastante claro el enorme trasfondo que existe sobre este asunto y que no es algo precisamente nuevo, ni siquiera la idea de las aplicaciones en el campo jurídico de estas herramientas, las II. AA han dado pequeños pasos para abrirse paso dentro de la sociedad en sus diferentes esferas, permeando casi todas las disciplinas del conocimiento, siendo algo cada vez más común y necesario en el diario de las personas, sin embargo, es claro que a pesar del enorme desarrollo que están

teniendo estas herramientas, cada vez se dibuja una gran división y limitación en lo que puede y no puede hacer una IA. Lo interesante de este asunto, es que a pesar de que siempre estuvo presente en el colectivo de las personas o de la academia, sólo trazaron algunas respuestas bastante someras para problemáticas realmente complejas como lo son las relativas a las causaciones de problemas o repercusiones negativas para las personas, pero este tema será analizado en capítulos posteriores.

Hay al menos, tres puntos importantes presentes en este capítulo que son importantes de resaltar; el primero y el principal es la definición y la forma de entender una IA, el segundo es lo relativo a la creación y el lenguaje, por último, los tipos de aprendizaje. Estos tres temas son pilares para el reconocimiento de las inteligencias artificiales, al igual que su distinción, esto ayudará a tener un mejor panorama sobre esta problemática.

Capitulo II. Errores en la programación y creación

Inteligencia artificial y errores de programación

La IA es, en su esencia, un tipo programa computacional o aplicación, como si se tratase de una relación Genero-Especie, siendo el género el programa computacional y la especie la IA. Así pues, la IA es creada a partir de bases bastante similares a las que una aplicación, como lo son los lenguajes propios de programación y realización de algoritmos. Sin embargo, la diferencia sustancial entre ambas radica en la toma de decisiones, ya que una IA puede tomar decisiones de forma autónoma, tal como sucede en el sistema de auto pilotaje de algún tipo de aeronave, mientras que, en las aplicaciones computacionales, se desarrollan mediante la codificación secuencial y lógica con la búsqueda de algún resultado concreto, pero sin el componente autónomo que tiene la IA, por ejemplo; una aplicación para comprar online. Es necesario realizar esta distinción, porque sí bien, es cierto que existe una diferencia tajante en ambos escenarios, ambos comparten las bases creativas, pero no funcionales.

Las aplicaciones, desarrolladas gracias al trabajo de los programadores, ofrecen herramientas capaces de ejecutar múltiples tareas para reducir la carga laboral o mejorar la vida de las personas. Sin embargo, en ocasiones pueden

presentar errores que dificultan, restringen o incluso dañan sus propias funciones u otros factores externos. Estos fallos pueden afectar desde componentes físicos del ordenador hasta aplicaciones bancarias en distintos dispositivos. La mayoría de estas afectaciones provienen de errores, los cuales se diferenciarán por la forma en la que se encuentra realizado el error, si se trata de una dificultad técnica o de escritura, si es por una mala planeación o si, por ejemplo, es un error realizado adrede para la inoperancia de algún tipo de aplicación.

Por ello la gravedad del error se encuentra sujeta a su naturaleza y el impacto que tendría en la aplicación y en el usuario. Así pues, habrán errores que no afectaran en gran medida al usuario, tales como frente agendas virtuales encargadas de organizar datos poco relevantes, mientras que otros errores, acorde a la aplicación en que se presenten, si podrán afectar de manera directa y gravosa al usuario, tales como aquellos generados dentro de aplicaciones bancarias (que pueden resultar en pérdidas económicas) o inclusive errores dentro de sistemas de defensa nacional, tales como la detección o direccionamiento de misiles (que pueden resultar no solo en pérdidas económicas, sino de vidas humanas).

Errores comunes en la programación de aplicaciones o programas computacionales

La programación y creación de aplicaciones, al tratarse de operaciones matemáticas o de complejas secuencias de codificaciones que pasan de mano en mano dentro de las empresas desarrolladoras, suelen presentar errores de funcionamiento una vez sean finalizadas las aplicaciones. Existe una gran cantidad de errores, pero entre los más comunes se encuentran los errores de sintaxis y los errores de diseño (o también llamados errores lógicos) y cada uno teniendo consecuencias distintas. (Dollard, 2023). Para el presente trabajo solo nos centraremos en los errores mencionados.

Errores de sintaxis

Los errores de sintaxis ocurren principalmente por las disonancias dentro de la estructura del código diseñada por los desarrolladores, tal como sucede en los errores de indentación; los cuales se presentan por no ubicar de forma correcta el algoritmo dentro del código (Fonden, 2018). Dichos errores suelen originarse por el movimiento constante de personal, ya sea por su reasignación a otros proyectos o por la participación simultánea en varias iniciativas, dejando a los lideres con menos personal o con nuevos desarrolladores, los cuales carecen de continuidad en el proceso, facilitando la aparición de errores involuntarios.

Los errores de sintaxis se pueden calificar en dos secciones, siendo el primero los errores de sintaxis inhabilitante y el segundo los errores de sintaxis puros. El primero error no permite la correcta ejecución de la secuencia deseada, por ejemplo, un error de escritura al momento de querer realizar o llamar una función que no permita la compilación del código. El segundo tipo se refiere a errores ocurridos en el *Back End*, esto al tratarse de fallos en los algoritmos o lenguaje de programación al momento de la edición o planteamiento de la aplicación de cara al usuario. Estos errores suelen ser inofensivos, sin embargo; es posible que puedan tener un resultado perjudicial para el usuario, empero, esto significaría un descuido enorme por parte del desarrollador. En un apartado posterior se ejemplificará como herramienta pedagógica un error puro de sintaxis que pueda tener resultados devastadores para el usuario o a la empresa desarrolladora.

Teniendo en cuenta la naturaleza del error de sintaxis, es complejo que este llegase a inhabilitar o alterar el comportamiento o resultado de una aplicación, por lo que es común que el resultado de estos errores sea la inoperatividad de la aplicación de forma completa, es decir, que el error evite que la aplicación puede ejecutarse o pueda compilar información de forma correcta. Sin embargo, en aquellos casos excepcionales, podría suceder que la aplicación tuviera un punto de partida en el cual todo el código esté dado de forma correcta, pero otra parte del código tenga error de indentación, esto provocará que el código que esté sin errores

se ejecute, omitiendo el resto del código y modificando de tal manera el comportamiento de la aplicación al ejecutarse de forma parcial.

Un caso frecuente sería eliminar alguna función, alterarla o que tenga algún error de sintaxis puro en una función que ponga fin a un bucle de la aplicación, de forma tal que al continue solicitándole al usuario datos o se le requiera que ejecute la misma opción múltiples veces sin que la aplicación pueda reconocer la ruptura del bucle. También es posible que la aplicación tenga algún error de sintaxis puro en la programación de su *Front End*, por ejemplo, que no se hayan identificado de forma correcta las variables que pueda reconocer un botón de la aplicación, esto imposibilitaría el correcto funcionamiento de la aplicación, pero está claro que los errores más comunes son los errores en el *Back End.*

Los errores de sintaxis puros son se identifican al tener como base la mala escritura por parte del desarrollador en los elementos del código de la aplicación, un ejemplo de este error sería el siguiente:

Un desarrollador pretende habilitar la opción de un buzón de PQRSD (quejas y reclamos) para el uso en su empresa, pero al momento de elaborar el botón en la pestaña de aplicación, comete un error y en vez de integrar el código que redirija al buzón, inserta un código de otra función de la aplicación, la cual para el presente ejemplo será la opción de comprar un producto. Así pues, cuando el usuario fuese a dirigir un PQRSD, en vez de entrar en el buzón, entraría en la opción de compra.

Aunque ambas opciones estén bien ejecutadas dentro de la aplicación y puedan compilar, el usuario final siempre que trate de entrar a la aplicación para realizar un PQRSD, en vez de ser redirigido al buzón, el botón lo llevará a la opción de compra de un producto. En sí mismo este error requiere de un descuido mayor por parte del desarrollador y del equipo de *testers*, por lo que es poco probable que en la práctica pueda tener resultados perjudiciales para sus usuarios. De igual manera, los errores de escritura, palabras escritas de forma incorrecta o un error ortográfico también comprende este apartado de errores.

A pesar de lo común que puede ser este error, al mismo tiempo es sumamente complicado que no sea detectado a tiempo previo a su lanzamiento al público, ya que las organizaciones poseen departamentos encargados para el análisis y manipulación de la información compilada en las aplicaciones, por lo que en caso de presentarse dicho descuido en el lanzamiento público de la aplicación, es factible asumir que la empresa se encuentra sujeta al régimen de responsabilidad bajo la modalidad de “culpa grave” acorde al artículo 63 de nuestro código civil.

Siguiendo con lo anterior, el reconocimiento e identificación de los errores de sintaxis es posible realizarlo mediante el uso de las herramientas propias para el desarrollo, por ejemplo, el *Visual Studio Code*, el cual es un programa computacional, es de uso frecuente para la creación de códigos y programas computacionales. Este programa otorga la capacidad al usuario de poder montar sus avances y ejecutarlos en tiempo real los errores o pudiendo comprarlos al

momento de compilar la aplicación, permitiendo realizar un análisis bastante simple para encontrar estos errores, pero cuando se tratan de códigos de gran extensión, se complejiza la identificación de dichos errores

Por otro lado del asunto, volviendo a la naturaleza de los errores de sintaxis, estos pueden interpretarse desde una perspectiva de género y especie, siendo los errores de sintaxis como un género, y teniendo múltiples especies dentro del apartado de errores de programación, dando lugar a los errores de ejecución, errores de enlazado, errores lógicos o hasta el apartado de errores de diseño, aunque estos últimos tienen sus características tan propias que van a tener su propio apartado.

- **Errores de ejecución**: previamente se habló de la posibilidad de que un fichero pueda compilar de forma óptima su variable o que la aplicación en sí misma tenga su punto de partida común y corriente, pero que al momento de que los *testers* o el usuario final pueda interactuar con la aplicación, se llegué a la conclusión de que al momento de realizar una acción dentro del programa esta sea infructuosa o que sencillamente no ocurra absolutamente nada. Esto corresponde a un error de ejecución dentro de la secuencia o algoritmo que plantee el desarrollador. Un ejemplo de esto sería en el diseño de una página web, podría habilitarse y estar de cara al usuario, dentro del apartado de la herramienta para programar no se encuentre error alguno y que al momento de que el usuario quiera iniciar sesión dentro de la página

no pueda lograrlo porque se saltó algún paso dentro de la creación de la aplicación. Estos errores, en sí mismos, son extremadamente extraños como resultado final, ya que implica un descuido desmedido por parte de los *testers* y de los desarrolladores. (Educación IT, 2020)

- **Errores de *enlazado***: para poder programar, es necesario el uso de bibliotecas, de la creación de “objetos”, definir variables, crear ficheros, en general; es necesario realizar la nomenclatura de datos para la creación de la aplicación, partiendo del supuesto que un desarrollador olvide realizar esta nomenclatura o la haga de forma equivocada, podría tener problemas para la correcta ejecución dentro de la aplicación, olvidó incluir alguna biblioteca o fichero y esto imposibilita el correcto desarrollo de la aplicación. Estos errores no llegan al usuario final y se pueden terminar en etapas tempranas del proceso. (Gonzales, 2018)

- **Errores lógicos**: estos errores en sí mismos son sumamente fáciles de reconocer e identificar, ya que provienen de un mal diseño o planeación de los algoritmos, no se profundizará demasiado en este apartado ya que el objetivo de esta investigación no es adentrarse en el terreno de la arquitectura de software, sencillamente para contextualizar se resumirá en qué; son errores que pueden ser sumamente variados así como sus

> consecuencias, pero que son sumamente fáciles de rastrear y de solucionar, tienen consecuencias como la inoperatividad de la aplicación o el bloqueo de la misma. (Icy Science, 2023)

En la práctica, para poder ajustar el nivel de del daño y su proporcionalidad se deberá de analizar desde la perspectiva de la responsabilidad civil extracontractual, aunque generalmente se puede encontrar una ventana de términos y condiciones para las aplicaciones en donde tratan de menguar la responsabilidad de las corporaciones y sus implicaciones legales. Si se parte del supuesto de que la aplicación no tuviera ningún tipo de términos y condiciones o clausulas habilitantes para el uso, se necesitaría que esta generara un daño sobre una cosa, algún tipo de derecho o una persona y que este sea imputable a una o varias personas.

En un caso hipotético en el que una aplicación bancaria generara un bucle sin fin debido a que no fue finalizado dentro del código de programación, esto daría pie a un error masivo, tanto para la entidad que generó la aplicación, como para sus usuarios, siendo los únicos responsables de esto la propia entidad y su grupo de desarrolladores. También es posible que se presenten errores al momento de la identificación de las variables, lo que al momento de realizar el desembolso de dinero no pueda llegar al lugar que la entidad desea sino, otro completamente distinto.

Consecuencias de los errores de sintaxis

Tal y como se ha explicado en todo el desarrollo de esta investigación, es complejo encontrar este tipo de errores para el usuario final, es posible encontrarlos cuando las etapas de la programación estaban apenas comenzando o se tenía muy poca visión sobre las responsabilidades posteriores a la finalización del proyecto. Algunos de los errores más impactantes desde una perspectiva económica, son:

Mariner I: para iniciar este apartado, es necesario hablar del Mariner 1 un cohete Atlas lanzado en 1962 por la NASA en su primera misión para poder sobrevolar Venus (NASA, S/F). Este cohete no era dirigido por algún controlador, sólo se necesitó de un programa de software que pudiera guiarlo hasta su destino, el problema sucedió minutos después del despegue, en donde se presentaron dos fallos cruciales en su sistema de navegación; el primero tuvo un pequeño fallo de transmisión de su señal al programa interno que permitía la corrección del rumbo, el segundo tuvo como fuente un error de programación en donde se omitió una sección del código, en dónde, por olvidar incluir un guion dentro del código dentro de las instrucciones del programa no se podía corregir el rumbo y entraba en conflicto con la recepción de las señales de radio. Actualmente, este problema no hubiese pasado, en esa época no era común el *testing*[3] por parte de los *testers*, permitiendo así poder configurar el programa una vez hubiese terminado su etapa

[3] Testeo.

de producción. Este error causó alrededor de 150 millones de dólares en pérdidas. (Zahumenszky, 2018)

Misiles Patriot: en la última década del siglo pasado se presenció una gran confrontación entre aproximadamente 34 países, la cual se conoció como la Guerra del Golfo. Los países, en vista de poder proteger sus intereses y a sus ciudadanos invirtieron un gran esfuerzo en la protección y desarrollo armamentístico que pudiera ofrecer cierto grado de seguridad para su gente, siendo bastante recurrentes los bombardeos de misiles de parte de Irak a Israel, lo que obligó a los países aliados a solucionar este problema (Corte Interamericana de Los derechos Humanos, s/f). EE. UU. En vista de todo esto, decidió desarrollar una cortina antimisiles llamada Patriot y la desplegó por todo el territorio israelí. El problema en cuestión ocurrió el 25 de febrero de 1991, en donde un misil fue pasado por alto por la cortina, lo que terminaría asesinando a 28 soldados. Este error proviene de un error matemático al momento de la elaboración del sistema de detección por parte del programa Raytheon, en donde el compilador sólo podía conservar datos con cierto número de dígitos y este ignoró por completo el ataque. (Rosique, 2022)

Errores de diseño

Los errores de diseño son también comunes, pero sus consecuencias suelen ser más invasivas que los errores de sintaxis. Estos errores son dados por una mala

planeación o falta de visión al momento de desarrollar la aplicación, es decir; que la aplicación que fue pensada para desarrollar una tarea no pueda ejecutarla o en lugar de ejecutar esa tarea ejecute otra distinta a la que se pensó en primer lugar, también es posible que la tarea pensada para ejecutarse sea excedida por parte del usuario y dentro de la planeación del diseño no se estimó el alcance que esta podría tener o que la tarea que se desea ejecutar no se ejecute desde ninguna óptica.

Consecuencias de los errores de diseño

Estos son bastante comunes y sus soluciones suelen ser parches de descarga para corregir errores o también llamados Bugs dentro del sistema. Algunos de estos errores tienen consecuencias millonarias para las compañías o para los usuarios tomando como ejemplo las aplicaciones recreativas, como juegos, un Bug que afecte a su tienda para realizar micropagos podría repercutir de forma sumamente negativa a los intereses de la empresa desarrolladora o de sus usuarios. López (2022)

Un ejemplo de estos errores es el que cometió la empresa fabricante de semiconductores Agilent Technologies debido a un problema en su transmisión de datos de su sistema de pedidos y de contabilidad llamado Oracle le provocó pérdidas de 105 millones de euros en facturación y de 70 millones en beneficios ocasionadas por las paradas de producción que causaba la inoperatividad del aplicativo. Este tipo de fallos presentaron una pérdida de 60.000 millones de euros

para EE. UU durante el año 2002. (Fernández & Fernández, 2002) Existe un gran listado de estos errores, pero los más relevantes para el medio son:

Therac – 25: esta es fue máquina creada en la década de los 70 del siglo pasado y permitía el tratamiento con radioterapia para personas enfermas de cáncer. Se puso en comercialización durante el 1982 y 1987 cuando la FDA prohibió por completo su distribución, en dónde fue descatalogada por un error en el diseño de su software (Ethics Unwrapped, 2020). Este error, trataba básicamente de una gran carga de radiación contra los pacientes, bombardeándolos con hasta 100 veces más de la cantidad esperada. Una investigación (Casey, 1998) llegó a la conclusión de que hubo una mala planeación para el desarrollo del software para la ejecución del aparato médico, de modo tal que la automatización de esta no estaba funcionando. Este error costó alrededor de 6 víctimas mortales.

Ariane 5: el 4 de junio de 1996, el cohete no tripulado Ariane 5 explotó después de unos pocos segundos de su lanzamiento. La misión de este cohete era la de poner en órbita cuatro satélites para la investigación del campo magnético de la tierra con relación a los vientos solares (Comisión Europea, 2003) El error en cuestión, tuvo lugar debido a la interpretación y lectura de datos, en este caso Bits que tenía el programa de ejecución. En consecuencia, el lector de velocidad del cohete transformó los datos del despegue, cambiándolos a números enteros, esto implicó un desvío y su explosión. Este tipo de errores solía llamarse como “error de coma

flotante de 64 bits” y se transformaba en “entero de 16 bits”, al momento de realizar el cálculo se pasó de números decimales a números enteros.

Investigaciones posteriores arrojaron los resultados, malos trabajos de investigación y de *testing* por parte de los desarrolladores de la aplicación, además de que este programa fue pensado para modelos anteriores, no se tomaron en consideración todas las variables que se debían de tener al momento del lanzamiento del nuevo cohete.

Errores de mala praxis y apreciaciones jurídicas

Existen otros inconvenientes ocasionados por las aplicaciones, siendo estos la mala praxis de los programadores, creando aplicaciones maliciosas, malwares o por medio de la suplantación de páginas de internet y aplicaciones. Este método de estafa es bastante común en Colombia. Lo que hacen los estafadores es copiar por completo el *Front End* de una página de internet y suplantan la información, desviando de esta forma los pagos que se realizan ante la entidad. Estas suplantaciones, o también llamadas phishing son tan frecuentes que las propias entidades bancarias destinan un apartado en sus páginas de internet para que sus usuarios puedan evitarlo. (Bancolombia, s. f.) A pesar de que las consecuencias legales de este son bastante obvias, son materia del derecho penal y por lo tanto no tiene necesidad de analizarse dentro de este escrito, sin embargo, es importante

recordar que este comportamiento está presente dentro de los daños ocasionados por las aplicaciones y programas. A partir del tipo de error se deberá de estudiar la lesión de este, el grado de participación de la aplicación, de los desarrolladores y también el papel que jugaron para que esto ocurriera.

Uno de los principales problemas que podría tener un análisis jurídico sobre estos errores es la vinculación objetiva del perjuicio con un autor dado que las tareas requeridas para generar una aplicación son titánicas y por tanto es usual la disposición de una cantidad considerable de recursos humanos. Por ello es común que cuando la entidad creadora del programa se le vincula a un análisis de responsabilidad, esta a su vez se remite a realizar una investigación interna para dar con los culpables del error mediante la asignación de un equipo especializado de análisis, o un equipo de peritos, con capacidad de rastrear dicho error y solucionar el problema.

El derecho siempre se adapta a las eras y es una respuesta directa a las problemáticas de cada sociedad. El aparato legislativo colombiano no tenía previsto un aumento tan masivo en el uso de aplicaciones o programas para la vida diaria, de tal forma que aún no existe legislación que sea expresa para los perjuicios causados por errores en aplicaciones. En casos de perjuicios, se debe remitir al Código Civil y algunas leyes subsidiarias creadas por la ley 1480 de 201, siendo estas el Estatuto del consumidor, la ley 23 de 1982 sobre de derechos de autor y

aquellas leyes específicas que se ajuste de mejor manera a lo que se requiera analizar.

Consecuencias de errores de Mala Praxis

Generalmente los errores son creados sin ánimo de defraudar o de causar algún tipo de daño, están los casos de errores de sintaxis y errores de diseño que se trataban en su gran mayoría de supuestos en donde los desarrolladores cometían equivocaciones moderadamente tolerables o que al menos podían justificarse de algún punto y se separaban completamente del ámbito volitivo de la acción en la realización de su aplicación. Este caso es completamente distinto, aquí los desarrolladores tenían el principal objetivo de perjudicar y lastimar de alguna forma a los usuarios incautos que terminaran presas de su creación, es claro que deben de tener algún tipo de propósito y generalmente tienen como principal fin una persecución de recursos económicos, sea a través del engaño directo a usuarios, extorción a empresas o hasta ataques directos a gobiernos. Algunos de estos ataques eran realizados usando aplicaciones conocidas como virus, las cuales tienen la intención de afectar el hardware o el software del ordenador, en algunas ocasiones, ni siquiera persiguen algún objetivo monetario, más allá del simple reconocimiento o gusto por sabotear los ordenadores de usuarios (Avast, s.f.)

Love Bug: también existe la posibilidad de que los desarrolladores se dediquen a realizar programas para afectar la estabilidad de un ordenador, sus funciones o

sencillamente inutilizar estos aparatos. Este tipo de ataques fue muy popular a finales del siglo XX y principios del siglo XXI, existiendo algunos casos con daños a hardware multimillonarios. Pero el que es quizás el primer gran virus informático fue el Love Bug (White, 2020) el cual tenía una premisa simple pero contundente, robar información a los infectados que le permitieran dar contraseñas para usar internet, debido a que en esa época, aún no existía una tarifa plana absoluta para poder acceder a internet, además de que su acceso estaba mayormente condicionado a las redes telefónicas, por lo tanto, navegar en internet era un gasto constante por minuto o por hora, dependiendo del plan de telefonía que se tuviese.

Caso Hive: en el capítulo siguiente, se explicará por qué están crucial e importante la seguridad en los datos, pero a grandes rasgos, la información es una herramienta en extremo importante, tan relevante que en nuestros tiempo se traduce en estrategias de marketing capaces de mover cientos de miles de millones, por esto es que existe una gran cantidad de casos en donde se roban información, algunas veces puede ser solo para rastrear hábitos de compra o acciones pequeñas como búsquedas en navegadores, pero también existe información que es más sensible, como información de tarjetas de crédito o secretos empresariales. Al secuestro de datos se le llama *Ransomware*, el grupo Hive eligió sus víctimas hospitales y escuelas, cobrando varios millones de euros como extorsión para poder regresar los datos secuestrados. En una operación conjunta entre la Europol, Países Bajos, Alemania y Estados Unidos, pudieron desmantelar el grupo y frustrar sus planes,

impidiendo el cobro de más de 130 millones de dólares a más de 300 víctimas. (Granadillo, 2023)

Incidente Target: además del secuestro de datos, los hackers buscan realizar más acciones delictivas con la información además de solamente incautarla y regresarla luego de tener algún incentivo financiero, también buscan literalmente hurtar el dinero de las cuentas de las personas que se ven afectadas por estos ataques. Esto sucedió al supermercado estadounidense Target, el cual fue víctima de un robo de datos masivo, alrededor de 70 millones de personas fueron afectadas con este acceso de información. Los datos sustraídos tenían información extremadamente sensible, como direcciones de residencia, tarjetas de crédito, cuentas bancarias, nombres de los usuarios y direcciones de correo electrónico, dándoles datos suficientes a los criminales de realizar robos de identidad. Este ataque disparó las alertas de la compañía, que de forma inmediata notificó a sus clientes y les explicó que no habría cargos a sus tarjetas de crédito por compras fraudulentas (Muñoz, 2014)

Síntesis

A lo largo de este capítulo se analizó el impacto que pueden tener los errores dentro de la programación de aplicaciones y no deja de ser curioso que al menos, en los aspectos más relevantes como en los mencionados asistentes de vuelos o

detectores en misiles los estándares de prueba y ensayo no fueron realmente los óptimos esperados para programas de una envergadura como esa, actualmente existen bastantes barreras que impiden resultados como esos, sin embargo, a pesar de la experiencia de los desarrolladores es sumamente difícil que estos errores no se vuelvan a replicar pero si reducir en una gran proporción.

Lo cierto es que en la actualidad existen diversas herramientas que pueden ayudar a disminuir la incidencia de estos errores dentro de las aplicaciones, así como una buena cantidad de expertos y peritos que pueden tratar de analizar estos errores antes de que sean probados por el público, así como grupos especializados en ensayar y probar estas aplicaciones. Lo ideal sería realizar una destinación por ley, de una parte, de los recursos que se usarán para el desarrollo de las aplicaciones, siempre y cuando, este sea un programa que tenga algún nivel de responsabilidad con la integridad física humana. Crear departamento especializados al análisis y prevención de estos errores. El Estado, a su vez, deberá de destinar parte de sus recursos para protección en un revestimiento y entrenamiento de su cuerpo policial para poder frenar esta problemática, la cual, al menos en Colombia, tiene un gran auge, pero que tristemente los esfuerzos policiales son bastante deficientes (Álvarez, 2023).

Para poder realizar de la mejor manera la capacitación del cuerpo policial, para que logre identificar estos delitos de forma oportuna, es necesario una capacitación profesional, que sea una integración entre las competencias de

análisis y reconocimiento, características del cuerpo policial, como de ingenieros en sistemas, capaces de identificar con facilidad estos crímenes. Es bastante notorio que, las características especiales que necesita este cuerpo de atención son bastante difíciles de complementar y en esto radica el principal problema del aumento de los delitos informáticos y de la carencia de aplicación de la normatividad a estos delincuentes.

El esfuerzo no debe de ser únicamente por parte del Estado para tratar de frenar esta problemática, sino también de las empresas y usuarios, mediante la participación en campañas pedagógicas que enseñen cuándo podrían ser víctimas de algún tipo de estafa o problema causado por las aplicaciones. El problema principal radica en el hecho de que no siempre los daños jurídicos son causados con dolo, sino que la mayor parte de estos problemas son causados por descuidos, podrán ser descuidos mayores o menores, pero que no comprenden ningún tipo de trasfondo volitivo, por tanto, a pesar de que se pueda entrenar de alguna forma a los usuarios, la capacidad de que exista algún tipo de error por parte de los desarrolladores siempre va a estar presente.

Finalmente, hay dos puntos importantes para poder frenar un poco la comisión de errores por parte de los desarrolladores: la primera es a través de la comisión de la que se habló previamente, el entrenamiento de brigadas especiales que puedan definir, estudiar y comprobar las aplicaciones. Sin embargo, esta medida constituye un gran gasto gubernamental, un componente volitivo y un gran

personal de policías entrenados, hecho que resulta muy lejano a la realidad de la mayoría de los países, incluyendo Colombia, sumado al hecho de que dichas brigadas tendrían que estudiar todas las aplicaciones que saldrían al mercado, lo cual también podría significar entrar en conflicto en materia de patentes o derechos de autor, aumentando la carga y reduciendo la eficiencia del servicio.

Asimismo, necesitarían del reconocimiento evidente de que dicha aplicación generase una infracción. Este último problema nos da paso al segundo punto, siendo este que las desarrolladoras de aplicaciones cuenten con su propio sistema de prueba, pero en la mayoría de los casos terminan siendo los mismos programadores de la aplicación quienes realizan las pruebas preliminares; por lo que en existe la posibilidad de que recaigan en los mismos errores y no puedan comprobar de forma exitosa el impacto que estos tendrían.

Por tanto, se debería de fijar un punto medio entre los desarrolladores y el Estado mediante la creación de políticas y entidades, ya sea dentro de las mismas desarrolladoras o siendo empresas independientes, que brinden servicios como probadores para las aplicaciones. Esto además de dar apertura a una nueva esfera de mercado y brindar una mayor protección frente a la responsabilidad de las desarrolladoras respecto a sus creaciones; debido a que la carga recaería en las empresas probadoras, podría reducir la generación estos errores. No obstante, dicha solución podría llegar a ser extremadamente restrictiva por la existencia de aplicaciones que pueden contener datos personales o datos sensibles, entrando en

un área gris de ponderación respecto a los principios de seguridad y de privacidad. Estos principios se abordarán más adelante durante la investigación.

Capitulo III. La ética en la IA

Limitaciones éticas de la IA

La importancia principal de este apartado, radica en la necesidad de ponerle un límite a la creación, calibración, entrenamiento y propósitos de las IA, así como todo lo relacionado con las consecuencias causadas a raíz de los problemas que estas herramientas puedan causar, sin embargo, es claro que antes de empezar a hablar sobre algún tipo de sistema normativo, es menester tener bases sólidas que no sean simplemente un puñado de texto jurídico, una fuente importante de donde van a emanar todas las normas que regulen las contingencias y creación de estas herramientas, es por esto que un simple texto normativo se queda corto para poder definir y regular un marco normativo.

En el derecho interno las fuentes normativas son diversas, a saber: la Constitución, la ley, la jurisprudencia, la costumbre, los principios generales del derecho y la doctrina, esto acorde a la definición dada por la Corte Constitucional en la sentencia C-104 de 1993. A pesar de lo anterior, suele existir conflicto respecto a la preponderancia entre estas fuentes de derecho, naciendo de dicha manera múltiples corrientes doctrinales. Una de ellas apuesta por los principios y/o marcos éticos – morales como principal fuente para crear contenido normativo. Así pues, el

principialismo jurídico justifica su pensamiento destacando al interpretarlo como estándares inmovibles que sirvan como pilares capaces de definir y estructurar un sistema normativo sólido y complejo.

Para la creación de los marcos teóricos se puede reconocer una gran influencia por parte de la cultura popular y la literatura. La sociedad siempre termina asimilando de forma paulatina todo lo relacionado con los sistemas normativos y éticos, siendo algo completamente curioso ya que existen diversos escritores de ciencia ficción que ya establecían parámetros muy semejantes a los que se podría encontrar en los marcos éticos actuales. La moral y la ética están fuertemente ligados con la sociedad, hoy, por ejemplo, en el marco ético-moral de América Latina se considera un dilema ético comer ciertas especies, mientras que en algunas zonas de Asia lo consumen. Sin embargo, no todo principio se encuentra sujeto al contexto geográfico y cultural, sino que se encuentra en un estado aparte, casi superior e idealizado, siendo estos los que permiten fijar un marco ético eficiente

Marco ético de las IA

Para poder definir lo que es un daño causado por una IA, es necesario primero; estudiar los errores característicos de las aplicaciones y segundo; poder definir realmente que es lo que se está protegiendo al momento de trasgredir los principios a través de estos errores. El segundo acápite de este texto tuvo como

objetivo definir y estudiar el alcance de los errores en las aplicaciones, sus causas, consecuencias y demás, este por otro lado, tendrá como objetivo explicar a través de los autores más representativos del medio cuál es todo el aparato ético que tiene como fondo el tema en cuestión, así como las diferentes aplicaciones de este.

Actualmente, los reglamentos y normativas existentes apenas se han ido ajustado al estruendoso y vertiginoso paso que van generando las II. AA en cuanto su impacto sociocultural y económico. Algunos Estados han tratado de configurar un marco legal, por ejemplo, la GDPR (Reglamento General de Protección de Datos de La Unión Europea) el cuál, tiene como propósito fijar y establecer pautas que permitan regular y velar por los datos de sus ciudadanos (Zaeem, R. N. & Barber, K. S, 2021).

A pesar de esto hay un consenso sobre lo que se interpreta como Principios dentro de esta problemática, existiendo algunos autores como o René Urueña o John Tasioulas[4] que han llegado a conclusiones bastante cercanas sobre lo que se interpreta como principios rectores, sin embargo, para la presente investigación, se tomara el articulo desarrollado por el Berkman Klein Center For Internet Society de la Universidad de Harvard titulado "*Principled artificial intelligence: mapping consensus in ethical and rights-based approaches to principles for A*I*"* (2020). convirtiéndose en un pilar fundamental para encontrar y delimitar una definición

[4] "*First Steps Towards an Ethics of Robots and Artificial Intelligence",*
"Autoridad algorítmica: ¿cómo empezar a pensar la protección de los derechos humanos en la era del "big data"?"

aproximada de los principios rectores. De igual manera, dicho artículo también funciona como un compendio recopilatorio de textos y autores afines al tema, nutriendo el debate y solidificando la estructuración doctrinal respecto a los principios, derechos y reglas de juego que deberán de tener los desarrolladores y los sistemas jurídicos para poder responder ante los diversos vacíos normativos.

Retomando lo anterior, uno de los aspectos más importantes del artículo es el establecimiento de principios rectores, a los cuales se le realizará su debido análisis en la presente investigación.

Los siete principios rectores de la IA son los siguientes:

- Privacidad
- Responsabilidad
- Seguridad y protección
- Transparencia y explicabilidad
- Equidad y no discriminación
- Control humano de la tecnología
- Responsabilidad profesional y promoción de los valores humanos.

Cada uno de estos, a su vez, presentan distintos apéndices que permiten desglosar y entender mejor el alcance y contenido que tiene cada principio.

Principio de privacidad

Este principio ha sido ampliamente analizado y estudiado alrededor del mundo. La preocupación por la intimidad y el tratamiento de los datos contenidos en estos sistemas no es algo que deba de tomarse a la ligera, ya que dicha información tiene usos en múltiples campos sociales, tales como la política o el marketing. Es por esto que la privacidad y la limitación a la información que se otorga es en sí mismo un bien. Por ejemplo, al momento de utilizar la gran mayoría de aplicaciones para el sistema operativo Android es necesario recurrir a un aviso que explique la política de privacidad que tiene el sistema para sus aplicaciones, siendo una obligación para los desarrolladores el explicar que hacen con los datos que son ingresados dentro de la aplicación, o si esta gestiona datos que puedan considerarse como datos sensibles. Android suele usar el RGPD como base para para la fundamentación de estas políticas.

También es posible reconocer otro ejemplo y este se encuentra en la mayoría de los teléfonos móviles con sus asistentes virtuales, los cuales son IA, tales como Amazon Alexa, Siri, Google Assistant Go, entre otras que sean similares o ejecutar funciones parecidas. Estas herramientas acceden a los números de contacto en el teléfono móvil, pueden realizar compras y tienen acceso al historial de internet. Al tener contacto con esta información sensible, como el acceso a las tarjetas de crédito para realizar las compras es común el pensar que hacen las compañías para proteger estos datos o qué hacen con ellos y que hacen con esos datos.

Para poder acceder al uso de estas aplicaciones es necesario aceptar la política de privacidad, que se pida al usuario aceptar los términos y condiciones del uso de la aplicación, en estos términos y condiciones está el apartado para el uso y tratamiento de datos, o en algunas ocasiones este índice es fijado a parte dentro de un consentimiento informado. Esta política variará dependiendo del país, del tipo de aplicación o de los datos suministrados en la misma. Si el usuario no acepta el destino de sus datos o lo que realizará la compañía con estos, no podrá acceder de los servicios de la aplicación. En Colombia este tratamiento de datos está regulado a través de la Ley 1581 del 2012.

Dentro de este consentimiento informado deberá de existir:

- La posibilidad de realizar modificaciones dentro de los datos otorgados a través de rectificación.
- Control sobre el uso de datos, en donde deberán de aclarar el motivo por el cual necesitan estos datos y que harán con ellos, dándole la oportunidad al usuario para disponer de estos como guste.
- Derecho a eliminar esta información, en Colombia está habilitado gracias al Artículo 9 de la Ley 1581 del 2012.

La importancia de estos datos, además, van más allá de proteger a los usuarios de estafas o delitos informáticos, es común que algunas de estas empresas utilicen estos datos como grandes fuentes de investigación o encuestas, para poder conocer gustos, patrones de compras, intereses personales, preferencia música y

muchas más, todos con fines de marketing o de interés para la empresa. A este tipo de información se le conoce como Big Data (Camargo-Vega, 2014).

Generalmente, al usar una aplicación que pueda recoger datos, se suele tener la idea errónea de que el uso de la misma es gratuito cuando en realidad la operación transaccional no se efectúa con dinero, sino con datos, como búsquedas en internet, existe un caso en el que un padre se enteró del embarazo de su hija porque, al momento del uso de la herramienta de búsqueda en internet, este era bombardeado por anuncios afines a lo que podría consumir una persona que esté próxima a tener un bebé o que esté en esa etapa, ¿Pero cómo sabía la herramienta de búsqueda que su hija estaba esperando un hijo? Sencillo, asoció los resultados de las búsquedas de los síntomas de la hija en internet con los síntomas que tiene una mujer en embarazo (Lane, 2012)

Principio de responsabilidad

Este principio es pilar para el entendimiento de los problemas ocasionados por las II. AA. Básicamente trata de fijar a los responsables por la toma de decisiones de las II. AA. Cuando se piensa en quién o como responder por un error humano es muy sencillo, corre un mar de tinta escrita por doctrinantes, aparatos burocráticos y legales que permiten definir quién es realmente el culpable al momento de un incidente que pueda afectar alguno de los bienes jurídicos de cada individuo. Por otro lado, cuando dicho error es provocado por una aplicación o IA, el

juicio de la culpabilidad y la definición de daño provocado por esta se complejiza. John Tassioulas (2019) aborda este tema dando una solución un tanto particular. El trata de ayudar a resolver esta problemática a través del sistema de indemnización preventiva otorgada por la institución de los seguros de responsabilidad civil, lo cual se ejemplifica en el día a día en las obligaciones impuestas respecto a ciertas actividades en las cuales se requiere tener un seguro respaldando, tal como ocurre al comprar un vehículo, es donde se torna necesario pagar un seguro de responsabilidad para terceros para poder tener su circulación en regla.

Para Tassioulas, las aplicaciones podrían tener este tipo de seguros de responsabilidad. En este punto se generan dos interrogantes: el primero es que no es posible comparar el riesgo que implica la conducción de un vehículo con los riesgos que se podrían causar con el uso de las aplicaciones; por decirlo de algún modo, el daño causado por una aplicación en la gran mayoría de los casos será de forma económica. El segundo es que sencillamente los desarrolladores podrían producir sus aplicaciones de modo tal que no se preocupen por el resultado final o por su responsabilidad dentro del proyecto ya que tienen el salvavidas del seguro, este podría ser considerado una excusa para que las empresas creadoras de aplicaciones realicen sus funciones de forma correcta.

Lo realmente importante al momento de este principio es que sea absoluto y severo, sin dar pie a posibilidades de desviación o de hacer trampa, sin importar el tamaño de la compañía. Amazon, por ejemplo, fue multado en el año 2023 por violar

sus propios términos y condiciones de seguridad (esto será explicado en el acápite de privacidad y protección) en su asistente virtual y en sus *Echo Dots* con su IA Alexa por grabar la voz de menores de edad sin permiso, teniendo que pagar una multimillonaria suma de dinero (Freire, 2023)

De igual manera, frente a este principio es necesario tener en cuenta las siguientes subdivisiones:

Verificabilidad y replicabilidad

Limitar el funcionamiento de las IA a arrojar siempre el mismo resultado por medio de la experimentación y el uso. Esto se realiza a través de los ya mencionados evaluadores.

Evaluaciones de impacto

Se debe de realizar un análisis de riesgo/beneficio sobre los impactos posibles a los derechos humanos. Esto en la práctica es un poco más complejo de comprender, porque si se piensa detenidamente, algunas de estas IA han reducido las oportunidades de trabajo en algunos sectores, es necesario entonces realizar una ponderación de principios, realizar un análisis concienzudo que permita

reconocer cuándo es realmente necesaria la creación de la herramienta, así como su impacto dentro de la sociedad.

A pesar de que el progreso deba de estar construido por sacrificios, deberán de ser justificados y siempre bajo la órbita del bien común y en protección de este. Actualmente el planeta tierra se encuentra atravesando una era digital, con un cambio constante, casi sofocante, dificultando y obligando a la sociedad ajustarse a sus cambios y a sus nuevos paradigmas, algunos tienen un pronóstico bastante negativo y pronostican unos 300 millones de trabajos perdidos a nivel mundial gracias a las IA (Diaz, 2023) John Tassioulas (2019) también toca el tema en su texto, sin embargo, él tiene un pronóstico un poco más optimista, diciendo algo obvio; no es la primera vez que la tierra se enfrenta a un cambio de esta magnitud y en ultimas, la sociedad y el ser humano siempre terminan adaptándose al cambio, inventando nuevos trabajos o simplemente ajustándose a las necesidad eventuales que se encontraran en el tiempo. Este es uno de los muchos ejemplos que se pueden relacionar a esta evaluación; sin embargo, debido a que es algo que está sucediendo actualmente tiene más impacto y se puede entender mejor este apéndice del principio.

Responsabilidad ambiental

Responsabilidad por los controladores y desarrolladores sobre sus riesgos ecológicos. Para crear estas herramientas es necesario de un amplio número de desarrolladores además de sus herramientas de trabajo, ordenadores y servidores, todos estos necesitan de energía para funcionar. También, es necesario realizar un estudio sobre el impacto mismo que la aplicación podrá tener al momento de su finalización y presentación al público. Podrían existir algunas aplicaciones que, de cierta forma no tienen el mismo impacto ecológico que podría tener alguna que ayude a conseguir un taxi o conseguir un servicio de transporte. Para poder almacenar datos se necesita de un gran esfuerzo y de bastantes recursos, tanto económicos, por la manutención y compra de servidores que sean capaz de guardar estos datos hasta energéticos y ecológicos. Es por eso necesario aumentar la carga de la responsabilidad sobre este tema. Por ejemplo, cada búsqueda en internet genera en promedio un 0.2 gramos de CO2 y el impacto energético es un consumo equivalente al 7% global (Castro, 2023).

Requisito de evaluación, auditoría y creación de un órgano de vigilancia

Deberán de crear aplicaciones que sean aptas para ser auditadas, así como crear mecanismos de aprendizaje que permitan aprender y evaluar sus propias aplicaciones. Los controles periódicos y eficientes permitirán un ajuste de cuentas mucho más sencillo de presentarse algún caso en el que pudiera ocurrir algún tipo de irregularidad con los servicios que brindan las compañías desarrolladoras.

Lo anterior, sin embargo, implica un desgaste económico y burocrático bastante elevado para los Estados, la creación de un organismo de control que permita revisar y analizar las aplicaciones lanzadas al público, así como el impacto que estas tendrán. Se necesitaría de un esfuerzo colosal de capacitación y de personas para formar grupo de trabajo bastante amplio, con peritos y distintos profesionales en la materia que pudieran definir y encontrar los problemas, el responsable y como estimarlo monetariamente. Esto, al menos en el corto plazo es algo muy poco probable, porque se necesitaría de un estudio y planeación por parte del Estado. Sería absurdo pensar en controles de revisión internos, en la práctica podrían ser parciales y nublar o dificultar un estudio concienzudo de los efectos que estas aplicaciones tendrán.

Existe la posibilidad de que agentes externos al Estado desempeñen una función de vigilancia y que estos respondan directamente ante él, solo fungiendo como un mecanismo de prueba o evaluadores y no como uno un ente capaz de castigar o investigar los desperfectos originados por las compañías, sin embargo, la tercerización de esta labor es una opción muy poco fiable, este mecanismo de control al tratarse de un ente de vigilancia y análisis tendría una gran cantidad de poder y podría desembocar en un conflicto de intereses entre la compañía Supervisora y la desarrolladora.

Capacidad de apelación y soluciones por decisiones automatizadas

Otorga la potestad a una persona, la cual fue juzgada por la decisión de una IA para pedir que sea analizado su caso de nuevo y que sea impugnada esa decisión. Por ejemplo, en el hipotético caso de que en Colombia existiera un sistema automatizado de análisis de tutelas que se encargara de fallar de forma igual en casos muy similares, podrían existir algunos componentes que generen disonancias entre los casos y esto podría generar en sí mismo un resultado completamente distinto al que fue emitido por la IA, en esos casos es, evidente que la parte afectada pueda exigir una apelación de la providencia emanada por la corte.

Actualmente existen algunos programas que toman decisiones judiciales o ayudan a los jueces a tomar este tipo de decisiones, para fines prácticos se consideran más una herramienta de ayuda que un juez capaz de impartir e imponer sentencias, a pesar de esto, es posible encontrar en las aplicaciones ciertos patrones que indican sesgos morales y éticos en la toma de decisiones de los programas. John Tassioulas plantea un panorama bastante interesante al respecto, en su texto (2019) Habla sobre una alternativa planteada por el Parlamento Europeo a algo similar a un seguro de responsabilidad sin culpa, similar al “deodand”. Esta propuesta, trata de aliviar el problema pero no de frenarlo, el uso de seguros para detener estas cosas no suele ser un disuasor para que los desarrolladores creen programas eficientes y confiables, esto de hecho, podría ser un detonante para que hayan aún más problemas involucrados por las IA debido a que no se gastarían tantos recursos para el análisis, estudio y experimentación de las aplicaciones, así

como de sus resultados, sino que menguaría la responsabilidad de las empresas reduciendo así sus obligaciones pecuniarias de cara a sus usuarios.

Obligación y responsabilidad jurídica

También llamado, principio de responsabilidad legal, está estrechamente relacionado con el anterior apéndice. Este principio tendrá como objetivo llevar a los culpables de los daños causados por la IA ante la justicia o que puedan indemnizar a las personas que sufrieron el daño de alguna medida.

Principio de Seguridad

En apartados previos se mencionó el Principio de Privacidad el cual aclaró la naturaleza sensible de los datos que podrían contener las II. AA, de tal modo que es necesario asegurar estas herramientas y blindarlas de ataques de agentes externos. Además de esto, también es necesario entender la seguridad como fiabilidad, es decir, que la aplicación desarrollada realice la operación por la cual fue diseñada. Para poder ejemplificar mejor este principio se necesitará realizarlo desde dos ópticas, la primera entender la seguridad, no como protección sino como fiabilidad y la otra óptica, siendo la más relevante, la que debe entenderse no como fiabilidad sino como protección.

Las aplicaciones son, en sentido estricto, herramientas que permiten realizar acciones, estas dependerán de los deseos o necesidades que quieran resolver los desolladores a través de la programación de estas. Si se considera una aplicación exitosa necesitará algo mucho más que la sencilla utilización en masa de esta, por ejemplo; nadie utilizaría WhatsApp si dejara de funcionar cada cinco minutos, nadie en su sano juicio optimizaría un sistema de ayuda en hospitales que mandará señales de alerta a las enfermeras si este tuviera periodos de inactividad no programada. Es por esto que el correcto funcionamiento de una aplicación es crucial. Por otro lado, la otra arista de este principio es sumamente vital para poder comprender el principio de Privacidad.

Actualmente en algunos países del mundo es posible utilizar Amazon para realizar casi que todas las compras del hogar, ya que este es dueño de Whole Foods (Rojas, 2017) y le permite garantizar el abastecimiento total de una casa sin tener la necesidad de salir de ella, esto implica que al momento de realizar y efectuar la transacción con la tienda hay involucrada una gran cantidad de información sensible, datos como: dirección, número de cuenta bancaría o tarjeta de crédito, hasta gustos y preferencias al momento de comprar X o Y artículo. Este tipo de información podría desembocar en robos o muchas actividades fraudulentas. La carga de la protección y seguridad de una aplicación deberá de ser en todo momento de la compañía desarrolladora, siendo la salvaguarda responsable de proteger cualquier tipo de dato que pueda contener su aplicación.

Se han presentado varios sucesos lamentables en compañías de alto impacto que sencillamente decidieron omitir o hacerse los de la “vista gorda” al respecto, como lo fue el caso de Sony en el año 2011. Sony, aparte de ser una de las empresas más importantes relativas a la manufacturación y fabricación de electrodomésticos, también tiene participación en el mundo del entretenimiento, siendo dueña de Play Station, ya por el año 2011 tenía todo un sistema bien elaborado que permitía la compra de contenido digital para poderlo usar en su consola, el problema fue que un grupo mal intencionado de Hackers decidió atentar contra la compañía robando la información de 2,5 millones de usuarios y con esto el número de sus tarjetas de crédito (Villanueva, 2013). Lo más curioso de este ataque no fue el deficiente y mediocre sistema de protección que tenía la compañía en ese entonces, si no su respuesta de cara a sus clientes, sugiriéndoles cancelar sus tarjetas de crédito y “compensándolos” mediante descuentos en su tienda virtual. Es por esta conducta y el hecho de haber recibido tres ataques más el mismo año, terminó recibiendo un premio por la peor falla de seguridad. (Laguna, 2021).

Lo realmente interesante de este suceso fue que la oficina del comisionado del Reino Unido trató de multar a Sony por esta falla enorme en sus servidores, siendo de igual forma una suma risible comparada con el gran daño que ellos hicieron, pero en respuesta, Sony alegó que ellos también eran victimas en esa situación (Villanueva, 2013). En pocas palabras, la empresa tuvo unas consecuencias muy leves por su grave desinterés y su falta de compromiso con sus

usuarios, poniéndolos en una situación sumamente grave, mientras que los Estados no tuvieron ni el menor interés en tratar de defender a sus ciudadanos como consumidores. Quizás este desinterés estatal se haya debido por la época tan “primitiva” en la que se encontraba aún toda la legislación referente al tema de aplicaciones o daños digitales, pero no deja de ser un agrio recordatorio a la necesidad de recrudecimiento de la legislación al respecto.

Principio de transparencia

Este principio establece que todas las aplicaciones IA deberán de ser fáciles de estudiar y analizar para poder trazar información sobre errores, así como el rastreo de fisuras en la seguridad o de los datos. Estas herramientas deberán de tener opciones que permitan una fácil supervisión de sus funcionalidades y operaciones. Es evidente que este principio no puede trasgredir el principio de privacidad.

Este principio se divide en códigos y algoritmos de fuente abierta. todas las IA están creadas usando como base códigos y secuencias de algoritmos. Es común encontrar repositorios en internet que contengan lenguajes de programación o herramientas para la creación de nuevas aplicaciones, a esto se le conoce como “bibliotecas”. Estas bibliotecas ayudan al entendimiento global de las aplicaciones ya que están al alcance de todos, eliminando la posibilidad de la creación de monopolios o que a estas solo puedan acceder algunos.

Principio de equidad

Es posible crear IA para diversas funciones, desde gestionar funciones pequeñas en un teléfono móvil, realizar la compra de víveres para tu casa o también la de tomar decisiones realmente importantes en la vida de una persona, decisiones de alto impacto que podrían comprometer para siempre el bienestar de un usuario. Previamente se mencionó un ejemplo de una IA en Colombia que ayudara a realizar sentencias de tutelas, el cual puede fallar y dictaminar sentencia a favor o en contra de la tutela que el usuario haya realizado. El motivo principal para la creación se esta aplicación es la de reducir las grandes cantidades de trabajo que tenía la Corte para tomar decisiones. Las tutelas deberán de ser falladas de forma igual, siempre y cuando el caso sea sobre una materia bastante similar a las que se fallaron en primer lugar. Esto es un problema porque es probable que un caso con particularidades pueda fallar de la misma forma que uno bastante común sólo por que esté relacionado con la materia no signifique que sea bajo los mismos estándares.

En EE. UU. existe una IA llamada COMPAS, esta es una herramienta al alcance de los jueces para poder determinar la tasa de reincidencia de un individuo en la cárcel. (Mattu, 2023). Este programa presentó un periodo de reincidencia mayor por sectores y por diferencias raciales. Aquí es donde empieza el problema de la correcta aplicación de este principio, es el eliminar los componentes de sesgos

personales que se puedan tener al momento de crear una IA, es necesario ser objetivo e imparcial al momento de cargar una IA con datos (*Machine learning*) o supervisarla para que no tenga predisposición si tiene un método de aprendizaje automatizado.

Principio de control humano de la tecnología

Los seres humanos deberán de ser capaces, en todo momento, de controlar y supervisar la toma de decisiones de una IA, este control dependerá de la incidencia que pueda tener esta IA en la vida de sus usuarios, además de la automatización en las funciones de esta. Los responsables de las IA deberán de revisar las decisiones automáticas generadas por sus creaciones.

Principio de responsabilidad profesional

Todo el aparato desarrollador deberá de estar comprometido con los anteriores principios mencionados, además de tener precisión con el diseño de las funciones de sus programas. En el anterior capítulo de esta investigación se habló de forma bastante extensa sobre los distintos errores que se pueden presentar al momento de realizar labores de desarrollo, algunos de estos sólo implicaban un descuido por parte del programador. Estos descuidos podrían ser desde unos muy grandes, hasta algunos que, aun teniendo la mayor diligencia y cuidado al momento

de realizar la codificación, era algo que se podía escaparle de las manos a cualquiera que realizara esa tarea. También existen los errores que involucran ya no descuidos, sino un deliberado comportamiento de hacer el mal o atentar contra los intereses de terceros. Dependerá entonces de dos factores, un factor objetivo que se podrá medir o calcular en cuanto al grado de participación, cargo que ostentaba dentro del proyecto y de uno subjetivo, como su voluntad y propósito al momento de realizar la labor asignada lo que logre determinar el alcance, el grado de culpabilidad y el cómo castigar al desarrollador.

Principio de promoción de valores humanos

Es común pensar en el impacto que pueden tener las IA de cara al ser humano, así como la posibilidad de que estas puedan dañar o lastimar en alguna medida al hombre, por eso estas creaciones deberán de estar guiadas por los principios éticos y morales que tienen los seres humanos. Generalmente al imaginar o pensar en Robots conscientes o con la capacidad de tomar decisiones lo primero en relacionar con ese pensamiento es la ciencia ficción, seres artificiales con capacidad de aprendizaje y que están extrañamente cercanos a los ideales humanos con competencias suficientes para realizar procesos de creación o modificación de un sinfín de variables.

Isaac Asimov (1950), con su basta imaginación también llegó la misma conclusión e ideó en sus obras literarias una pequeña, pero muy eficiente guía moral

hipotética que debían seguir los robots para poder preservar los ideales y vidas humanas. Pensar entonces en una guía moral que determine la creación o utilización de programas computacionales no es algo visionario o soñador, sino necesario. La fundamentación principal para realizar intervenciones legislativas, para desarrollar leyes y normativas que puedan proteger los intereses de los hombres y los bienes jurídicos personales emanan directamente de la moral y de la ética de cada sociedad, establecer entonces principios capaces de fungir como una brújula moral que ayude a determinar el rumbo de las IA y programas computacionales es un menester por parte de toda la comunidad de filósofos y doctrinantes afines al tema.

Marco ético en Colombia

En la actualidad, el Ministerio de Ciencia, Tecnología e Innovación emitió un documento para la discusión en donde se aglomeraban una buena cantidad de principios que se analizaron en este capítulo, abordando temas como los retos para la implementación, cómo realizar la adopción y la relación entre estos y los derechos humanos. Si bien, este estudio es un excelente punto de partida para abrir los impulsos legislativos en nuestro país, no deja de ser una recopilación de otros manuales de principios sobre este tema, siendo algo recurrente dentro del documento la referencia a la investigación realizada por el Berkman Klein Center.

Los principios analizados dentro de esta discusión fueron diez: transparencia, explicación, privacidad, control humano de las decisiones propias de un sistema de IA, seguridad, responsabilidad, no discriminación, inclusión prevalencia de los derechos de niños y adolescentes, beneficio social. De esta lista de principios, el único del que no se habló en la parte anterior de este artículo fue el de la prevalencia de los derechos de niños y adolescentes, en dónde Guío (2020) propone un punto de vista interesante que no se había abordado antes y es el carácter de especial protección que tienen los menores, el cual no puede ser menoscabado de ninguna forma.

Este principio, habla básicamente de una integración sana y enseñanza para los menores, en su manipulación al igual que en la creación de estos sistemas, siendo claros y fácilmente comprensibles para los menores. Además, no deja de ser evidente el cuestionamiento ético del alcance de estas herramientas para los menores, si bien, actualmente no hay muchas opciones que puedan ser realmente perjudiciales para los menores, en un futuro podrían existir IA que pudiesen contener material inapropiado o nocivo para los menores, es por esto que este principio cobra una especial importancia dentro de un marco ético, no sólo para ajustar las regulaciones en pro de los menores y su estado como sujetos revestidos de protección especial, sino también como una barrera que se deberá fijar para impedir el acceso de estos a contenido inapropiado.

Caso de discusión: pornografía *deep fake* y la relación con los principios mencionados

Para ejemplificar mejor el alcance que tienen los principios y como podrían ser aplicados, se analizará la problemática actual que se está presentando con las aplicaciones *Deep fake* y la pornografía. *El Deep fake*, es una herramienta de inteligencia artificial entrenada por medio del *Deep learning*, la cual utiliza el rostro de una persona y lo inserta en un video externo. Esta técnica ha sido utilizada en otros escenarios (Bañuelos, 2020), como en el cine común y corriente, como lo hizo Disney con la muerte de la actriz de Star Wars, Carrie Fisher o en Fast And Furious con la muerte de Paul Walker.

Más allá de que esta práctica en manos equivocadas pueda generar infinidad de problemas legales que van desde la creación y fabricación de pruebas para poder evadir delitos, o también con la creación de imágenes para la implicación de alguna persona en delitos o un sinfín de posibilidades, esto genera un nuevo problema y un vacío del que no se ha profundizado lo suficiente y es el caso de la pornografía usando rostros de menores.

Hoy en día es bastante sencillo encontrar estas herramientas en las tiendas de aplicaciones de los teléfonos móviles, aplicaciones de redes sociales o en la web y esta facilidad para usarlas no es privativa únicamente a las aplicaciones que las utilizan como una mera novedad, también existen para temas de entretenimiento para adultos. En principio, estas aplicaciones tienen una base similar a los filtros

que se usan en algunas plataformas de redes sociales, aunque también son capaces de generar escenarios inventados, con personajes imaginarios. Las posibilidades solo están ligadas a la capacidad de emular por parte de la aplicación y la capacidad de imaginar del lado del usuario, por lo tanto, pueden crear cualquier cosa que pase por la mente retorcida de quien la use. No hay verificación de edad para los datos insertados que sean concernientes a la creación de la obra, o de donde se han conseguido las imágenes fuentes para realizar las obras, es decir; es bastante sencillo evadir los precarios sistemas de seguridad que tienen estas aplicaciones, basta con mentir para acceder a la aplicación o sencillamente aceptar los términos y condiciones y violarlos deliberadamente.

El uso de estas herramientas arroja varios cuestionamientos: ¿cómo se puede realmente defender el principio de seguridad de la información si estas aplicaciones no tienen ningún tipo de control?, son herramientas automatizadas que permiten la realización de un video sin muchas complicaciones. De hecho, es más sencillo analizar el tema desde una óptica de exclusión y no de implementación, ya que este problema vulnera casi todos los principios estudiados y el problema más grande actualmente es el silencio por la mayor parte de los sistemas. Si las obras son realizadas usando datos de mayores de edad, pueden entrar en categorías penales que actualmente están presentes en el código penal de la mayoría de los países legales como lo injuria o la difamación, sin embargo, ¿cómo se puede hablar a ciencia cierta de pornografía infantil en este caso? ¿son proporcionales condenas

tan pequeñas para un hecho tan dañino? En este escenario no sólo se afecta al menor, sino también a su familia y a todo su entorno. Este supuesto deja en claro que realmente, en la práctica la aplicación de estos principios no siempre es entendida como se debe, dejando un gran margen de situaciones en donde se vulneran, siendo esta la principal dificultad de los marcos éticos sin una fuerza vinculante para los desarrolladores.

Debido al gran estallido de estas herramientas en el sector del entretenimiento para adultos, ya no se hablan de casos aislados o como novedades, sino de algo bastante común en los entornos pornográficos, pero los Estados están notando el cuestionable impacto negativo y de mal gusto que tienen estas aplicaciones sobre los ciudadanos, país como Reino Unido (BBC News, 2024) y Bélgica (Sahuquillo, 2024) ya están tipificando esta práctica y la están reconociendo como un delito y es posible rastrear algunas personas que han sido consideradas culpables de la comisión de estos delitos, como es el caso de Hugh Nelson , en donde el sujeto usaba fotos de menores de edad dentro de aplicaciones pornográficas *deep fake* y fue condenado a 18 años de prisión (Al-Othman, 2024).

Síntesis

Para la elaboración de un marco ético eficiente se requiere de una perspectiva global y contemporánea del tipo de problemática que se está analizando, en este caso, cada uno de los principios aquí contenidos dan muestra

de la necesidad que se tiene para realizar una regulación fija que pueda impedir la causación de daños o el límite a las aplicaciones IA. Lo cierto es que este marco, recoge las necesidades de la sociedad contemporánea, actualmente el acceso a nuestros datos personales es sumamente importante, ya que con estos damos cualquier tipo de información que, dependiendo de la entidad a la que se le otorgaron podrían contener desde claves de tarjetas de crédito o información de correo electrónico que contengan datos bancarios.

La estructuración de este marco recoge a grandes rasgos la mayoría de los problemas de alto impacto que se podrían encontrar en de forma inmediata, dando nociones claras y precisas de cómo realizar aparatos jurídicos competentes y revestidos de gran fuerza. En el presente ya la mayoría de las legislaciones están en la búsqueda de incorporación de leyes y normatividad que pueda analizar estos problemas y toman como base la mayoría de estos principios o criterios éticos para desarrollar su legislación, pero es claro que hay una jerarquía de principios, unos más importantes que otros; los cuales son: Principios de promoción de los valores humanos, principio de equidad y principio de seguridad, de este triunvirato de principios, fácilmente se podrían extraer la mayoría de otros principios, a su vez que un aparato jurídico completo.

Al menos en la inmediatez, la idea de trasgresión de los derechos humanos por una IA es demasiado compleja, pero no es algo que sea imposible dentro de

algunos años, es muy probable que a medida de que los estudios, análisis y la práctica relacionada con la creación y calibración de estas herramientas escale a tal punto que tengan distintos grados de autonomía, no sólo para la toma de decisiones para la realización de alguna tarea en específico, sino también, tener algún grado de autonomía para realizar actividades humanas que le otorguen algún grado de protector de los bienes jurídicos de los seres humanos.

En nuestro tiempo, podría existir un sistema de detección de escritura que reconozca las palabras mal sonantes o que hablen mal de algún tipo de gobierno y elimine o notifique a las autoridades de que es lo que se publicó y quién lo publicó, infringiendo así el derecho a la libertad de expresión, esto, aunque pueda considerarse sacado de una novela distopía, es algo que ya se está viviendo en China por ejemplo, realiza este tipo de persecuciones inquisitivas a personas que tengan una perspectiva distinta a la de su régimen, realizan análisis de datos usando personal humano, pero en unos años esta labor es probable que se la otorguen a alguna IA.

El tema, por ejemplo, con los sistemas guía de misiles podría entrar en esa categoría, es evidente el objetivo que tiene un misil, impactar en alguna zona y causar el mayor daño posible, esto es una violación directa al pilar de los derechos humanos que es la vida, cómo estos hay cientos de ejemplos más que se evidencian. El principio de seguridad, por su parte; tiene un componente de que, en

sentido estricto, al menos la gran mayoría de las empresas cumplen con su responsabilidad de ser salvaguarda de los datos en ellos contenidos, sin embargo; existen algunos ejemplos de empresas que usan la recolección de datos como monedas de cambio, el usuario paga con sus datos o en algunas ocasiones es el sistema mismo que puede comprar la información para entregársela a algún comprador, entonces, ¿realmente cuál es el objetivo? ¿Impedir la propagación del contenido? O ¿solamente entregarles esta información si pagan por ella?

Por otro lado, se encuentra el principio de equidad, este es importante en la medida de la capacidad y el objetivo que tenga la IA. La imparcialidad es necesaria para realizar una aplicación IA, teniendo en cuenta su capacidad de adaptarse, de aprender y mejorar, esto podría incorporar problemas para la aplicación dependiendo del tipo de aplicación que sea, no tiene el mismo impacto una aplicación que ayuda con la sistematización de documentos a una que es herramienta para juicios, aquí radica la principal crítica, la imparcialidad solo es necesaria dependiendo del tipo de aplicación, no tiene que ser absoluto.

En la implementación o incorporación de datos suministrados a una IA, en teoría no podría haber parcialidad, siempre y cuando se ingresen todos los datos exigidos para el funcionamiento de la aplicación, otro escenario completamente distinto es que se escondan intencionalmente datos para arrojar un determinado resultado, ahora algo completamente distinto es que se realice el entrenamiento con

la información ya comprendida y que de forma arbitraria esto corresponda a opinión de terceros externos a un sesgo o parcialización hecho adrede, está como ejemplo la aplicación COMPASS (Mattu, 2023) en donde algunos afirmaban que esta aplicación tenía un componente racista ya que aumentaba las posibilidades de reinserción carcelaria a jóvenes afrodescendientes o que vivieran en barrios con un gran afluente de afrodescendientes, esto podrá sonar controversial, pero existe una alta capacidad de reinserción. Loury, (s.f.), en su artículo: "*Los nuevos intocables: crimen, castigo y raza en los Estados Unidos"* da una noción del grave problema que se tiene para poder realizar un informe objetivo sobre este tema, si un joven afrodescendiente de cada nueve puede ir a la cárcel, en contra posición de tres de cada doscientos caucásicos se nota una diferencia abismal entre las opciones. Es claro que al momento de interpretar la información para subirla a la IA se deben de hacer valoraciones y estudios, pero hacer eso significaría realizar un sesgo. En sí mismo el problema de la equidad al momento de ingresar la información en la IA es realmente pensar si se puede realizar una valoración o no y hasta qué punto esa valoración significaría caer en el prejuicio, porque está claro que la información arrojada sin ningún tipo de filtro y análisis genera más problemas que soluciones, o al menos al momento de realizar este juicio.

Capitulo IV. Propuesta de aplicación de principios éticos dentro de la IA

Modelos de regulación

A lo largo de este trabajo se ha mencionado la falta de normatividad sobre la IA. Existen varios puntos importantes que logran explicar esta falta de legislación, ya sea por lo novedoso del tema, la falta de previsibilidad por parte de los estados, la carrera entre los hechos y el derecho y el extremo formalismo y falta de adaptación que tiene el aparato legislativo en los estados. Sin embargo, hay algunos marcos legislativos a nivel mundial que sirven para fijar una especie de rumbo ante este borroso panorama, el cuál podría usarse como punto de partida para los otros estados y así poder fijar legislaciones robustas que puedan dar solución a estas problemáticas jurídicos. Cada una de estas normas tendrán en mayor o menor medida una base en los marcos éticos previamente analizados, adaptándolos como normas de obligatorio cumplimiento. Algunos de estos tratados normativos tienen como principio una clara preocupación sobre el horizonte económico de sus territorios, sin embargo, hablando en sentido estricto, suelen ser más barreras de protección para los consumidores y políticas anti monopolio, tal y como se podrá observar en las regulaciones creadas por el bloque regional de la Unión europea o en algunas de las analizadas en países específicos, tales como Estados Unidos, empero, teniendo leyes que propiamente hablan de temas y disputas originadas por entornos digitales, sin tener como principal fin la contención de daños de las

inteligencias artificiales, pero siendo fácilmente aplicables para las situaciones que se relacionen con IA, España por el desarrollo de marcos jurídicos y éticos, adaptados de las pautas de la Unión Europea, y por tratarse como patrón de referencia para el régimen normativito por parte de Colombia

Unión Europea

Europa es por mucho uno de los más grandes exponentes de legislación en cuanto a temas digitales, existen tres reglamentos relevantes para el caso: Reglamento de servicios Digitales (Comisión Europea, 2022) Reglamento de mercados digitales (Comisión Europea, 2022) y reglamento de las inteligencias artificiales (Comisión Europea, 2021). Adicional a lo anterior, también es importante destacar el Libro Blanco sobre la inteligencia artificial - un enfoque europeo orientado a la excelencia y la confianza. Cada uno de estos reglamentos tiene un objetivo específico y en principio, surgen como respuesta a las necesidades inexploradas de regulación referentes a entornos digitales.

- **Reglamento de Servicios Digitales**

Este apartado normativo tiene como principal fin el de regular el espacio en internet, es decir; otorgar seguridad a los usuarios y asegurar la protección de sus derechos fundamentales dentro del entorno digital (Consejo de la Unión Europea s.f.). Básicamente, trataba de impedir el tratamiento y distribución de material ilícito como la pornografía ilegal, *cyber bullying,* violencia, ciber acoso, entre otros delitos informáticos. Este reglamento tiene especial importancia, ya que es el que vigila a las redes sociales, así como en el comercio electrónico, sin embargo, en los siguientes apartados se abordará un reglamento que tendrá esto como principal fin. Este apartado es relativamente nuevo y se adoptó el 4 de octubre de 2022 y entró en vigor el 9 de noviembre del mismo año, aunque; su método de aplicación era parcial, su aplicación total empezó a regir desde el 14 de febrero del año 2024.

La ley define a los servicios de redes sociales o de mercados online como servicios intermediarios. Estos servicios funcionan a través del tratamiento de datos personales y de la aceptación de los términos y condiciones, de modo tal que este marco normativo define el cómo debe de ser este tratamiento de datos. El principal objetivo de este reglamento es el de brindar seguridad jurídica sobre la difusión de los datos y su protección, definiendo el marco de responsabilidad al que se enfrentan los vendedores online, así como el deber de protección y vigilancia que tienen las redes sociales.

Puntos importantes de este reglamento:

1. Permitió la regulación de la venta masiva a través del *drop shipping*, este tipo de ventas se popularizó bastante gracias a los grandes mayoristas como Amazon y su esquema de negocio es bastante amigable con el vendedor ya que este no necesita tener los artículos en su tienda o en su bodega, el cliente realiza la orden y esta orden se despachará a través del proveedor, de modo que el vendedor en este caso es un simple intermediario. Esto facilita la capacidad de envío, ya que abarata costos por cercanía, además de ser una excelente forma de ingresos para el vendedor ya que en sí mismo este no dispone nunca del producto, sencillamente lo compra de un tercero y realiza el envío al comprador.

2. Fijo las reglas para la creación de perfiles en las redes sociales, así como la información contenida en ella, impidiendo la publicación y difusión de material pornográfico ilegal, esto va desde la falta de consentimiento de la difusión hasta la pornografía infantil, el ciber acoso y *cyber bullying*.

- **Reglamento de Mercados Digitales**

El principal objetivo de la Ley de Mercados Digitales es el de garantizar la libre competencia de mercado. Así pues, define su aplicación a las plataformas gigantes

que se consideran “guardianas de acceso” (EUR-Lex, 2022) fijando un marco regulatorio por el cual grandes compañías como por ejemplo Google. Estas compañías, además de tener un increíble poder adquisitivo, gozan también de un gran poder mediático e informativo, lo cual provoca un impacto sumamente relevante dentro del territorio europeo. La ley, menciona que existen empresas que dependen en gran medida de estas “guardianas de acceso” tanto como para ofrecer sus servicios (EUR-Lex, 2022). De igual manera. esta ley permite que pequeñas compañías emergentes puedan competir contra estas “guardianas de acceso”, según la ley (EUR-Lex, 2022) existe una notoria diferencia de poder entre las empresas pequeñas o emergentes contra estas guardianas, por lo tanto, podrían encontrarse ciertas características abusivas por parte de las guardianas de acceso.

El criterio de delimitación para ser considerado guardián de acceso es algo extremadamente difícil de replicar, ya que requiere de un alto volumen de usuarios y ventas, en dónde las plataformas de ventas necesitan de un volumen de ventas igual o superior a 7.500 millones de euros dentro de la Unión Europea y 45 millones de usuarios al mes y de una capitalización de mercado de al menos 75.000 millones de euros, este requisito es inalcanzable para la mayoría de los sitios web de ventas o las redes sociales emergentes y es por esto mismo, en virtud de la protección de los usuarios y de las pequeñas compañías que brindan servicios de redes sociales. Además de las regulaciones que se puedan presentar dentro de los mercados digitales, también se revisaron puntos como publicidad en línea, sistemas o

servicios de mensajería y en general, servicios normales que puedan brindar las grandes empresas de compra y venta online (EUR-Lex, 2022).

Esta ley fue diseñada durante el mismo momento que la regulación de servicios digitales y comprende lo que se denomina Ley digital europea. Algunas empresas que serán objetivo de esta ley son: Google, Amazon, Meta, Apple y Microsoft. Lo relevante de esta ley es que permitirá una libre competencia tal y como se había mencionado previamente, reduciendo la predilección de estas compañías para promocionar o mostrar sus propios servicios antes que los de la competencia. La compañía Amazon, usaba datos de terceros para poder competir contra ellos, demostrando un evidente ánimo de acaparar el mercado y destruir a los emprendimientos rivales que usaban a Amazon como un puente con los clientes, este comportamiento con intención de monopolizar el mercado encendió las alarmas de la Unión Europea (García, 2020)

A pesar de los esfuerzos de la unión europea para fijar unos lineamientos que permitan tener un tránsito seguro en ambientes digitales, la legislación básicamente trata de proteger a los usuarios y pequeñas compañías, sin embargo, no queda claro la posición de los usuarios frente a fallas por errores dentro de las aplicaciones ya que estos reglamentos tienen como principal fin la protección al consumidor, protección de datos y protección. Dentro de la regulación de Servicios Digitales se fijó la responsabilidad por parte de las compañías y trazó cierta seguridad jurídica para sus usuarios, sin embargo, esta responsabilidad es más sobre el contenido y

prácticas de las compañías y no de cómo se comportan los errores o las problemáticas causadas por sus aplicaciones con sus clientes.

- **Reglamento de inteligencias artificiales**

Debido al alto grado de complejidad y el amplio rango de valores y capacidades que podrían tener las inteligencias artificiales, sumado a su increíble masificación, era de esperarse que el parlamento europeo tratara de fijar ciertos lineamientos para poder prevenir las problemáticas jurídicas, así como para fijar un marco en el cual estas aplicaciones pudieran desarrollarse de la forma más optima posible, protegiendo así los intereses de los usuarios y consumidores, además de sus derechos fundamentales, sin embargo, este reglamento genera varias zonas grises dentro de su ley, ya que este reglamento no será aplicable a autoridades públicas, países ajenos a la unión u organizaciones de internacionales, siempre que estas desempeñen un rol de aplicación policial.

Esta excepción a la aplicación podría desencadenar un sinfín de problemas jurídicos y violaciones a varios derechos fundamentales. A diferencia de los anteriores reglamentos, esta ley si contempla la posibilidad de los errores de operatividad, pero este análisis solamente se aborda de forma superficial y no logra definir los temas de responsabilidad aplicable para los desarrolladores,

fungiendo meramente como deberes abstractos de realización técnica y como abstención de realización de errores, sesgos o fallos que se podrían presentar. Esta normativa podría ser un excelente punto de partida para poder crear un sistema de protección para los usuarios, algo que tenga mucho más peso y no sea meramente un sistema de derecho blando, permitiendo configurar un marco de normatividad robusto que sea más eficiente.

Los artículos 5, parágrafos 40 y 44, y 10 en su parágrafo 3 y 15, en su tercer parágrafo mencionan la posibilidad y la evitación de errores dentro del desarrollo y entrenamiento de las inteligencias artificiales. Lo realmente valioso de esta ley es que permite realizar distinciones dentro de las inteligenciar artificiales, definiéndolas como IA de alto riesgo, esta lista es taxativa, centrándose en las que tienen la capacidad de repercutir negativamente en riesgos a la salud, seguridad, derechos fundamentales e integridad. Sin embargo, esta lista solo contempla la posibilidad de realización de menos cabo para personas físicas y realmente no contempla la posibilidad de las responsabilidades que se pueden generar a personas jurídicas. Todo lo relevante a la discusión sobre los sistemas de alto riesgo está comprendido en el capítulo tercero de este reglamento.

Adicional a los reglamentos anteriores, es importante incluir “el libro blanco sobre la inteligencia artificia”, documento también realizado por la unión europea cuyo énfasis se enmarca en la necesidad de reforzar las capacidades

industriales y tecnológicas que impulse el crecimiento de las capacidades y talento mediante la adopción de la IA en el mercado de manera ética y fiable

Libro Blanco

El propósito de esta política es actuar no como un reglamento sino como guía frente a la necesidad moderna de los países europeos de reforzar sus capacidades industriales y tecnológicas mediante la adopción de II. AA en el mercado de manera ética y confiable. Así pues, el Libro Blanco expone el potencial desarrollo e implementación de la IA para su uso en múltiples sectores sociales, tales como la agricultura, industria y salud. No obstante, es consciente de los riesgos asociados frente al uso de la IA, dado a que esta se encuentra moldeada por humanos los cuales, ya sea de forma consciente o inconsciente, impregnan sus pensamientos; doctrinas, errores y censuras que llegan a repercutir en los usuarios de dichas II. AA, además de estar obteniendo datos, sensibles o no, de los mismos usuarios, volviendo a retomar el tema de la transparencia respecto a la toma de decisiones y la privacidad.

Es por ello que el Libro Blanco propone que el desarrollo y regulación de la IA sea mediante una estrategia de inversión conjunta entre sectores públicos y privados para fomentar de dicha forma un ecosistema innovador, flexible en su medida, y confiable. Pero, por encima de tomo, exhibe la necesidad de que las

II. AA se encuentren sujetas a los estándares éticos globales definidos por los derechos humanos.

Así pues, el Libro Blanco sugiere siete requisitos esenciales para el desarrollo de la IA en aras de fomentar confianza entre los consumidores y las empresas: Solidez técnica y seguridad; buscando que la IA se encuentre bajo control humano, Gestión de privacidad y protección de dato; garantizando la privacidad y de seguridad de los datos personales, Transparencia; respecto al funcionamiento de los algoritmos, Diversidad, no discriminación y equidad; esto relacionado con la transparencia pero con el énfasis de evitar que en dichos algoritmos se encuentren sesgos discriminatorios, Bienestar social y medioambiental; por cuanto el propósito de la IA debe siempre de propender por impactos positivos en la sociedad y finalmente la Rendición de cuentas en donde se debe de definir las responsabilidades claras en caso de errores y daños provocados por la IA a causa de mala decisiones.

España

Teniendo en consideración los lineamientos realizados por la Unión Europea, destacando los compromisos de la agenda digital para Europa (entre otros), España ha respondido a dicho compromiso mediante la elaboración de su proyecto “Agenda España Digital 2025”, mediante el cual ha sido destacada por

sus avances respecto a la estructuración normativa de la nueva era digital. De dicha agenda se destacará para la presente investigación uno de sus ejes, siendo este el “ENIA” (Estructuración Nacional de Inteligencia Artificial). En dicho proyecto, el gobierno de España pretende reconocer el panorama actual del uso de II. AA en cuanto su aplicación en términos locales para así realizar una estrategia de implementación y consolidación del uso de la II. AA en el ecosistema laboral español, creando de dicha manera un marco de referencia e impulso para los sectores públicos y privados frente al uso de esta tecnología.

Así pues, dentro del documento de la ENIA (citación) se establecen 6 ejes estratégicos. Pero para la presente investigación nos centraremos en el sexto eje ya que este se centra en el establecimiento de un marco ético y normativo que refuerce la protección de los derechos individuales y colectivos.

Dicho lo anterior, el sexto eje busca articular y desarrollar los servicios tecnológicos en donde hay incidencia de la IA desde tres ámbitos clave:

- **Jurídico**. En el que deben protegerse derechos fundamentales que ya son reconocidos, identificarse reformas legales necesarias, así como lagunas jurídicas que requieran regulación adicional.
- **Socio-tecnológico**. Creando una serie de metodologías, estándares y procesos con los que desarrollar servicios automatizados.

- **Ético**. Que es fundamental para asegurar que el uso de la IA acompañe los valores de la sociedad y opere en beneficio de la inclusión y el bienestar. (Gobierno de España, 2020, p. 65).

En términos de marco normativo, la ENIA se acoge a la legislación específica de Inteligencia Artificial presentada ante la Unión Europea, destacando entre ellos el “libro Blanco sobre Inteligencia Artificial, poniendo como énfasis el respeto a los derechos fundamentales, privacidad y no discriminación.

De igual manera, frente a la necesidad de tener sistemas trasparentes y auditables, la ENIA establece un catálogo de medidas para poner el practica los principios éticos para el desarrollo de “sistemas justos de IA”. Dicho catalogo responde a 3 pilares claves:

- Supervisión humana. La IA debe estar sometida a supervisión continua, y debe ser comprensible para las personas.
- Gobierno de los datos y sistemas. Los datos no se utilizarán para perjudicar a la sociedad, o violar los derechos fundamentales de los ciudadanos. Los datos tienen tanto un aspecto personal, como un carácter de bien público. Las normas éticas y jurídicas con las que establecer el equilibrio democrático entre ambas deberán ser profundizadas tanto en el comité ético de la IA como en la revisión y reforma legal pertinentes.

- Transparencia (trazabilidad). Se debe garantizar la trazabilidad de los sistemas de IA. Esto significa garantizar que las decisiones ejecutadas por sistemas algorítmicos puedan ser auditadas, evaluadas y explicadas por las personas responsables. (Gobierno de España, 2020, p. 67)

Finalmente, para el desarrollo de un marco ético es necesario que las medidas a implementar se encuentren regidas bajo una esfera de principios éticos. Así pues, la ENIA destaca 3 principios para su desarrollo:

- Inclusión. No discriminación. Los sistemas de AI deben considerar toda la gama de habilidades y requisitos humanos, y garantizar la accesibilidad.
- Bienestar social. La IA debe contribuir al bien común, apoyando el bienestar y los derechos fundamentales de los seres humanos, y no disminuir, limitar o desviar la autonomía de estos.
- Sostenibilidad. Los sistemas de IA deben utilizarse para mejorar la sostenibilidad y la responsabilidad ecológica (Gobierno de España, 2020, p. 68)

Por último, la ENIA establece la necesidad de la participación directa de la ciudadanía en aras de lograr una verdadera garantía a la protección de los derechos. Dicha participación se realizaría mediante foros de dialogo entre gobierno, sector privado y sociedad civil cuyo énfasis seria la promoción de un debate que abarca múltiples áreas del saber (ciencia, filosofía, ética y derecho)

manteniendo la preponderancia de dimensión humanista y practica en los procesos de innovación tecnológica de creación de II. AA, garantizando la inclusión y pluralidad de opiniones entre los ciudadanos, empresas privadas, entidades públicas y el Estado mismo en aras de promocionar un sistema que se ajuste en la mejor medida a la promoción del desarrollo y la protección de los derechos y valores colectivos.

Estados Unidos

Al igual que en la Unión Europea, Estados Unidos utiliza un sistema jurídico de estructura similar a los reglamentos europeos. Las regulaciones norteamericanas tienen como fin principal la protección de datos de sus usuarios, control y vigilancia de redes sociales y sobre las inteligencias artificiales. Esta regulación es también una de las más analizadas en los compendios de investigaciones sobre el tema y partió del Marco Ético creado por la universidad de Harvard (2020).

Este país ha realizado una notable labor legislativa sobre esta materia, teniendo en muy corto tiempo más de seis regulaciones sobre el tema, teniendo muchos puntos similares con la regulación europea, pero a diferencia de la unión europea, tiene además de los propósitos regulatorios para poder solucionar

problemas derivados a las inteligencias artificiales y las contingencias que pueden surgir a partir de esos dilemas; trata de glorificar y enaltecer la supremacía americana en esta nueva rama de la tecnología, invitando a la inversión y desarrollo de estas herramientas para poder seguir ostentando el puesto de liderazgo sobre la creación y desarrollo de inteligencias artificiales. Las regulaciones norteamericanas son bastante extensas, pero en esta investigación solo se abordarán cuatro de estas leyes, las cuales son: *Executive order on maintaining american leadership in Artificial Intelligence, National artificial intelligence initiative Act (2020), Federal trade commission (FTC), Ethical Principles for Artificial Intelligence and Autonomous Systems (Department of Defense)*

Los esfuerzos del país norteamericano para legislar sobre esta materia empezaron desde 2019 con la *Executive order on maintaining american leadership in artificial intelligence*, el cual es un compendio normativo que busca promover la investigación, uso, destinación de fondos, la potenciación de la fuerza laboral sobre el uso de estas herramientas y lo más novedoso de esta ley, es la pretensión estadounidense de seguir estando en el pináculo del conocimiento y el desarrollo sobre la creación de inteligencias artificiales. Esta pretensión se encuentra dentro del artículo 1 y el artículo 2.8, el primero enuncia la pretensión y plantea la necesidad del país sobre seguir liderando el desarrollo de estas herramientas y el 2.8 exige la creación de un plan de acción para que

el primer artículo se pueda cumplir, pero lo realmente relevante dentro de ley es la creación de incentivos que permitan a estudiantes, profesores o trabajadores acceder a becas o programas educativos para poder ser entrenados para poder concebir estas aplicaciones, siendo una iniciativa que no se ha visto replicada en otras partes del mundo. Esta ley, es fundamentalmente, una declaración de apoyo, gestión e incentivar la investigación y creación de estas aplicaciones. Es importante mencionar, que si bien, esto en sentido estricto tiene forma de orden ejecutiva, es también una ley, en dónde se obliga a legislar al respecto de las anteriores consideraciones, es por esto que, a partir del acta nacional de Inteligencia Artificial, se logra cumplir con los objetivos de esta orden.

La ley nacional de inteligencia artificial es por mucho la más grande producción legislativa en materia de investigación y desarrollo que posee el país norteamericano. Consta de cinco títulos, los cuales constan de: Iniciativa sobre la inteligencia Artificial (algo que es similar a la anterior ley estudiada) Institutos nacionales de investigación sobre la Inteligencia Artificial, Actividades del instituto nacional de normas y tecnología relacionado con las inteligencias artificiales, Actividades de Inteligencia Artificial de la fundación nacional de ciencias y el programa de investigación de Inteligencia Artificial del departamento de energía. Esta acta, es fundamentalmente una ley marco, la cual trata de cumplir con las obligaciones impuestas por la orden ejecutiva.

El tercer apartado del cual es importante mencionar en la presente investigación será la sobre la guía realizada por realizada por la Comisión federal de comercio (FTC por sus siglas en inglés), en la cual se recopila un puñado de principios que estaban incorporados en distintos marcos éticos, tratando de enfatizar en el uso responsable y ético sobre las inteligencias artificiales. Esta guía fue publicada en febrero del 2024, siendo una de las más recientes, sin embargo; esta guía solo es una acentuación de los distintos desarrollos doctrinales sobre el apartado ético y de uso de las inteligencias artificiales, siendo sólo una aclaración por medios legales de estos marcos.

La FTC es un organismo gubernamental que ha tratado de velar por la protección de los intereses de consumidores y de usuarios en Norteamérica y ha demandado a empresas traten de cambiar o ajustarse de forma negativa a las exigencias legales y marcos éticos creados por los distintos órganos y doctrinantes, tratando de esta forma, proteger el derecho de los consumidores sobre la sana competencia y obligando a las compañías a seguir los lineamientos obligatorios para sus términos en el servicio. Este marco a pesar de tener una estructura de marco ético, que en principio se podría considerar que no tiene carácter de norma imperativa, la FTC lo usa como un método coercitivo y su violación genera repercusiones legales y económicas, por lo tanto, se puede concluir que es de obligatorio cumplimiento y, por tanto, tiene estructura normativa (Crowell & Moring, 2024)

Los esfuerzos realizados por los aparatos gubernamentales estadounidenses son masivos y bien direccionados, dando un buen panorama del cómo realizar estas intervenciones normativas por parte del poder legislativo, contando también con una fuerte intervención por el sector defensa del país, siendo el departamento de defensa el creador de *Ethical Principles for Artificial Intelligence and Autonomous Systems,* otro nombre que se le da es el de *DOD Ethical principles IA* (por sus siglas en inglés, principios éticos del departamento de defensa), que si bien, al igual que el apartado anterior, podría considerarse meramente como un marco ético, también genera implicaciones legales y es fuente coercitiva, siendo algo más que un puñado de directrices que no cumplen el carácter de norma.

El organismo que tiene como función proteger estos principios es la jefatura de inteligencia digital y artificial (CDAO) la cual cumple cinco funciones principales: Liderar y supervisar el desarrollo de estrategias y creación de políticas del Departamento de defensa de datos, análisis e Inteligencia Artificial, Trabajar para derribar barreras a la adopción de datos de las inteligencias artificiales dentro de los procesos institucionales en el Departamento de defensa, crea infraestructura y servicios digitales habilitantes que respalden el desarrollo y la implementación de datos, análisis sobre la Inteligencia Artificial y soluciones digitales y la selección de soluciones digitales probadas y habilitadas para las IA para el uso empresarial (CDAO, s.f). Estos objetivos, son alcanzados gracias al

DOD IA. Este marco ético comparte una gran semejanza con los principios mencionados en el anterior capitulo, pero sólo aborda cinco principios: Responsabilidad, equidad, rastreabilidad, fiabilidad y gobernanza, excluyendo otros principios que son vitales como el de preservación de los derechos humanos, transparencia y protección.

Es claro que los intentos americanos de crear legislación sobre el tema están más dirigidos a incentivar, protocolizar y producir nuevas inteligencias artificiales para mantener su puesto como principales generadores de estas herramientas y estar a la vanguardia de la tecnología, sin embargo, a pesar de que sus marcos normativos puedan tener carácter vinculante y ser un símil de ley, hay algunos puntos que se dejan a la interpretación o que sencillamente, se debe de acudir a otras ramas para poder realizar el estudio del caso pertinente. Están invirtiendo todo su esfuerzo en publicitar y fomentar la creación, pero su regulación, aunque basta, en algunos puntos es redundante y no logra llenar todos los vacíos legales que se puedan originar como resultado de los dilemas o las relaciones jurídicos que se puedan presentar.

Colombia.

En Colombia los la regulación es más limitada en comparación con la normativa europea. Hay varios puntos de vista que podrían explicar esta

situación: las dificultades que experimentan los ciudadanos para poder acceder a estas herramientas, por lo que, en un pasado no muy lejano, estas problemáticas no representaban en sí mismas un problema inmediato para analizarse, la falta de adaptación de la que ha gozado el sistema jurídico colombiano, tal y como se puede contrastar en temas como la adopción homosexual, matrimonio igualitario y otras problemáticas en donde se ha evidenciado un evidente tradicionalismo por parte de las altas cortes y por el poder legislativo colombiano y una enorme falta de previsibilidad de impacto, al no evaluar de forma correcta las posibles consecuencias al dejar al azar los temas concernientes a las regulaciones digitales y de IA.

Actualmente se están desarrollando algunos proyectos de ley que buscan regular disposiciones concernientes a las inteligencias artificiales, sin embargo, el sistema jurídico colombiano aún no ha implementado casos de contingencia para consecuencias causadas por errores de programación o de inteligencias artificiales, por lo que aún se espera una pronta solución a este enorme vacío normativo.

Se podría recurrir, por medio de analogías a otras leyes que busquen proteger el tratamiento de datos personales o sensibles, la ley 1581 del 2012 podría funcionar como una excelente forma para fijar directrices que puedan beneficiar a los usuarios del entorno digital y en algunos casos, es posible realizar la aplicación de esta ley, sin embargo, propiamente hablando, aún no

existe ningún aparato legislativo que funcione como un medio de control o una barrera que pueda otorgarle protección y seguridad jurídica a los usuarios digitales. Uno de los primeros acercamientos de algún esquema legal en Colombia sobre esta materia fue durante el 2020, con la creación de un marco ético sobre la IA, siendo un compendio que recogía distintos a portes que ya se habían analizado en otros estudios alrededor del mundo, sin embargo, el problema principal con estos marcos éticos es que son una fuente eficiente de creación normativa, no obstante, carecen de poder vinculante al no tratarse de normas imperativas. Guío (2020) en su documento trata de recopilar los principios más importantes, básicamente todos los que se mencionaron en el capítulo anterior de esta investigación, el problema con esta recopilación es que el órgano legislativo colombiano no ha tenido mucho interés en darle un uso a ese marco ético y a pesar de que ya casi se cumple un lustro de su publicación.

El poder ejecutivo ha tratado de manifestar su preocupación sobre este tema, existiendo algunas intervenciones por parte del actual presidente Gustavo Petro y su gabinete, realizando una Hoja de ruta para el desarrollo y la aplicación de la inteligencia artificial en Colombia, a cargo del Ministerio de Ciencia, Tecnología e Innovación publicada a penas durante el año 2024. El objetivo de esta Hoja de ruta es la de la planeación, incorporación y adopción de esquemas regulatorios, definición de alcance de las políticas relativas a las inteligencias artificiales y su plan de acción, siempre velando por la adopción ética de las IA.

Adopción de las IA

Este es un proceso de aceptación e implementación de estas herramientas en virtud de mejorar la calidad de vida de los colombianos, así como la mejora en la prestación de servicios por parte del gobierno, al momento de análisis de datos, su seguridad y accesibilidad. Por parte de los colombianos, esta adopción es un gran alivio para las empresas como también para los ciudadanos, permitiéndoles mejorar su eficiencia en el trabajo.

Ética en la IA

A pesar de que en el capítulo anterior se abordó este tema, la Hoja de Ruta trata no sólo de fijar y esclarecer el porqué de la importancia de una implementación ética dentro de la programación y utilización de las inteligencias artificiales. La ética funge como un dique de contención necesario para la salvaguarda de los usuarios y fijar límites al alcance que tendrán estas herramientas. El entrenamiento y capacitación de las IA requieren de experimentación y de inserción de datos, es en este punto en donde la importancia de la seguridad y la intimidad de los usuarios es una preocupación real, con la existencia de prácticas como Big data, el acceso y uso de los datos de los usuarios como una especie de moneda transaccional para alimentar y

entrenar a estas herramientas con fines comerciales fijan nuevos problemas que antiguamente dentro de nuestra regulación no se habían contemplado, obligando a la adopción de medidas por parte de los órganos estatales, será entonces necesario, establecer medidas que permitan el entendimiento eficiente por parte de los usuarios con independencia a su nivel, tanto de escolaridad como de capacidades, para que estén enterados en todo momento de cómo serán usados sus datos y con que propósito.

Existen tres puntos importantes dentro de esta regulación que tratan de fijar medidas de seguridad y protección a los usuarios de IA relativo al uso de sus datos, los cuales son: Respeto de las personas, beneficencia y justicia.

- Respeto de las personas: la creación de una inteligencia artificial deberá de estar supeditada al dominio y control del ser humano, otorgándole siempre autonomía y capacidad de elección a los usuarios a través del consentimiento informado. Es posible que existan usuarios que requieran del uso de estas herramientas y tengan algún nivel de necesidades especiales que necesitan de una protección robusta debido a su autonomía disminuida con motivo de su condición, por lo que se deberá de explicar y dar a conocer al usuario, de la forma más optima posible de los posibles riesgos o los beneficios que pudieran obtener al usar estas herramientas, así como la capacidad de elección de participar o rechazar su uso.

- Beneficencia: Las IA no podrán lastimar, la implementación de los algoritmos deberá de ser siempre en pro del ser humano y no podrán tener la capacidad de dañar.

- Justicia: El uso de estas herramientas deberá de ser equitativo para que los usuarios no deban de ceder excesivamente sus beneficios en contraposición de lo otorgado por las investigaciones y desarrollos algorítmicos, esta deberá de ser proporcional a los servicios que se podrán obtener de estas herramientas.

A lo largo de esta Hoja de Ruta se agrupa nuevamente algunos de los principios éticos estudiados dentro del marco ético de Guío (2020), sin embargo, realiza un enfoque importante en la sostenibilidad de las inteligencias artificiales. La preocupación de una afectación por parte de las IA a diferentes esferas de la sociedad es algo más que hipotético y en esto radica la importancia de la sostenibilidad, tanto económica, social y ambiental.

Teniendo en cuenta el contexto anterior, el gobierno colombiano en febrero de 2025 expidió el documento CONPES 4144 siendo este la política nacional de inteligencia artificial. El propósito de este es el de proporcionar una mejor estructura nacional referente a la hoja de ruta para la estructuración, desarrollo y uso de la Inteligencia artificial, mediante diagnósticos y líneas de acción, para impulsar la transformación social y económica de Colombia. Así pues, el CONPES 4144 se

desarrolla principalmente torno a 6 ejes, siendo estos Ética y Gobernanza, Datos e Infraestructura, Investigación, Desarrollo e Innovación, Desarrollo de Capacidades y Talento Digital, Mitigación de Riesgos y Uso y Adopción de la IA; aunque de igual manera incluye dentro de su desarrollo políticas respecto a la equidad; inclusión y sostenibilidad ambiental, seguridad y confianza, propiedad intelectual y datos relacionados a la IA.

En el eje de Ética y Gobernanza, se destaca la adopción de Colombia a tratados internacionales tales como *la Recomendación del Consejo de la OCDE sobre inteligencia artificial*, para el establecimiento de cinco principios éticos para la gestión responsable de la IA, siendo estos los de crecimiento (i) Crecimiento inclusivo, desarrollo sostenible y bienestar; (ii) Valores centrados en el ser humano y equidad; (iii) Transparencia y explicabilidad; (iv) Robustez, seguridad y protección; y (v) Responsabilidad y políticas nacionales y cooperación internacional para una IA confiable humanos (Departamento Nacional de Planeación [DNP], 2025), encontrándose estos a su vez sujetos al principio general de protección de los derechos humanos todo esto sujeto al principio general centrado en la protección de los derechos, y la *Recomendación sobre la ética de la inteligencia artificial de la Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura (Unesco)*, integrando de dicha manera una serie de “valores y acciones en políticas públicas para fortalecer evaluaciones de impacto, mecanismos de gobernanza,

políticas éticas de datos, y promover un entorno propicio para la ética de la IA" (Departamento Nacional de Planeación [DNP], 2025)

Posterior a la sujeción por parte del Estado Colombiano a las recomendaciones, viene el primer intento de estructuración de un marco ético mediante la publicación de *Marco Ético Para La Inteligencia Artificial En Colombia* en 2021. Sin embargo, en este se desarrolló previo al crecimiento exponencial de los modelos y sistemas de la IA generativa no tampoco estableció de forma clara la implementación de los principios éticos en el ciclo de la vida, volviéndola insuficiente para realmente estructurar una implementación real de un marco ético a la sociedad colombiana (Departamento Nacional de Planeación [DNP], 2025), denotando de dicha manera que el país, a pesar de contar con suscripciones a tratados y sugerencias internacionales, además de elaboraciones propias de políticas de IA, sigue presentando un bajo nivel de desarrollo al ser "insuficientes las capacidades nacionales para verificar el cumplimiento de los principios éticos en las aplicaciones, sistemas y usos de la IA, ya sea de las recomendaciones y principios éticos acogidos, como de aquellos que puedan surgir durante la evolución de esta tecnología" (Departamento Nacional de Planeación [DNP], 2025)

A raíz de lo anterior, el CONPES 4144 estableció como línea de acción, entre otras, el fortalecimiento de los mecanismos de gobernanza y aplicación de principios éticos frente al uso de la IA, mediante el cual establece una coordinación entre el

DAPRE[5], Ministerio de Tecnologías de la Información y las Comunicaciones, el Ministerio de Ciencia, Tecnología e Innovación, y el DNP[6] para la formalización y ejecución de modelos de gobernanza alrededor de la IA, además de mecanismos de articulación para monitorear su impacto ético y alineación con la visión estratégica nacional y prácticas internacionales. Para ello, sugiere promocionarlo mediante la participación de todos los actores de la sociedad colombiana; incluyendo el sector público, privado y civil (Departamento Nacional de Planeación [DNP], 2025).

Síntesis

En este capítulo se pudo evidenciar el panorama internacional respecto a la regulación de las II. AA, encontrándose en una permanente evolución bajo dos ópticas: La regulación general, representada por la Unión Europea, y la regulación atómica, representada por Estados Unidos

Por un lado, la regulación general busca el establecimiento de un marco normativo integral y vinculante dentro de un sistema jurídico unificado. Dicho marco busca abarcar una mayor cantidad de regulación en todas las posibles áreas de

[5] Departamento Administrativo de la Presidencia
[6] Departamento Nacional de Planeación

injerencia de la IA mediante el establecimiento de un marco ético claro, estricto y universal.

Lo anterior se evidencia de tres maneras: mediante el establecimiento de regulaciones como el Reglamento de Servicios Digitales, el Reglamento de Mercados Digitales y el Reglamento de Inteligencias Artificiales, los cuales permiten la centralización del control sobre actividades digitales; a través de lineamientos como los reflejados por el Libro Blanco, mismo que, aun no siendo vinculantes, representan una serie de sugerencias que evocan una fuerza de obligatoriedad por su correlación con los reglamentos emitidos en materia de IA y por tratarse de un establecimiento del marco ético universal; y finalmente en su aplicación nacional, tomando como ejemplo a España, la cual ajusto su Estrategia Nacional de Inteligencia Artificial acorde a las políticas expedidas por la Unión Europea en materia de IA y ajusto sus estándares éticos basados en los expuestos por el Libro Blanco, buscando que en los desarrollos y aplicación de las II. AA en la cotidianidad siempre prime el respeto de los derechos fundamentales sobre el resto de los principios y/o acciones, además de fomentar la supervisión, la inclusión y la responsabilidad de los desarrolladores

Por otro lado, se encuentra el modelo de regulación atómica, defendido por los Estados Unidos, el no busca la creación de un modelo normativo de amplio margen vinculante, sino la promoción de la innovación tecnológica al encontrarse en un espacio sin restricciones estrictas; permitiendo que las empresas

desarrolladoras de II. AA tengan un margen amplio de autorregulación de su creación. Esto se realiza al fragmentar la regulación en múltiples normativas sectoriales dirigidas más hacia la creación lineamientos y no normativa vinculante. Un ejemplo de ello se toma a partir de leyes como la *National Artificial Intelligence Initiative Act* (2020) y guías emitidas por la Federal Trade Commission (FTC) y el Departamento de Defensa (DOD), las cuales, aunque establecen una normatividad respecto al uso de las II. AA, lo efectúan mediante un margen amplio y poco cohesivo, dependiendo de la interpretación y aplicación discrecional de cada entidad

Finalmente, en Colombia se encuentra poca regulación respecto al uso de la IA, sin embargo y acorde a los lineamientos presentados en la hoja de ruta, es factible determinar que en la nación se opta más por la regulación general en búsqueda de la creación de un marco legal y vinculante que permita establecer la predominancia del respeto a los derechos fundamentales y de los principios que consagraran el marco ético de la IA en Colombia.

Así pues, ambos modelos de regulación tienen como propósito el mantener el desarrollo de la IA y establecer pautas claras para los desarrolladores. No obstante, el modelo atómico presentado por Estados Unidos, aunque en principio brinda más libertad para su desarrollo, no termina por responder de forma adecuada a las problemáticas generadas por la IA dado a su misma esencia, la cual al ser fragmentada no solo evita la consagración de un marco ético general, sino que

establece diversos marcos éticos regidos por la discrecionalidad de su operador que pueden tener como consecuencia diversos problemas en cuanto a la seguridad jurídica y generación de aun más zonas grises de en materia de responsabilidad.

Capitulo V. Conclusión

La II. AA han dejado de ser materia de estudios hipotéticos con el paso del tiempo, su implementación ha sido cada vez más común y natural. Están presentes en más campos; desde las ocupaciones científicas, hasta en el ocio y en el día diario de las personas, teniendo la capacidad de aprender y adaptarse a su entorno, dotándolas de un talento extraordinario para adaptarse y desarrollarse, con algo de ayuda de sus usuarios y también de sus desarrolladores.

Existen dos formas en las que una IA pueda aprender. La primera es a través del *Machine Learning*, que necesita una base de datos establecida por sus desarrolladores, mientras que la segunda, el *Deep Learning*; que además de la base de datos, también aprende de su entorno y usuarios, permitiendo mejorar su ecosistema y entrenarse para satisfacer los deseos de estos. A pesar de que dichos sistemas computacionales sean en gran medida increíblemente precisos, tienen la capacidad de cometer errores y dependiendo del error en sí o de sus consecuencias tendrán su propia clasificación: los errores de sintaxis, los errores de diseño y los errores de mala praxis. Los errores de sintaxis son referidos a errores de escritura al momento de la redacción del código, estos pueden tener resultados inofensivos en sí mismos, pero pueden llegar a ser catastróficos. Los errores de diseño se

originan de una falta de planeación al momento de estructurar la IA y, por último, los errores de mala praxis necesitan de un dolo de sus creadores para que puedan existir. Cada uno de estos errores pueden llegar a ser mayor o menormente gravosos dependiendo de la razón y funcionamiento de la IA.

Ahora bien, las II. AA para poder ser aplicadas en la sociedad requieren del establecimiento estructural de un marco ético y normativo en torno a ellas. Así pues, para su desarrollo eficaz es necesario que dicha normatividad se encuentre sujeta a una serie de principios éticos capaces de moldear el marco legal de forma que la normatividad expuesta sea clara, aplicable y, en especial, tenga capacidad de mantenerse actualizada sin una constante intervención humana. En la publicación del Berkman Klein Center for Internet Society (2020) de la Universidad de Harvard se exponen siete principios rectores de la IA: “Privacidad; responsabilidad; seguridad y protección; transparencia y explicabilidad; equidad y no discriminación; control humano de la tecnología y responsabilidad profesional y promoción de los valores humanos” y resaltan la importancia de estos en el campo de aplicación de la IA.

En esta misma línea, en Colombia se han tenido en consideración los siete principios propuestos, pero a su vez se han realizado proposiciones para implementarlos y adaptarlos a la normatividad local mediante la estructuración de los siguientes principios: transparencia, explicación, privacidad, control humano de

las decisiones propias de un sistema de IA, seguridad, responsabilidad, no discriminación, inclusión prevalencia de los derechos de niños y adolescentes, beneficio social. Así pues, se denota que en la discusión se hace especial énfasis en la protección del menor en aras de fomentar una integración sana respecto a la enseñanza y manipulación de la IA para los menores y su especial protección en caso de que, mediante la IA, se intente vulnerar algún derecho de estos.

Estos principios han proporcionado una base para la estructuración de un marco ético propio para la IA, pero no han terminado por consolidarse de forma adecuada al sistema por falta de legislación y estructuración de un marco ético firme. La importancia de esta estructuración nacional no solo radica en la creación de normas sino en la consolidación de pilares para prevenir riegos de vulneración de derechos humanos. Dichos riesgos surgen de la aplicación de una IA sin control previo o posterior en cuanto normatividad, generando vacíos legales que pueden dejar sin protección a aquellos sujetos que se encuentran en estado de indefensión, tal como los menores de edad.

Finalmente, los modelos de la IA han sido desarrollados bajo parámetros acordes al lugar de creación careciendo de uniformidad en cuanto al régimen normativo aplicable, razón por la cual, en la actualidad, existen dos grandes modelos de regulación.

El primer modelo, impulsado por la Unión Europea se refiere a un amplio espectro de intervención por parte del Estado respecto al desarrollo de las II. AA, esto mediante la creación de un marco normativo amplio, ético, estricto, riguroso y universal. Dicho sistema se justifica en la predominancia de los Derechos Humanos, razón por la cual orbita bajo la esfera de “dignidad” y “no discriminación”. Sin embargo, este sistema requiere un amplio esquema de consenso; tanto en el Parlamento europeo como su adaptación al estado en sí, respecto a márgenes filosóficos ambiguos tales como la justicia o lo “éticamente correcto”, lo que conlleva a que el desarrollo de la IA encuentre innumerables obstáculos que entorpezcan su evolución.

El segundo modelo, impulsado por los Estados Unidos, a diferencia del propuesto por la Unión Europea, busca la promoción de la innovación tecnológica y, por tanto, de la predominancia del desarrollo de la IA sobre la regulación de esta, concediendo una mayor libertad a los desarrolladores para plantearse ellos mismos una regulación atómica o de normatividad sectorial. A pesar de lo anterior, dicho sistema propende a la discrecionalidad jurídica al no tener una base normativa general, lo cual puede evocar en que la instalación del marco ético de las II. AA. se realice a favor del esquema ético-moral de la desarrolladora y no necesariamente sujeta a los derechos humanos y con ello, volviéndose una herramienta propagandista y/o que vulnere derechos tales como la “no discriminación” o el principio de “dignidad humana”.

Así pues, mediante esta investigación se ha evidenciado a la IA como una herramienta en desarrollo con potencial de modificar la estructura actual de la sociedad. Sin embargo, su aplicación en el derecho sigue sin ser del todo clara; no por su funcionamiento sino por la carencia de medidas suficientes para establecer modelos claros, precisos, estructurados y, sobre todo, normativizados de IA para su uso masivo y amplio por parte de la sociedad y del Estado. Dicho lo anterior, en Colombia, tal como se mencionó en el capítulo primero, ya se ha implementado IA para diversas ramas del Estado, como lo son Prometea y PretorIA para la rama judicial, o Fiscal Watson por parte de la fiscalía. Pero estas II. AA. tienen tres problemas: su alcance, la responsabilidad y la falta de una normatividad clara y un marco ético estable.

Respecto al alcance, se ha de recordar que, en Colombia, aun no existe una normatividad clara respecto al desarrollo y usos de la IA más allá de las propuestas por el DNP en el CONPES 4144; las recomendaciones de la OCDE y de la UNESCO y el "Marco Ético para la Inteligencia Artificial en Colombia". Razón por la cual el alcance de dichas IA se encuentra limitada a usos específicos y mecánicos, requiriendo una presencia casi constante de un operador humano que apruebe el contenido propuesto por la IA y que dicha IA, acorde al operador, no evidencie resultados bajo una esfera discriminatoria.

Ahora bien, en el aspecto de la responsabilidad, ninguno de los documentos mencionados resuelve dicha disyuntiva. Ni siquiera el doctrinante John Tassioulas, en su texto del 2019: “First steps towards an ethics of robots and artificial intelligence” da una respuesta insatisfactoria, reduciendo el argumento a la aplicación del régimen de seguros, mediante el uso de una póliza, para que este responda ante el régimen de responsabilidad, dejándonos nuevamente en el mismo vacío. Debido a lo anterior, es menester establecer un real nexo de responsabilidad que pueda solventar el problema generado por parte de los grupos de desarrolladores de software.

Una de estas posibles respuestas seria mediante la aplicación análoga del concepto novedoso del Magistrado Ariel Salazar Ramírez “Culpa organizacional”. Dicho concepto nace de la sentencia SC13925 de 2016 la cual trata de un caso de responsabilidad en la prestación del servicio de salud, servicio que, al igual que en los casos de los desarrolladores, presenta conflictos en el aspecto de la imputación dada la imposibilidad, en ciertos casos, de atribuirle culpa a un agente determinado dentro del todo el circuito de acción. Dicho lo anterior, se menciona lo siguiente:

> La masificación del servicio de salud trajo consigo la despersonalización de la responsabilidad civil médica, que ahora no sólo se puede originar en la culpa del facultativo sino en la propia culpa organizacional, en muchos casos no atribuible a un agente determinado. *(*Corte Suprema de Justicia, Sala de

Casación Civil, sentencia del 30 de septiembre de 2016, M.P. Ariel Salazar Ramírez, p. 52*)*

Así pues, la culpa organizacional se toma como una responsabilidad subjetiva en la que una persona jurídica incurre en un error estructural en su desarrollo cotidiano. Dicho error puede nacer, entre otros, de la falta de establecimiento de controles de calidad y se evidencian mediante la causación de daños injustificados a terceros. Sin embargo, dichos errores, al no poder ser atribuibles a individuos específicos (dado a que, de hacerlo, no se genera el nexo de responsabilidad y con ello, se rompe cualquier imputación) el deber de prevención del daño (y, por tanto, la culpa) se traslada a la entidad misma, atribuyéndole dicho deber y, al incumplirlo, se convierte en la responsable.

Establecido lo anterior, la culpa organizacional, mediante la presente aplicación analógica, puede llegar a convertirse en una alternativa viable para la real estructuración de un marco de responsabilidad en el desarrollo de la IA. Al establecer la responsabilidad como subjetiva y evitar el rompimiento del nexo causal al identificar a la entidad como encargada de velar por los deberes jurídicos y no a los trabajadores de este.

Finalmente, el problema con la falta de normativa de la IA en Colombia no sólo radica en la falta de acción real por parte de los legisladores para su regulación sino también la previsión por parte de estos. Es claro que aún no logran dimensionar

el gran alcance que tienen las II. AA dentro de la vida cotidiana de los ciudadanos. Tal como se mencionó respecto al alcance, ha existido ánimo por parte del gobierno para configurar algunas hojas de ruta e intentar definir un marco ético, pero dichos esfuerzos han resultado ser tímidos y palidecen frente a la gran necesidad de tener un sistema normativo robusto que logre, de algún modo, mitigar los errores realizados por los desarrolladores, así como ofrecer seguridad jurídica a los que se vean vulnerados de alguna forma por estas herramientas.

La creación del marco ético normalmente ha sido utilizada como guía para la implementación, no sólo de directrices vinculantes para que los legisladores entiendan un poco más de tema, sino también para fortalecer el marco teórico de la IA. La importancia de este tipo de actividades es la de formar lineamientos, guías que permitan a los legisladores entender la problemática y revisar el tema, sin embargo, este marco ético es aún bastante escueto.

Es por ello que, para el desarrollo de la IA, es menester que el marco ético se convierta en verdadero protagonista en la regulación, funcionando no solo como medio para la estructuración del marco teórico o pautas sino como “reglas de juego” para la normativización, permitiendo una mejor adaptabilidad y libertad para el desarrollo de las II. AA; tal como lo evoca el modelo autorregulatorio, pero siempre encontrándose sujeto a una normatividad, regida por los principios pertenecientes a las “reglas de juego” siendo estos claros; estrictos y universales que obliguen a los desarrolladores a no llegar a pautas que contradigan o vulneren cualquiera de

los expuestos en el marco ético, primando de dicha forma la protección de los derechos fundamentales y fomentando la supervisión, inclusión y responsabilidad de los desarrolladores respecto a la creación de las II. AA, tal como lo evoca el modelo de regulación universal.

Dicho de forma ejemplificativa, es como si el desarrollo de la IA se tratase de un camino en el que las normas son el material del cual está construido (tierra, piedras, cemento, ladrillos) mientras que el marco ético, demostrado a través de principios específicos y de interpretaciones no discrecionales, son aquellas líneas delimitantes que establecen qué es camino y qué no, lo que lleva a lo siguiente: no importa el estado en que se encuentre el camino (material normativo), ya sea ineficiente, este lleno de baches o sea muy robusto, la persona que transite dicho camino (desarrollador) siempre se deberá de encontrar dentro de este (delimitado bajo los lineamientos principialistas) para poder continuar con el desarrollo de la IA, y en caso de salirse del camino, los actos que presente el desarrollador podrán ser sujeto a judicialización al haber vulnerado los acuerdos pactados (lineamientos del camino).

Referencias

Bibliografía

- Al-Othman, H. (2024, 28 de octubre). *Man who used AI to create child abuse images jailed for 18 years*. The Guardian. https://www.theguardian.com/uk-news/2024/oct/28/man-who-used-ai-to-create-child-abuse-images-jailed-for-18-years
- Álvarez, C. (2023, 13 enero). Colombia registró un crecimiento de ataques informáticos en el último año. *Voz de América*. https://www.vozdeamerica.com/a/col
- Asimov, I. (2009). *Yo robot*. Ciudad Autónoma de Buenos Aires, Argentina: Sudamericana
- Bancolombia. (s. f.). *¿Qué es y cómo evitar el Phishing en Bancolombia?* https://www.bancolombia.com/centro-de-ayuda/preguntas-frecuentes/que-es-phishing-evitarlo
- Bañuelos, J. (2020). *Deepfake: La imagen en tiempos de la posverdad.* Obtenido de Revista Panamericana de Comunicación
- BBC News Mundo. (2011, abril 26). *Roban datos de decenas de millones de usuarios de PlayStation*.

https://www.bbc.com/mundo/noticias/2011/04/110426_sony_playstaton_robo_datos_tarjetas_credito_jrg

- BBC News Mundo. (2024, abril 16). *Creating sexually explicit deepfakes to become a criminal offence*. https://www.bbc.com/news/uk-68823042
- Bobadilla, Jesús. *Machine Learning y Deep Learning: Usando Python, Scikit y Keras*. Ra-Ma, 2020.
- Casey, S. M. (1998). *Set phasers on stun: And other true tales of design, technology and human error* (2a ed.). Aegean Publishing Company.
- Castro, M. (2023) *¿Sabés cuánto contaminás al usar internet? La Huella ambiental que nadie nombra*, *Fundación Greenpeace Argentina*. Available at: https://www.greenpeace.org/argentina/blog/problemas/contaminacion/sabes-cuanto-contaminas-al-usar-internet-la-huella-ambiental-que-nadie-nombra/#:~:text=Lo%20cierto%20es%20que%20cada,7%25%20de%20la%20energ%C3%ADa%20mundial.
- *CDAO - Chief Digital and Artificial Intelligence Office*. (s. f.). https://www.ai.mil/
- CORDIS. (2003, 8 de enero). *La explosión de Ariane 5, causada por un fallo en el sistema de refrigeración del motor principal*. https://cordis.europa.eu/article/id/19509-ariane-5-explosion-caused-by-fault-in-main-engine-cooling-system/es

- *Corte Constitucional de Colombia. (2020, julio 27). PRETORIA, un ejemplo de incorporación de tecnologías de punta en el sector justicia. https://www.corteconstitucional.gov.co/noticia.php?PRETORIA,-un-ejemplo-de-incorporaci%C3%B3n-de-tecnolog%C3%ADas-de-punta-en-el-sector-justicia-8970*
- *Corte Interamericana de Derechos Humanos. (s. f.). Guerra del Golfo. https://www.corteidh.or.cr/sitios/tesauro/tr1414.htm*
- Crowell & Moring LLP. (2024, febrero 22). *Again, AI does not change the law: FTC guidance on unfair and deceptive practices involving privacy policies*. https://www.crowell.com/en/insights/client-alerts/again-ai-does-not-change-the-law-ftc-guidance-on-unfair-and-deceptive-practices-involving-privacy-policies
- Deutsche Welle. (2025, enero 7). *Reino Unido penalizará la creación de 'deepfakes' sexuales*. https://www.dw.com/es/reino-unido-penalizar%C3%A1-la-creaci%C3%B3n-de-deepfakes-sexuales/a-71236153
- Diaz, R. (2023) *La Inteligencia artificial pone en riesgo 300 millones de puestos de trabajo en todo el mundo*, *ELMUNDO*. Available at: https://www.elmundo.es/tecnologia/2023/03/29/64248311fdddffab0b8b45cf.html
- EducaciónIT, P. (2020, noviembre 2). *Los tipos de errores más comunes en programación que debes conocer*. EducaciónIT.

https://blog.educacionit.com/2020/11/02/los-tipos-de-errores-mas-comunes-en-programacion-que-debes-conocer/

- Fjeld, Jessica and Achten, Nele and Hilligoss, Hannah and Nagy, Adam and Srikumar, Madhulika, Principled Artificial Intelligence: Mapping Consensus in Ethical and Rights-Based Approaches to Principles for AI (January 15, 2020). Berkman Klein Center Research Publication No. 2020-1, Available at SSRN: https://ssrn.com/abstract=3518482 or http://dx.doi.org/10.2139/ssrn.3518482
- Fonden Calzadilla, J. C., Stuart Cárdenas, M. L., & Rodríguez Matos, L. (2018). La algoritmización: requisito necesario para la solución de problemas con el empleo de un lenguaje de programación. *LUZ*, *17*(3), 30-43. Recuperado a partir de https://luz.uho.edu.cu/index.php/luz/article/view/920
- Freire, D. (2023) *Amazon Pagará una multa millonaria Porque Alexa Guardaba Grabaciones de Voz de los Niños Sin Permiso*, *La Vanguardia*. Available at: https://www.lavanguardia.com/andro4all/amazon/amazon-pagara-una-multa-millonaria-porque-alexa-guardaba-grabaciones-de-voz-de-los-ninos-sin-permiso
- García, J. (2020, 11 noviembre). La Comisión Europea carga contra Amazon: la acusa de usar los datos de vendedores de terceros para… Xataka. https://www.xataka.com/empresas-y-economia/comision-europea-carga-amazonacusa-usar-datos-vendedores-terceros-para-competir-ellos

- González, F. (2023) *Sony investiga posible Hackeo Masivo a sus servidores*, *Wired*. Available at: https://es.wired.com/articulos/sony-investiga-posible-hackeo-masivo-a-sus-servidores#:~:text=millones%20de%20d%C3%B3lares.-,En%202011%2C%20Sony%20sufri%C3%B3%20un%20ataque%20cibern%C3%A9tico%20que%20comprometi%C3%B3%20la,de%20100%20millones%20de%20d%C3%B3lares.
- González, J. D. M. (2018, marzo 24). *Errores de programación y su solución*. Programarya.com; ProgramarYa. https://www.programarya.com/Cursos/Fundamentacion/Errores
- Goretty Carolina Martínez Bahena (2012) Uc *La Inteligencia artificial y su aplicación al campo del derecho*, *Biblioteca Corte IDH*. Available at: https://biblioteca.corteidh.or.cr/documento/65450
- Granadillo, A. (2023, 26 enero). El FBI «hackea a los hackers» responsables del secuestro de datos empresariales. *France 24*. https://www.france24.com/es/ee-uu-y-canad%C3%A1/20230126-el-fbi-hackea-a-los-hackers-responsables-del-secuestro-de-datos-empresariales
- Ibarra, S. D., Quispe, J., Mullicundo, F. F., & Lamas, D. M. (2021). *Herramientas y tecnologías para el desarrollo web desde el FrontEnd al BackEnd*. XXIII Workshop de Investigadores en Ciencias de la Computación

(WICC 2021, Chilecito, La Rioja). http://sedici.unlp.edu.ar/handle/10915/120476

- Kathleen Dollard. (2023, 7 abril). *Tipos de errores - Visual Basic*. Microsoft Learn. https://learn.microsoft.com/es-es/dotnet/visual-basic/programming-guide/language-features/error-types
- Laguna, D. (2021) *Se Cumplen 10 años del hackeo a PS network que afectó a millones de usuarios*, *LevelUp*. Available at: https://www.levelup.com/noticias/618698/Se-cumplen-10-anos-del-hackeo-a-PS-Network-que-afecto-a-millones-de-usuarios
- Lane, M. (2012) *¿Cómo se entera una tienda antes que tus padres de que estás embarazada?*, *CNN*. Available at: https://cnnespanol.cnn.com/2012/04/23/como-se-entera-una-tienda-antes-que-tus-padres-de-que-estas-embarazada/
- Mattu, J. L. A. K. (2023, 20 diciembre). How We Analyzed the COMPAS Recidivism Algorithm. *ProPublica*. https://www.propublica.org/article/how-we-analyzed-the-compas-recidivism-algorithm
- McCulloch, W.S., Pitts, W.H.: A Logical Calculus of the Ideas Immanent in nervous Activity. Bulletin of Mathematical Biophysics 5, 115–133 (1943)
- *MTP. (2022, 8 de septiembre). QAbalgando por la historia (VI): Los Patriot ignoran un misil Scud que alcanza la base de Dhahran en la Guerra del Golfo.*

https://www.mtp.es/blog/testing-software/qabalgando-por-la-historia-misiles-patriot/

- Muñoz, J. A. (2014, 10 enero). *70 millones de clientes de Target afectados por hackeo de información*. CNN. https://cnnespanol.cnn.com/2014/01/10/70-millones-de-clientes-de-target-afectados-por-hackeo-de-informacion/
- *NASA Jet Propulsion Laboratory. (s. f.). Mariner 1. https://www.jpl.nasa.gov/missions/mariner-1*
- *Norton. (2018, 8 de agosto). ¿Qué es un virus informático? Norton. https://co.norton.com/blog/malware/what-is-a-computer-virus*
- Palacios, L., Forero, V., & Labarthe, S. (2024). *Fiscal Watson: Estudio sobre el uso de inteligencia artificial en la Fiscalía General de la Nación en Colombia. Derechos Digitales.* https://ia.derechosdigitales.org/
- Rawls, J. (1979). teoría de la justicia. *Apuntes Electorales*, *16*. https://apunteca.usal.edu.ar/id/eprint/1420/
- Rojas, J.C. (2017) *Amazon compra La Cadena Whole Foods por 13.700 millones de dólares*, *El Tiempo*. Available at: https://www.eltiempo.com/economia/empresas/por-que-amazon-compra-la-cadena-whole-foods-100344
- Rouhiainen, L. (2018) *Inteligencia artificial: 101 cosas que debes saber hoy sobre nuestro futuro*, *Google Books*. Available at:

https://books.google.com/books/about/Inteligencia_artificial.html?id=_T9xDwAAQBAJ

- Sahuquillo, M. R. (2024, 5 de febrero). *Bruselas penalizará material generado por IA y las 'deepfake' sexuales de menores como pornografía infantil*. El País. https://elpais.com/sociedad/2024-02-05/bruselas-penalizara-material-generado-por-ai-y-las-deepfake-sexuales-de-menores-como-pornografia-infantil.html
- *The Astrology Page. (s.f.). Logic error. The Astrology Page. https://es.theastrologypage.com/logic-error*
- U.S. Department of Defense. (2020, February 24). *DOD adopts ethical principles for artificial intelligence*. https://www.defense.gov/News/Releases/release/article/2091996/dod-adopts-ethical-principles-for-artificial-intelligence/
- United Nations. (s. f.). *Los nuevos Intocables: Crimen, castigo y raza en los Estados Unidos | Naciones Unidas*. https://www.un.org/es/chronicle/article/los-nuevos-intocables-crimen-castigo-y-raza-en-los-estados-unidos
- *University of Texas at Austin. (s.f.). Therac-25. Ethics Unwrapped. https://ethicsunwrapped.utexas.edu/case-study/therac-25?lang=es*

- Villanueva, R. (2013, enero 24). *Multan a Sony por hackeo de 2011*. LevelUp. https://www.levelup.com/noticias/205831/Multan-a-Sony-por-hackeo-de-2011
- Wall Matthew. (2014, 6 marzo). ¿Estamos listos para la revolución de los «grandes datos»? *BBC News Mundo*. https://www.bbc.com/mundo/noticias/2014/03/140304_big_data_grandes_datos_rg#:~:text=Se%20trata%20de%20la%20gesti%C3%B3n,de%20las%20herramientas%20habitualmente%20utilizadas.
- White Geoff. (2020, 4 mayo). 20 años del Love Bug: la confesión del creador del primer gran virus informático de la historia. *BBC News Mundo*. https://www.bbc.com/mundo/noticias-52521030
- Zahumenszky, C. (2018, June 25). *Cómo un solo error de código le costó a la NASA 150 millones de dólares: el desastre de la Mariner 1*. Gizmodo en Español. https://es.gizmodo.com/como-una-sola-errata-de-codigo-le-costo-a-la-nasa-150-m-1827097911

Normatividad

- Consejo de la Unión Europea. (s.f.). Acto relativo a los servicios digitales. Recuperado de https://www.consilium.europa.eu/es/policies/digital-services-act/
- Departamento Nacional de Planeación. (2025). *Política Nacional de Inteligencia Artificial* (Documento CONPES 4144). https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/4144.pdf
- Estrategia Nacional de Inteligencia Artificial: Gobierno de España. (2020) *Estrategia Nacional de Inteligencia Artificial*. España: Gobierno de España.
- EUR-LEX - 52021PC0206 - EN - EUR-LEX. (2021). https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex%3A52021PC0206
- H.R.6216 — 116th Congress (2019-2020). (2020, 12 febrero). Congress.gov. Recuperado 17 de mayo de 2024, de https://www.congress.gov/bill/116th-congress/house-bill/6216
- Ley de Mercados Digitales | EUR-Lex. (2022). https://eur-lex.europa.eu/ES/legal-content/summary/digital-markets-act.html
- Libro Blanco sobre la inteligencia artificial: Comisión Europea. (2020). *Libro blanco sobre la inteligencia artificial: Un enfoque europeo orientado a la excelencia y la confianza* (COM (2020) 65 final). Bruselas: Comisión Europea.

- Reglamento de Servicios Digitales | EUR-Lex. (2022). https://eur-lex.europa.eu/ES/legal-content/summary/digital-services-act.html
- The White House. (2019, febrero 11). Executive Order 13859: Maintaining American leadership in artificial intelligence. Federal Register, 84(31), 3967–3972.

Jurisprudencia

- Corte Constitucional. Sentencia C-104-1993 (M.P. Alejandro Martinez Caballero; marzo 11 de 1993).
- Corte Suprema de Justicia. Sala de Casación Civil. Proceso 05001-31-03-003-2005-00174-01, (M.P. Ariel Salazar Ramírez; 30 de septiembre de 2016).