

**El Principio de Precaución y la Inteligencia Artificial en la Administración de Justicia**

**Dayron Arley Villalba Arenas, William Maldonado Delgado**

**Trabajo de grado para optar el título de Magíster en Derecho**

**Director**

**Milton Duban Monsalve Mantilla**

**Doctor en Derecho**

**Universidad Santo Tomás, Bucaramanga**

**División de Ciencias Jurídicas y Políticas**

**Maestría en Derecho**

**2025**

**Contenido**

Introducción .....	8
1. Aplicación del Principio de Precaución y la Inteligencia Artificial en la Administración de Justicia .....	10
1.1 Planteamiento del problema.....	10
1.2 Justificación .....	12
1.3 Objetivos .....	17
1.3.1 Objetivo general.....	17
1.3.2 Objetivos específicos .....	17
2. Marco referencial.....	18
2.1 Marco teórico .....	18
2.2 Estado del arte.....	22
3. Método .....	42
4. Responsabilidad Administrativa Extracontractual del Estado e IA Generativa.....	43
4.1 Inteligencia artificial generativa en el ámbito judicial.....	48
4.2 Avances de la legislación europea en IA.....	57
4.3 Marco ético y legal para la IA en Colombia .....	61
5. Análisis del Principio de Precaución en la Jurisprudencia del Consejo de Estado.....	67

5.1 El daño ambiental como escenario complejo en la regulación de tecnologías basadas en inteligencia artificial. ....	77
5.2 El Principio de Precaución y su relación con la responsabilidad patrimonial del Estado. .	79
6. Criterios y Condiciones del Principio de Precaución en la Utilización de IA Generativa en Decisiones Judiciales. ....	81
6.1 Impacto de la utilización de algoritmos predictivos en Decisiones Judiciales .....	82
6.2 Inteligencia Artificial y la violación de derechos fundamentales de las partes procesales.	89
6.3 Análisis del caso práctico: el caso Loomis vs. Wisconsin .....	94
6.4 Análisis del Caso del Juez laboral de fecha 30 de enero de 2023 .....	99
6.5 Antecedentes y dogmática de la responsabilidad extracontractual del Estado en el uso de Inteligencia artificial: riesgos y el principio de Precaución. ....	103
6.6 Teorías de imputación y el principio de precaución en el uso de IA .....	107
6.7 Aplicación del principio de precaución en la IA.....	112
7. Conclusiones .....	117
Referencias.....	119

### Resumen

Este documento aborda el desarrollo conceptual y jurisprudencial de la responsabilidad administrativa extracontractual del Estado en Colombia, destacando la transición hacia un régimen de responsabilidad directa fundamentado en la Constitución de 1991. Se examinan los elementos constitutivos de la responsabilidad extracontractual, incluidos el daño antijurídico y su imputación. Además, se discute la influencia de la inteligencia artificial generativa en la administración de justicia, particularmente en la toma de decisiones judiciales. Se destaca el uso de tecnologías emergentes y su potencial impacto en la justicia predictiva, evaluando tanto las oportunidades como los desafíos éticos y legales que plantea. A lo largo del análisis, se considera cómo la adopción de la IA en la justicia puede mejorar la accesibilidad y eficiencia del sistema judicial, al tiempo que se reconoce la necesidad de una regulación cuidadosa para proteger los derechos fundamentales y mantener la integridad del proceso judicial.

*Palabras Clave:* Principio de precaución, inteligencia artificial, responsabilidad extracontractual del estado, daño antijurídico, imputación del daño

### **Abstract**

This document explores the conceptual and jurisprudential development of the extracontractual administrative liability of the State in Colombia, highlighting the transition to a regime of direct liability grounded in the 1991 Constitution. It examines the constitutive elements of extracontractual liability, including wrongful damage and its imputation. Additionally, the influence of generative artificial intelligence in the judicial field, particularly in judicial decision-making, is discussed. The use of emerging technologies and their potential impact on predictive justice is assessed, evaluating both the opportunities and ethical and legal challenges they pose. Throughout the analysis, the potential of AI adoption in justice to enhance the accessibility and efficiency of the judicial system is considered, while recognizing the need for careful regulation to protect fundamental rights and maintain the integrity of the judicial process.

*Keywords:* Precautionary principle, artificial intelligence, extracontractual liability of the state, wrongful damage, attribution of damage.

### Glosario

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

*Algoritmo*: serie de normas o directrices claras y explícitas que facilitan la ejecución de una actividad o la solución de un problema concreto mediante etapas consecutivas.

*Aprendizaje Profundo (Deep Learning)*: campo del aprendizaje automático que utiliza redes neuronales artificiales de múltiples capas (también conocidas como profundas) para examinar patrones complejos en amplios volúmenes de datos.

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

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

*Chat-GPT*: prototipo de IA generativa capaz de crear contenido completamente novedoso mediante el uso del procesamiento del lenguaje natural y algoritmos de aprendizaje profundo.

*Daño Antijurídico*: daño causado por la administración que no debería soportar el afectado conforme a la ley.

*Falla del Servicio*: situación en la que el servicio público no funciona como debería y causa un daño, implicando responsabilidad para la administración.

*Imputación del Daño*: criterio para atribuir al Estado la responsabilidad por el daño antijurídico causado.

*Inteligencia Artificial (IA)*: integración de tecnologías, metodologías, técnicas y algoritmos diseñados con el objetivo de desarrollar máquinas que exhiban capacidades similares a las del ser

humano. Se ordena en cuatro etapas: ingeniería de control, IA clásica inferencial, aprendizaje automático y aprendizaje profundo.

*Machine Learning (Aprendizaje Automático):* una rama de la inteligencia artificial, permite a los sistemas aprender y adaptarse de la experiencia, sin requerir programación explícita. Utiliza algoritmos que analizan datos y general pronósticos basados en estos.

*Redes Neuronales:* sistemas informáticos modelados según la estructura cerebral humana, creados para identificar patrones y procesar información de manera similar a las neuronas en el cerebro.

*Responsabilidad Extracontractual del Estado:* obligación del Estado de reparar daños causados por su acción u omisión, que no están relacionados con incumplimientos contractuales.

*Riesgo Creado:* teoría según la cual quien crea un riesgo por medio de sus actividades es responsable de los daños resultantes de dicho riesgo.

## Introducción

En el contexto contemporáneo, la responsabilidad administrativa y extracontractual del Estado ha adquirido una relevancia particular, sobre todo en situaciones en las que se emplea la inteligencia artificial (IA) en la toma de decisiones judiciales. Este estudio se centra en el análisis del principio de precaución aplicado al uso de IA generativa en la administración de justicia, explorando cómo este principio puede limitar la responsabilidad administrativa y extracontractual del Estado en Colombia frente a riesgos excepcionales.

La irrupción de la tecnología en el escenario judicial no es solo una promesa de mayor eficiencia, sino también una fuente potencial de complejidades legales y éticas. A medida que la IA comienza a desempeñar un papel más activo en los procesos judiciales, desde la evaluación de evidencia hasta la predicción de resultados legales, surgen interrogantes acerca de la responsabilidad cuando estos sistemas actúan de manera inesperada o incluso errónea. El principio de precaución, una estrategia de gestión de riesgos que busca prevenir el daño antes de que este sea cierto e irreversible, se presenta como un marco de análisis vital para abordar estos desafíos.

Este trabajo se enmarca en la Maestría en Derecho de la Universidad Santo Tomás, Bucaramanga, y se guía por la supervisión del Doctor Milton Duban Monsalve Mantilla. A través de un examen detallado de la legislación, la jurisprudencia, y la doctrina, se busca comprender mejor cómo las innovaciones en IA pueden influir en la responsabilidad del Estado y cómo el principio de precaución podría servir como un mecanismo limitador efectivo en este nuevo contexto tecnológico.

La investigación procederá a desglosar los fundamentos y aplicaciones del principio de precaución, con especial atención a su impacto sobre las decisiones judiciales automatizadas y la responsabilidad que de estas derive. Al explorar este tema, no solo se busca aportar al debate

académico sino también ofrecer recomendaciones prácticas para legisladores, operadores judiciales, y desarrolladores de tecnología en IA, sobre cómo balancear innovación y precaución para proteger los derechos de los ciudadanos y mantener la integridad del proceso judicial en Colombia.

## **1. Aplicación del Principio de Precaución y la Inteligencia Artificial en la Administración de Justicia**

### **1.1 Planteamiento del problema**

La administración pública enfrenta un desafío significativo en la gestión de riesgos inherentes a sus operaciones. La falta de una gestión adecuada de estos riesgos ha dado lugar a innumerables demandas contra el Estado, lo que refleja una problemática grave en el funcionamiento y la percepción de la eficiencia gubernamental. En el proceso de modernización, es imperativo que la administración pública identifique y gestione los riesgos que pueden afectar el normal funcionamiento del Estado, ya que las consecuencias de no hacerlo son evidentes y perjudiciales.

La Agencia Nacional de Defensa Jurídica del Estado informa que, al 31 de diciembre de 2023, el Estado colombiano enfrenta más de 353,000 procesos judiciales, con pretensiones que ascienden a 603 billones de pesos. Muchos de estos casos están vinculados a una gestión inadecuada de los riesgos en el desempeño de las funciones públicas, especialmente en materia laboral y prestaciones sociales (Robledo, 2024, p.15).

La Ley 87 de 1993 establece la necesidad de un control interno para las entidades públicas, con objetivos claros como la protección de los recursos de la organización y la prevención de riesgos que puedan afectarlos (congreso de la Republica Ley 83, 1993). La Ley 489 de 1998 y su capítulo VI refuerzan este mandato, creando el sistema nacional de control interno, que incluye políticas, normas, procedimientos y tecnologías destinadas a garantizar una gestión adecuada de los riesgos (Congreso de la Republica, Ley 489, 1998, pág. Art. 8 y 68).

Diversos decretos, como el 2145 de 1999, 2593 de 2000, 1537 de 2001, 1599 de 2005 y 4485 de 2009, han sido promulgados para fortalecer el sistema de control interno y la gestión de riesgos en la administración pública. Estos decretos establecen la necesidad de controles específicos sobre los riesgos identificados y valorados, así como la implementación de acciones correctivas cuando un riesgo se materializa.

Finalmente, la Ley 1474 de 2011, conocida como el estatuto anticorrupción, en el artículo 73 exige a todas las entidades la elaboración anual de un plan de anticorrupción y atención al ciudadano, que incluye un mapa de riesgos de corrupción y medidas para mitigar estos riesgos (Congreso de la Republica Ley 1474, 2011).

A pesar de la normatividad relacionada el diagnóstico del Departamento de Planeación Nacional afirmó que el aparato estatal se ha rezagado a las necesidades del desarrollo, su organización, es anticuada, ineficiente e ineficaz, lo que implica que las demandas colectivas continúan en crecimiento, desbordando la capacidad de respuesta del Estado conllevando aún incumplimiento de las funciones asignadas por la Constitución (Departamento Nacional de Planeación, 2021, p.3).

Entonces, la administración pública tiene el deber de gestionar los riesgos inherentes a sus operaciones. La normativa existente proporciona un marco robusto para esta gestión, sin embargo, la creciente cantidad de demandas indica una implementación insuficiente o ineficaz de estas medidas, según la evolución de la deuda litigiosa del sector público y de nivel nacional en el periodo comprendido entre 2010 a 2022 (Contaduría General de la Nación, 2023, p.14). Es crucial que se fortalezcan y se apliquen rigurosamente los mecanismos de control interno y gestión de riesgos para evitar las consecuencias negativas que actualmente enfrenta el Estado colombiano.

En el contexto actual, la inteligencia artificial generativa, como ChatGPT, Copilot, ha emergido como una herramienta innovadora con potencial para transformar diversos campos, incluyendo el ámbito judicial. Sin embargo, su utilización en decisiones judiciales plantea desafíos significativos debido a los riesgos inherentes asociados con su precisión, imparcialidad y confiabilidad. Estos riesgos pueden derivar en consecuencias negativas, tanto para los individuos involucrados en los procesos judiciales como para la responsabilidad administrativa y extracontractual del Estado colombiano.

El principio de precaución, originalmente concebido para gestionar riesgos ambientales, ofrece un marco conceptual valioso para abordar la incertidumbre y los potenciales daños que podrían derivarse del uso de tecnologías avanzadas como la inteligencia artificial generativa. Este principio implica la adopción de medidas preventivas en situaciones donde existe una falta de certeza científica, para evitar o mitigar daños graves o irreversibles.

## **1.2 Justificación**

La creciente complejidad de los riesgos tecnológicos y ambientales demanda un análisis profundo de cómo las administraciones públicas manejan estos desafíos. Comprender y mejorar los mecanismos de responsabilidad y la implementación del principio de precaución es esencial para fortalecer la rendición de cuentas y la protección de los derechos ciudadanos en contextos de crisis.

El principio de precaución se centra en la prevención de daños antes de que ocurran, especialmente en contextos donde la ciencia no puede proporcionar certezas absolutas en tiempo real (Jonas, 1990, p.25). Aplicar este principio en la toma de decisiones públicas implica que el

Estado adopta una postura proactiva, minimizando la probabilidad de eventos adversos que puedan generar responsabilidades extracontractuales a título de daño de naturaleza especial.

Lo que implica que la administración pública, con la normatividad antes mencionada, debe gestionar el riesgo incluyendo la identificación y evaluación de riesgos potenciales, incluso aquellos con incertidumbre científica. Al implementar medidas preventivas basadas en estos análisis, el Estado puede evitar daños mayores, protegiendo así tanto a la sociedad como a sí mismo de reclamaciones futuras.

La implementación del principio de precaución requiere un enfoque sistemático en la gestión del riesgo, lo cual fortalece el sistema de control interno de las entidades públicas (Union Europea, 2010, p.86). Este enfoque no solo identifica y mitiga riesgos, sino que también establece políticas claras y procedimientos efectivos que pueden reducir la probabilidad de que se materialicen eventos adversos.

Es decir que la administración del riesgo establece que la gestión del riesgo debe ser integral y sistemática, involucrando a todos los niveles de la entidad pública (Congreso de la Republica, Ley 1523, 2012, p.1). Esto incluye la identificación, análisis, valoración y monitoreo continuo de los riesgos. Un sistema robusto de control interno, basado en el principio de precaución, demuestra el compromiso del Estado con la gestión proactiva y preventiva del riesgo, lo que puede reducir significativamente la responsabilidad extracontractual.

Ahora bien, la toma de decisiones informada y basada en el análisis de riesgos y la aplicación del principio de precaución permite al Estado tomar acciones justificadas y defendibles en situaciones de incertidumbre. Esto no solo protege al público, sino que también limita la responsabilidad del Estado al demostrar que las decisiones fueron tomadas con base en el mejor conocimiento disponible y en metodologías establecidas (Steele, 2006, p.21).

Recalcando que la comunicación y consulta continuas, asegura que las decisiones se tomen con información pertinente y actualizada. Al hacerlo, el Estado puede justificar sus acciones y decisiones, reduciendo así el riesgo de responsabilidad extracontractual debido a la transparencia y la rendición de cuentas en el proceso de toma de decisiones, conforme lo exige el artículo 48 y siguientes de la ley 1757 de 2015.

No obstante, lo anterior, por sí solo no bastaría, en razón a que se debe implementar una cultura organizacional que valore la gestión del riesgo y el principio de precaución asegura que todos los miembros de la entidad pública estén alineados con los objetivos de prevención y mitigación de riesgos. La capacitación adecuada de los equipos garantiza que se implementen correctamente las políticas de riesgo, reduciendo la posibilidad de errores y omisiones que podrían llevar a responsabilidades (Steele, 2006, p.21).

Una cultura organizacional sólida y bien capacitada no solo mejora la efectividad de la gestión del riesgo, sino que también fortalece la defensa del Estado contra posibles reclamaciones extracontractuales, demostrando que se han tomado todas las medidas necesarias y razonables para prevenir daños.

En el entorno legal y administrativo contemporáneo, la gestión de riesgos y la protección de los ciudadanos frente a posibles daños emergen como desafíos cruciales para el Estado. La aplicación del principio de precaución juega un papel indispensable en este contexto, orientando las acciones preventivas del Estado en escenarios de incertidumbre científica o técnica. Esta investigación se justifica por la necesidad de explorar cómo este principio no solo guía la toma de decisiones, sino que también limita la responsabilidad extracontractual del Estado, bajo la teoría de daño especial, cuando se han tomado medidas adecuadas para prevenir daños.

La “doctrina del daño especial”, que trata los perjuicios inusuales y desproporcionados que sufren los administrados debido a la acción o inacción estatal, se analiza bajo el prisma del principio de precaución. Este enfoque es crucial para entender cómo las decisiones estatales, encaminadas a proteger la salud, la seguridad y el bienestar general, pueden al mismo tiempo mitigar la exposición del Estado a reclamaciones de responsabilidad cuando se actúa de manera proactiva y considerada (García de Enterría & Fernández , 1999, p.353).

Esta investigación es fundamental porque proporciona un marco legal y teórico para comprender y aplicar el principio de precaución de manera que contribuya efectivamente a la justicia distributiva y a la equidad. Además, aborda la escasez de estudios enfocados en la relación entre la adopción de este principio y la limitación de la responsabilidad del Estado en contextos de “daño especial”, lo que es especialmente relevante en Colombia, donde la gestión del riesgo y la responsabilidad estatal son temas de creciente importancia (Consejo de Estado, Sentencia, 1947, p.46).

El estudio propuesto tiene, por tanto, un valor significativo tanto para la teoría legal como para la práctica administrativa. Permitirá a los tomadores de decisiones y a los profesionales del derecho obtener una comprensión más profunda de cómo las medidas preventivas, basadas en el principio de precaución, pueden proteger al Estado de litigios potencialmente onerosos, al tiempo que salvaguardan los derechos e intereses de los ciudadanos. Así, esta investigación no solo es relevante para los académicos, sino también para los legisladores y funcionarios encargados de diseñar políticas públicas que equilibren eficazmente los riesgos y responsabilidades.

Además de lo anterior, el principio de precaución y la administración del riesgo implican una gestión transparente y una rendición de cuentas efectiva. Al documentar y comunicar claramente las acciones y decisiones tomadas para gestionar los riesgos, el Estado puede demostrar

su diligencia y compromiso con la protección del interés público. Mantener un registro claro y accesible de las decisiones y acciones tomadas permite al Estado justificar sus medidas, lo cual es crucial para limitar la responsabilidad extracontractual al mostrar que todas las decisiones fueron tomadas de manera informada y responsable, como lo exige el principio sistémico regulado en el artículo 3 de la Ley 1523 de 2012.

Entonces la aplicación del principio de precaución como un estándar en la toma de decisiones públicas en situaciones de incertidumbre no solo protege a la sociedad de posibles daños de naturaleza especial, sino que también limita la responsabilidad extracontractual del Estado. Al adoptar un enfoque sistemático y proactivo en la gestión del riesgo, basado en la información disponible, la transparencia, y la capacitación adecuada, el Estado puede demostrar su compromiso con la prevención y la mitigación de riesgos, asegurando así una mayor protección legal y administrativa.

En el contexto de la creciente incorporación de tecnologías avanzadas, como la inteligencia artificial (IA) generativa, en el ámbito judicial, surge la necesidad de evaluar cómo los principios jurídicos tradicionales se adaptan a estas innovaciones. En particular, el principio de precaución, aunque no constituye una regla jurídica en sentido estricto, se ha consolidado como un estándar fundamental en la evaluación y gestión de riesgos, especialmente en situaciones de incertidumbre.

La integración de IA generativa por parte de los operadores judiciales plantea nuevos desafíos y oportunidades para el sistema legal. La IA generativa, al proporcionar herramientas avanzadas para el análisis y la toma de decisiones, también introduce riesgos asociados con posibles errores o malentendidos en su aplicación. En este contexto, la utilización de IA generativa conforme al principio de precaución puede demostrar el cumplimiento del deber de diligencia por parte de los operadores judiciales.

El deber de diligencia se puede demostrar cuando un operador judicial ha implementado todas las medidas preventivas razonables en el uso de IA generativa, siguiendo los lineamientos del principio de precaución, esto podría constituir una defensa válida para el Estado en casos de responsabilidad extracontractual.

La investigación se centra en explorar y delimitar el alcance del principio de precaución, evaluar la aplicación de la IA generativa en la administración de justicia y analizar su influencia en la responsabilidad extracontractual del Estado. La combinación de estos aspectos permitirá desarrollar una comprensión más profunda de cómo los principios jurídicos pueden evolucionar y adaptarse en la era de la tecnología avanzada, asegurando que la responsabilidad y la diligencia sigan siendo pilares fundamentales en las decisiones judiciales.

## **1.3 Objetivos**

### ***1.3.1 Objetivo general***

Analizar la aplicación del principio de precaución y el uso de inteligencia artificial generativa, como ChatGPT o Copilot, en la administración de justicia para evitar la responsabilidad administrativa y extracontractual del Estado en Colombia ante posibles daños de naturaleza especial.

### ***1.3.2 Objetivos específicos***

Sintetizar la evolución y aplicación del principio de precaución en la jurisprudencia colombiana, particularmente en la gestión de riesgos en situaciones de incertidumbre. A través de una revisión exhaustiva de la literatura y el análisis de casos relevantes a partir de la decisión

constitucional C-988/2004 donde se le da el alcance al principio de precaución como norma aplicable por los jueces.

Identificar los avances en la legislación de la unión europea del 2024 en la regulación de la utilización de IA generativa extrayendo las mejores prácticas y recomendaciones internacionales, con el fin de destacar las estrategias más efectivas para garantizar un uso responsable y diligente de la IA generativa en el sistema judicial.

Identificar los estándares de adherencia al principio de precaución por parte de los operadores judiciales en el contexto del uso de IA generativa puede contribuir a limitar la responsabilidad extracontractual del Estado.

## **2. Marco referencial**

### **2.1 Marco teórico**

La globalización ha interconectado las economías, culturas y tecnologías de manera que los riesgos y peligros generados en una región pueden tener repercusiones en todo el mundo. Ejemplos de esto son el cambio climático, las pandemias y las crisis financieras, que trascienden fronteras nacionales y requieren una respuesta global. Es decir que, en la sociedad moderna, los riesgos ya no son locales sino globales (Ulrich , 1998, p.233).

A diferencia de los riesgos visibles del pasado, como los desastres naturales, los riesgos actuales como la radiación, la contaminación química y “los ciberataques” son difíciles de percibir sin herramientas científicas avanzadas. Esta invisibilidad aumenta la complejidad en la gestión del riesgo. La dependencia de la ciencia y la tecnología para identificar y gestionar riesgos pone de relieve la importancia de la investigación y la innovación. Además, plantea la necesidad de

desarrollar sistemas de alerta temprana y políticas de comunicación efectiva para informar al público sobre estos riesgos (Centro Cibernético de la Policía, 2023, p.1).

Los riesgos afectan a todos, aunque su impacto puede ser desigual. En la sociedad del riesgo, ningún individuo o grupo está completamente a salvo de los peligros globales. Sin embargo, la exposición a riesgos y la capacidad de mitigarlos varían según factores socioeconómicos. Las comunidades vulnerables suelen sufrir de manera desproporcionada las consecuencias de los riesgos, mientras que las élites, al contar con mayores recursos, pueden protegerse eficazmente. Esto resalta la necesidad de implementar políticas equitativas que aborden la distribución desigual de los riesgos. Estas políticas deben traducirse en estrategias de gestión que incluyan medidas específicas para proteger a las poblaciones más vulnerables y reducir las desigualdades existentes (Ulrich , 1998, p.27).

La gestión del riesgo en la sociedad moderna se basa en la precaución y la prevención. En lugar de reaccionar a los desastres después de que ocurran, la teoría de Beck aboga por una aproximación proactiva que anticipe y mitigue riesgos antes de que se materialicen. Esto implica la implementación de regulaciones estrictas, evaluaciones de impacto y planes de contingencia cuando una duda razonable surja en relación con la peligrosidad de cualquier actividad (Loperena, 1998, p. 62).

Entonces, adoptar el principio de precaución en la formulación de políticas puede reducir significativamente la probabilidad y el impacto de los riesgos. Esto requiere una colaboración estrecha entre científicos, legisladores y la sociedad civil para identificar y abordar riesgos emergentes (Lagadec, 1984, p.72).

El principio de precaución se presenta, en el estado actual de las doctrinas y del derecho positivo, más como un vector social que aborda la incertidumbre en torno a riesgos potencialmente

graves o irreversibles, que como una norma jurídica que estructura un espacio de regulación social. Su propósito es mantener viva esta cuestión de incertidumbre en la sociedad, exigiendo que se enfrente directamente.

En este sentido, se centra más en identificar y reconocer los problemas que en proporcionar soluciones concretas. Esto lleva a ciertos malentendidos entre quienes esperan resultados más allá de lo posible, así como frustraciones en aquellos que no encuentran en él una herramienta adecuada para actuar de inmediato. Puede considerarse una construcción intermedia que sirve como puente entre los nuevos problemas derivados de riesgos cuya existencia solo se sospecha y la posterior formulación de soluciones.

El papel del principio de precaución hoy es estimular el cuerpo social y la innovación pública para que se puedan inventar respuestas. Ofrece a los actores sociales las primeras palabras de una historia que aún deben inventar.

Este posicionamiento de la precaución tiene un trasfondo político-filosófico. Una interpretación del “principio de responsabilidad” de Hans Jonas lleva a analistas y activistas a considerar el principio de precaución como un nuevo imperativo categórico que genera obligaciones, no solo morales sino también jurídicas, que exigirían que las autoridades tomaran medidas firmes y, estrictamente hablando, "indiscutibles". Por "indiscutible" se refiere a medidas que escaparían a cualquier discusión pública, a los procedimientos habituales de instrucción, deliberación y justificación (Jonas, 1990, p.25).

El principio de precaución es fundamentalmente un concepto desarrollado para abordar riesgos ambientales. Sin embargo, su aplicación y relevancia pueden extenderse más allá de estos límites. Este principio, al enfatizar la prevención en ausencia de certezas científicas absolutas,

puede servir como una guía para la toma de decisiones en múltiples áreas de la política pública y, al mismo tiempo, actuar como un límite a la responsabilidad del Estado.

El principio de precaución se origina en la necesidad de una gestión responsable de los riesgos, especialmente en contextos donde los daños potenciales son graves e irreversibles, aunque la certeza científica completa esté ausente. Este concepto se encuentra fuertemente vinculado a la “ética de la responsabilidad” propuesta por Hans Jonas, quien argumenta que debemos actuar de manera que los efectos de nuestras acciones sean compatibles con la permanencia de la vida humana auténtica sobre la Tierra (Jonas, 1990, p.81).

Más allá del ámbito ambiental, el principio de precaución puede aplicarse en áreas como la salud pública, la biotecnología, y la gestión de riesgos tecnológicos. Por ejemplo, en la gestión de tecnologías emergentes como la inteligencia artificial o la ingeniería genética, donde los posibles efectos a largo plazo son inciertos, el principio de precaución puede guiar la implementación de regulaciones que prevengan daños potenciales sin sofocar la innovación.

El principio de precaución puede funcionar como un límite a la responsabilidad estatal al establecer estándares para la toma de decisiones bajo incertidumbre. En este contexto, los estados deben adoptar medidas preventivas en situaciones de riesgo potencial significativo, lo que implica una responsabilidad proactiva de evaluar y gestionar estos riesgos antes de que se materialicen en daños.

Al mismo tiempo, este principio puede servir para limitar la responsabilidad extracontractual del Estado. Si el Estado colombiano ha actuado de acuerdo con el principio de precaución, tomando todas las medidas preventivas razonables para evitar daños, puede argumentar que ha cumplido con su deber de diligencia, incluso si eventualmente ocurren daños.

Esto es particularmente relevante en situaciones donde los riesgos eran inciertos y las decisiones tuvieron que ser tomadas sin información completa.

La incorporación del principio de precaución en diversas convenciones internacionales y la jurisprudencia de cortes internacionales subraya su creciente aceptación y aplicación. Estas normativas y decisiones judiciales refuerzan la idea de que los estados tienen una obligación de actuar preventivamente y pueden limitar su responsabilidad si demuestran haber seguido el principio de precaución (Organización de Naciones Unidas, 1992, p.1).

El principio de precaución, aunque originado en el contexto de la gestión de riesgos ambientales, tiene un potencial significativo para aplicarse en otros ámbitos de política pública y la utilización de herramientas tecnológicas. Al guiar la toma de decisiones bajo incertidumbre y establecer estándares de acción preventiva, este principio no solo promueve una gestión más responsable y ética de los riesgos, sino que también puede actuar como un límite a la responsabilidad extracontractual del Estado. De esta manera, el principio de precaución se convierte en una herramienta esencial para la gobernanza moderna en un mundo cada vez más complejo y lleno de incertidumbres.

## **2.2 Estado del arte**

El principio de precaución ha emergido como una respuesta esencial a la crisis ecológica global, impulsada por el desarrollo descontrolado de la tecnociencia y su impacto negativo en el medio ambiente. Este principio se centra en la prevención de daños potenciales al medio ambiente, especialmente cuando hay incertidumbre científica sobre los riesgos. Su fundamento filosófico se encuentra en la obra de Hans Jonas, particularmente en su "Principio de Responsabilidad", que

aboga por una ética preventiva frente a los peligros que enfrenta la humanidad y la biosfera (Jonas, 1990, p.25).

Desde la Revolución Industrial, la humanidad ha experimentado una acelerada industrialización y urbanización, acompañada de un creciente deterioro ecológico. Este contexto histórico ha impulsado el surgimiento de movimientos ecologistas y la formulación de principios éticos y jurídicos para enfrentar estos desafíos. La publicación de obras como "Primavera Silenciosa" de Rachel Carson y el informe "Los límites del crecimiento" del Club de Roma marcaron hitos importantes en la toma de conciencia ecológica (Henríquez, 2014, p.1).

Hans Jonas (1990) plantea que la tecnociencia ha transformado la promesa de un mundo mejor en una amenaza existencial. Su ética de la responsabilidad aboga por la preservación de la vida y la naturaleza, enfatizando la necesidad de una "heurística del temor" que nos alerte sobre los riesgos potenciales. El principio de precaución, en este marco, se convierte en una herramienta crucial para gestionar los riesgos ambientales y proteger el futuro de la humanidad (p.80).

El principio de precaución fue inicialmente adoptado en el ámbito de la protección ambiental y la gestión de recursos naturales, especialmente en la regulación de los medios marinos. En la década de 1960, Alemania lo incorporó en sus políticas públicas bajo el nombre de "Vorsorgeprinzip". Hans Jonas (1990) expuso que este principio ha sido clave en la formulación de normativas ambientales que buscan anticipar y prevenir daños ecológicos antes de que se conviertan en problemas irreversibles (p.81).

En palabras de Monsalve, (s.f.) el principio de precaución puede definirse a primera vista como aquel que, aun con la falta de certeza o claridad científica sobre los potenciales riesgos de una acción u objeto, deberán adoptarse las medidas necesarias para evitar un perjuicio irremediable o el agravamiento de una situación o derecho que afecte a la sociedad. Desde el marco normativo

internacional, este principio se encuentra implícito en la Declaración de Río sobre Medio Ambiente y el Desarrollo, afirmando que en los Estados recae la responsabilidad de proteger el medio ambiente, mediante la aplicación de principios como el de precaución, conforme a sus capacidades (p.188).

Respecto a sus orígenes, este se consolidó según (Artigas, 2001, p.11) como una herramienta jurídica, enmarcada en los daños a la salud y al medio ambiente, a causa del uso de productos químicos, cuyos efectos negativos, se manifestaban con el paso de los años. De otra parte, (Granja, 2017, p.17) manifiesta en su estudio, que este principio surge como un mecanismo de reparación de dichos daños.

Desde la perspectiva de Boehemer, (1994) citado por Artigas, (2001) el origen se remonta al socialismo democrático de los años treinta, fundamentado en el buen manejo doméstico. Sin embargo, esta concepción ha venido evolucionando, para trascender al término de planificación preventiva, adoptando el concepto alemán *Vorsorgeprinzip*, que constituye una serie de principios como la prevención de riesgos, la relación costo-efectividad en un marco flexible, y responsabilidades éticas para proteger los sistemas naturales, reconociendo los límites del conocimiento humano (p.12).

Citando nuevamente a Artigas, (2001) afirma que el principio de precaución se ha venido desarrollando en el contexto ambiental, a partir de algunos elementos esenciales como el actuar anticipadamente ante riesgos inciertos, proteger áreas de impacto ambiental, asegurar la proporcionalidad de las medidas adoptadas, hacer el traslado de la prueba a quien asume el riesgo, y visibilizar los derechos intrínsecos en la naturaleza, como el régimen sancionatorio por omisiones (p.15).

Artigas (2001) detalla que el principio de precaución se ha implementado progresivamente en el ámbito ambiental, con elementos clave como: actuar anticipadamente ante riesgos inciertos, proteger áreas del impacto ambiental, asegurar la proporcionalidad de las medidas adoptadas (p. 15).

Desde los años ochenta, en diferentes escenarios internacionales, se ha venido promoviendo el principio de precaución, especialmente ante la falta de certeza científica sobre los efectos específicos. En relación con ello, algunos autores como Rodríguez, (2017) en su análisis, ha determinado que el principio de prevención es un estándar anticipatorio que actúa como criterio práctico entre las ciencias jurídicas, políticas y ambientales (p.18).

Uprimny, (2014) asegura que este principio se aplica ante las amenazas de daño, aunque las probabilidades y los mecanismos causales no sean del todo claros (p.18). Más adelante, Briceño, (2017) considera que es un marco positivizado para decisiones preventivas en situaciones con potencial de daño ambiental irreversible (p.19).

En el artículo "Animales silvestres y derecho procesal constitucional", Milton Dubán Monsalve Mantilla resalta la relevancia del principio de precaución en la protección de los animales silvestres en Colombia. El autor señala que este principio constituye un deber primordial e inaplazable de carácter constitucional para las autoridades ambientales y judiciales. Según Monsalve, la defensa del medio ambiente es un pilar del Estado social de derecho, y el principio de precaución actúa como una herramienta jurídica esencial para anticiparse a posibles daños ambientales, especialmente en el contexto de las acciones populares (Monsalve Mantilla, 2021, P.19).

Monsalve (2021), describe el principio de precaución como un "instrumento cautelar proporcional y adecuado al daño que se estima que puede sufrir el medio ambiente". Este principio

debe ser aplicado cuando las circunstancias fácticas lo ameriten, siguiendo el mandato constitucional ecológico y el principio in dubio pro ambiente, que prioriza la protección ambiental en caso de duda. De esta forma, el principio no solo guía la actuación administrativa, sino que también inspira medidas cautelares en los procesos judiciales (P.20).

Monsalve (2021), En el marco de las acciones populares, el autor resalta que los jueces pueden decretar medidas preventivas basadas en el principio de precaución para proteger a las especies animales silvestres frente a posibles amenazas, como el riesgo de extinción. Ejemplos de estas medidas incluyen la repoblación faunística, definida como "todo acto que conduzca a la reimplantación de poblaciones de especies o subespecies nativas de fauna silvestre en áreas en las cuales existen o existieron". Estas acciones buscan garantizar la conservación y la sostenibilidad de las especies, evitando su desaparición (p. 20).

Sin embargo, Monsalve también critica las carencias en la práctica judicial respecto a la aplicación del principio de precaución. Señala que "no se encuentran muchos fallos en la jurisprudencia al respecto, en los que se proteja a la especie animal individualmente considerada", lo que refleja una visión predominante antropocéntrica y conservadora en el sistema jurídico colombiano. Esto evidencia que, aunque el marco jurídico reconoce la importancia de proteger a los animales como parte del medio ambiente, en la práctica se da prioridad a los intereses humanos sobre el valor intrínseco de las especies animales (p.21).

Es de resaltar que el autor destaca la importancia del principio de precaución como una herramienta jurídica clave para la protección de los animales silvestres. Sin embargo, también pone de manifiesto la necesidad de fortalecer su aplicación práctica y superar las limitaciones impuestas por una visión jurídica tradicionalista que restringe el alcance de las medidas preventivas en favor de los animales.

En el desarrollo de la jurisprudencia colombiana, también se encuentran algunos antecedentes en esta materia. Al respecto, la Honorable Corte Constitucional mediante Sentencia C-703 de 2010, hace un análisis sobre el principio de prevención, a partir del concepto de prever el daño con base en conocimientos disponibles, y el de precaución como aquel que opera cuando no existe certeza científica sobre los efectos futuros de una acción, pero si un riesgo potencial.

El Estado enfrenta desafíos significativos frente a su modernización, la gestión integral del riesgo es uno de ellos modernización del principio de precaución enfrenta desafíos significativos, como la necesidad de equilibrar el desarrollo económico con la protección ambiental y avances tecnológicos. Además, su aplicación puede ser criticada por frenar la innovación tecnológica y el progreso económico. Sin embargo, la creciente evidencia de los impactos negativos del cambio climático y la pérdida de biodiversidad refuerzan la relevancia de este principio como una guía ética y práctica para la toma de decisiones ambientales.

Al respecto algunos antecedentes importantes, han venido abordando el estudio de los avances y retos de la implementación en la administración pública. Ospina & Zambrano, (2022) afirman que, mediante la digitalización del Estado, a través del uso de la IA, se han venido promoviendo gobiernos más ágiles, transparentes e innovadores. Con aportes significativos en la eficiencia administrativa y en la calidad de los servicios (p.1).

En la implementación de la inteligencia artificial en el sector público en Colombia, se han venido potencializando los servicios públicos, tal como lo emana la misma Constitución Política y el régimen normativo vigente. Actualmente, se encuentran avances progresivos en adoptar herramientas de la IA en diversos sectores, dinamizando y optimización dichas áreas.

Conforme con la revisión de antecedentes, asegura la Cámara Colombiana de Informática y Telecomunicaciones, (2024) en el sector de la salud pública se implementó una herramienta

basada en la IA que permite mediante un algoritmo de IA, identificar en cuestión de segundos casos positivos de COVID-19, mejorando así tanto el diagnóstico como el tratamiento de esta enfermedad (p.1).

No obstante, hay que destacar que aún existen muchos desafíos al respecto, especialmente en la adopción de la IA, por factores como la falta de talento especializado en las entidades públicas, aunque existen grandes avances, se tiene hoy por hoy, que la demanda continúa superando a la oferta, lo que dificulta la implementación y gestión efectiva. Así mismo, también hay que destacar que Colombia carece de un marco normativo integral y sumado a ello, no promueve una infraestructura tecnológica óptima para este tipo de herramientas, lo que representa una brecha significativa en su implementación efectiva y eficiente (Cano & Díaz, 2023, p.12).

En la actualidad, la implementación de la IA en el sector público, se encuentra a cargo del Ministerio de las Tecnologías de la Información y las Comunicaciones, MinTic, es decir, que esta entidad, juega un rol fundamental, en la optimización de los procesos públicos, mediante el uso de la IA, lo que enmarca la necesidad de abordar un estudio investigativo, de corte académico, que permita determinar el impacto del uso de la IA en los procesos administrativos de este Ministerio, como también identificar las barreras y limitaciones, mediante el caso de estudio.

Referente al uso de la IA, se han desarrollado un sinnúmero de debates, que plantean criterios importantes para la presente investigación. De esta forma, (Morales, 2021, p.20) ha asegurado que, en el desarrollo de este tipo de tecnologías, es necesario que hagan orientaciones para la protección de los derechos humanos y la responsabilidad social (p.18). En este contexto, proponer dos principios fundamentales, como son: privacidad del diseño, que integra la privacidad desde el diseño de los sistemas de IA, y Responsabilidad proactiva, exigiendo a los desarrolladores anticipar y mitigar posibles riesgos.

De la misma manera, ha asegurado, que en casos donde el uso de la IA resulte un factor generador de daños, es necesario plantear la responsabilidad objetiva, priorizando a las víctimas (Morales, 2021, p.20).

La innovación de la tecnología se plasmó en un documento teórico desarrollado en 1950 por Alan Turing, donde se plantea la idea de que las máquinas inteligentes puedan simular la inteligencia de los humanos. Así las cosas, el término de inteligencia artificial surgió oficialmente en 1956 bajo los fundamentos de John Mc Carthy en el marco de la conferencia “Dartmouth Summer Research Proyecto sobre IA”, reconocido como el hito fundacional de la IA como campo de estudio (Cabrol et al., 2020, p.12).

Sin embargo, con posterioridad a estos planteamientos teóricos, se ha venido despertando el interés por crear robots o máquinas inteligentes dotadas con algunas características de los seres humanos. Ahora bien, no se puede desconocer que los avances realizados durante las últimas décadas han permitido la evolución de algunas tareas y funciones en diferentes áreas, y también ha dinamizado las actividades que buscan la realización de las funciones del sector público (Duarte, Alegre, Ramírez, 2023, p.15).

A partir de este tipo de necesidades y demandas del mundo moderno, las tecnologías modernas han planteado la extracción de información de datos y la realización de predicciones. En el sector público, la digitalización de la información ha llevado a las autoridades a aumentar sistemas eficientes dentro de sus procesos internos que impacten positivamente los servicios al servicio de la comunidad.

Desde la óptica del sector privado, es quizá donde mayor innovación se ha dado en materia de tecnología, apostando hoy en día a la llamada inteligencia artificial, que tiene como “objetivo el estudio y el análisis del comportamiento humano en los ámbitos de la comprensión, de la

percepción, de la resolución de problemas y de la toma de decisiones con el fin de poder reproducirlos con la ayuda de un computador” (Suarez, 2018, p.22).

También es importante, tener en cuentas las conclusiones a las que se llegaron, en el trabajo de investigación titulado “Responsabilidad civil extracontractual de la inteligencia artificial en el régimen jurídico colombiano ¿necesidad de un cambio normativo?”, afirmando que, dentro del régimen colombiano, las disposiciones que contiene el Código Civil, en los artículos 2353 y 2354, no son adaptables a la IA, porque se enfocan en seres vivos. Sin embargo, en la figura del control compartido, usado en caso de animales no fieros, podría adaptarse; en relación con la responsabilidad civil en la realización de actividades peligrosas, asegurando que existen barreras en el régimen jurídico colombiano, al no existir quien controle los riesgos que se asocian con la IA (Cárdenas & Gómez, 2020, p.15).

En síntesis, el manejo de la responsabilidad civil por los daños de la IA debe basarse en un enfoque flexible que combine aspectos de los regímenes objetivos y subjetivos existentes, adaptándolos a las características únicas de la tecnología (Cárdenas & Gómez, 2020, p.15).

En la obra “Constitución e Inteligencia Artificial en proceso” se aborda un análisis referente a la integración de las tecnologías de la información y la comunicación, en los procesos judiciales, independientemente de la jurisdicción. Analiza la autora que, en las Constituciones Iberoamericanas, como ocurre con Colombia y Venezuela, a partir del reconocimiento de sus ejes axiales, como son la dignidad humana, la justicia, la igualdad, la libertad y la paz, que sirven de guía para el régimen normativo, también fundamentan la incorporación de las tecnologías avanzadas, como la IA en el ámbito social y judicial (Guerra, 2022, p.15).

Dentro de este escenario, se plantea que, si bien es cierto los derechos fundamentales, son preexistentes a la promulgación de las Constituciones Políticas, también es cierto que deben ser

salvaguardados en el marco del desarrollo y uso de la IA. Conforme a ello, es preciso que, con la implementación de la IA, también se promueva el cumplimiento de los parámetros internacionales definidos para la protección de derechos humanos, garantizando la imparcialidad, y los sesgos con el fin de comprometer la equidad. Sumado a ello, también deben formularse mecanismos de control y responsabilidad para la evaluación del comportamiento de la IA y la mitigación de sus riesgos (Guerra, 2022, p.15).

Desde el contexto de la administración de justicia, es preciso tener presente el reconocimiento del acceso a la justicia como derecho fundamental, desde la órbita internacional, tal como lo dispone la Convención Americana sobre Derechos Humanos, en sus artículos 8 y 25, para que la IA se convierta en una herramienta transformadora. Sin embargo, el proceso no puede generarse exclusivamente desde el ámbito técnico, creándose algoritmos con la IA, sino un proceso de transformación sistémico que contemple la integración tecnológica de manera coherente, donde se incluyan, elementos como el acceso a los recursos judiciales, la transparencia de los algoritmos utilizados y la promoción de la ética en el diseño de los programas y sistemas de la IA. A partir de lo expuesto, es determinante que se tenga presente dentro del marco regulatorio para la incorporación de la IA, el marco de principios constitucionales, garantizando la preservación de los derechos fundamentales y se respete la dignidad humana (Guerra, 2022, p.15).

Otra posición al respecto de la IA como un fenómeno tecnológico transformador, con un impacto a gran escala. No obstante, también se hacen precisiones, sobre los desafíos éticos y jurídicos, que se derivan, especialmente con la creación y difusión de contenidos denigrantes generados por la IA, como imágenes que generan vulneración de derechos fundamentales.

Analógicamente, afirman Ortiz y Ortiz (2024) que cuando la IA toma decisiones autónomas e inferencias que impactan diversos entornos físicos y virtuales, sin poder asumir

responsabilidad debido a su naturaleza no jurídica. De esta manera, los daños que generen por el uso de la IA, es necesario que se analicen a través de los principios de responsabilidad civil, identificando conductas específicas que constituyan un hecho generado del daño, lo que implica un estudio parara identificar el nexa causal y la imputación de responsabilidad, basándose en teorías como la de la causalidad adecuada (Ortiz & Ortiz, 2024, p.28).

Desde la perspectiva de la Corte Constitucional Colombia, se ha identificado un reciente fallo, ha entrado a analizar las decisiones judiciales a partir del uso de la IA, específicamente de la plataforma ChatGPT 3.5, como herramienta para la proyección de un fallo de tutela, haciendo un análisis frente a la vulneración del derecho fundamental al debido proceso. En contexto, la Corte, argumento que no existió la sustitución del ejercicio de la función jurisdicción por parte del sistema IA, toda vez que el juez había tomado una decisión con anterioridad y solo activo la herramienta de la IA, para elevar una consulta con el fin de obtener respuestas adicionales. No obstante, aseguro que, pese a que no existió una vulneración de los datos personales de los accionantes, no se cumplen los principios de transparencia y responsabilidad en el uso de la IA (Corte Constitucional de Colombia, Sentencia T-323 de 2024).

En el marco de las consideraciones de la Corte Constitucional, también se puso en contexto, la necesidad de reconocer los retos que enfrenta la adopción de un régimen para la administración de la IA, todas que aun el panorama no es claro en el ámbito nacional, ni en el internacional. Taxativamente afirmó que:

La falta de normas y puntos de referencia comunes entre los marcos nacionales y multinacionales de gestión de riesgos, así como las múltiples definiciones de IA utilizadas en dichos marcos han complicado el panorama de la gobernanza de la IA, a pesar de la necesidad de espacio para que coexistan diferentes enfoques reguladores que reflejen la

diversidad social y cultural del mundo (Corte Constitucional de Colombia, Sentencia T-323 de 2024).

Al paso de esta decisión de la Corte Constitucional, (Herrera, 2024) manifiesta que existen diversas definiciones sobre la IA, como un fenómeno que no puede reducirse a la cuestión meramente tecnológica, sino que sus aplicaciones están condicionadas al funcionamiento de los sistemas democráticos, las políticas públicas, la innovación, la producción cultural, la economía e incluso los espacios íntimos de las relaciones sentimentales. Es decir, que es preciso abordar la misma desde sus aspectos positivos, como también un manejo cauteloso (p.33).

Haciendo un repaso por lo expuesto en este apartado, se puede indicar que en la actualidad se aborda un tema crucial, y son los desafíos jurídicos que se derivan del uso de los sistemas de IA, en diferentes escenarios y contextos, especialmente en lo que tiene que ver con la responsabilidad por los daños causados. A medida que la IA se va integrando en los procesos del sector público y del sector privado, también se avizoran sus fallas o errores, lo que determina grandes retos para el legislador, pero principalmente el debate central se enmarca en la figura de la responsabilidad civil, como la responsabilidad administrativa y extracontractual que recae en el Estado (Jiménez, 2024, p.37).

Conforme al análisis planteado, en Colombia desde el sector privado se han venido adoptando las tecnologías basadas en la IA, permitiendo determinar la necesidad de determinar aquellas situaciones donde se requiere una compensación por daños, lo que exige una reflexión jurídica sobre los marcos legales, que, en la actualidad en nuestra legislación, no contemplan los daños derivados de la IA.

En la actualidad, la tendencia se enmarca en la figura de la responsabilidad extracontractual, no es posible pasar por alto la relevancia de la responsabilidad contractual, que

implica un enfoque más preventivo y detallado, centrado en la correcta identificación y distribución de riesgos en los contratos (Jiménez, 2024, p.37).

Uno de los aspectos elementales es la categorización de los riesgos asociados con la IA, que se clasifican en riesgos directos, secundarios y no previsibles. Los primeros, se relacionan con fallas o defectos inherentes al sistema de la IA, por su parte los riesgos secundarios parten del uso irresponsable de la persona, afectando el cumplimiento contractual, como es el caso de la filtración de información confidencial. Sumado a ello, se encuentran los riesgos previsibles, que son de alta complejidad en su definición y abordaje por la rapidez con la que evoluciona la tecnología.

Otra problemática que identifica Jiménez, (2024) tiene relación con la probar la responsabilidad extracontractual, toda vez que los sistemas de la IA operan de forma autónoma y toman decisiones sin la intervención directa de un ser humano, dificultando elementos propios como es la causalidad, la culpa y el nexo causal. Sumado a ello, se encuentra, la opacidad de estos sistemas ("cajas negras") añade una capa de complejidad, ya que puede ser difícil comprender cómo los sistemas llegan a ciertas conclusiones (p.1).

En este escenario, se tiene como una necesidad imperante, que se aborden los nuevos desafíos de la IA, proponiendo dentro de los contratos nuevas cláusulas, pero también desde la responsabilidad del legislador, promover un marco legal capaz para la gestión eficiente de los riesgos y responsabilidad relacionados con la IA. En Colombia, se necesita un sistema especial, en materia de responsabilidad, que se aplique frente a los riesgos que representa el uso de la IA. Este es un tema complejo que debe ser abordado con una visión crítica, creativa e innovadora para lograr una adecuada protección legal en un contexto tecnológico en constante cambio (Jiménez, 2024, p.37).

En la misma línea, es preciso citar a Rodríguez, et al, (2024) quien asegura que la IA generativa, ha revolucionado varios escenarios, permitiendo a través de herramientas como ChatGPT, abrir nuevas oportunidades para el aprendizaje. No obstante, hay que establecer que es necesario que se revise el impacto que tienen en dichos procesos, para evaluar la relevancia y efectividad en las actividades académicas (p.1).

En un análisis reciente de Colmenares, (2024) se analiza como las transformaciones globales derivadas de la cuarta revolución industrial, han generado cambios estructurales en las sociedades modernas, reflejándose especialmente en el campo del derecho o los regímenes normativos, donde se ha recreado la necesidad imperante de crear de mecanismos modernos de justicia, buscando mejorar los procesos y garantizar el acceso. De la misma manera, al aterrizarlos en el ámbito iberoamericano, se puede establecer que el impulso por las reformas políticas públicas ha promovido la modernización de la justicia, a través de la implementación de las tecnologías de la información y la comunicación, acompañados de las herramientas de la IA (p.1).

En línea con lo anterior, analiza Colmenares, (2024) que la incorporación de estas tecnologías, ha reformado los sistemas judiciales, planteándose procesos eficientes, y la optimización de los recursos, convirtiéndose en tendencias relevantes para el derecho proceso contemporáneo, permitiendo además cerrar brechas de desigualdad, promoviendo la inclusión en sistemas confiables y eficaces, consolidándose como un elemento clave para el bienestar colectivo, reflejando las garantías constitucionales reconocidas en los países iberoamericanos (p.1).

Durante la última década, el auge la IA generativa, también ha generado debates frente al potencial en la implementación dentro de los procesos judiciales, destacando las ventajas de los algoritmos en los procesos judiciales, que permite eliminar la congestión judicial, especialmente en la emisión de fallos.

No obstante, el debate central se ha posicionado sobre la viabilidad de la IA generativa en la toma de decisiones. Al respecto, se debe decir que, aunque este tipo de tecnologías están diseñadas para predecir respuestas basadas en datos y patrones pre-entrenados, evidentemente carecen del razonamiento humano, así como de la capacidad para realizar juicios abstractos y contextuales, lo que puede llevar a que se emitan decisiones que trasgredan los derechos fundamentales del ciudadano (Colmenares, 2024, p.1).

Dicha problemática, se enmarca especialmente en aquellas decisiones que son tomadas a partir de los algoritmos, que en un país como Colombia, donde fenómenos como la brecha de desigualdad ha estado presente por siglos, perpetuando estas dinámicas, al no tenerse en cuenta elementos subjetivos, emocionales o contextuales propios del razonamiento humano, toda vez que las decisiones humanas, aunque no están exentas de irregularidades, ofrecen un mayor grado de análisis y reflexión, así como la posibilidad de una revisión jerárquica que las decisiones autónomas tomadas con la IA no garantizan.

En cuanto al derecho procesal contemporáneo, hay que precisar, que si bien es cierto el juez no es un actor central, si está encargado de hacer una interpretación y contextualización del régimen jurídico, aplicándola al caso concreto. Ahora bien, su rol no puede ser reducido exclusivamente al análisis lógico- matemático como el que se realiza con los algoritmos, toda vez que, en derecho, es necesario construir a partir de la experiencia, más que de la lógica.

En este escenario, se puede tomar de las reflexiones del citado autor, que el proceso de digitalización y modernización en la justicia es un proceso inevitable, y que evidentemente la implementación de la IA genera grandes beneficios, pero no es viable, que pueda sustituir al ser humano, en cuanto al análisis que requiere una decisión judicial, máxime en el marco de un Estado Social de derecho. Es decir, que los jueces requieren de altos estándares morales y capacidad de

razonamiento para ejercer sus funciones, algo que los algoritmos no podrán sustituir, ni tampoco replicar.

En este orden de ideas, se puede establecer de la investigación de Colmenares, (2014) que los proyectos que se han venido abordando en cuanto a la modernización judicial en Iberoamérica, con enfoque en la implementación de las tecnologías emergentes, promueven desarrollar los procesos con cautela, enfocándose en la optimización de los procesos técnicos, sin que se comprometa la esencia del juicio humano. Como bien apunta Carnelutti: "Un ordenamiento jurídico puede imaginarse sin leyes, pero no sin jueces" (p.12).

Haciendo una síntesis de los estudios citados en este apartado, se puede establecer que sobre el principio de precaución se han emergido algunas concepciones doctrinales y jurídicas, que apuntan a una respuesta ética y legal en materia de la crisis ambiental global a causa del desarrollo acelerado de la tecnociencia. Basándose en las tesis de Jonás, este principio se enmarca en la prevención de daños potenciales al medio ambiente, máxime cuando no existe certeza sobre los riesgos en el ámbito científico.

Por su parte, desde el contexto de la jurisprudencia colombiana, se destaca la importancia de proteger los derechos colectivos, diferenciándolo el derecho de precaución y el de prevención, toda vez que opera ante incertidumbres científicas.

En paralelo con lo que se ha venido exponiendo en este apartado, es tiene que la IA ha venido transformación los procesos y tramites que se originan en el sector público, permitiendo una optimización en áreas como la salud, entre otros. Sin embargo, también hay que dejar claridad, en torno a estas reflexiones, que la implementación de este tipo de herramientas también enfrenta desafíos significativos, a partir de circunstancias como la carencia de talento especializado, la falta de un régimen normativo integral y una infraestructura tecnología limitada. Es decir, que el uso de

la IA deberá regirse por principios éticos, como son la privacidad desde el diseño y la responsabilidad proactiva, para garantizar que sus beneficios no vulneren derechos fundamentales.

En conclusión, se establece que el principio de precaución como la IA enfrenta grandes retos, en la actualidad. No obstante, es primordial abordar las barreras, para asegurar una implementación responsable y promover el equilibrio entre el desarrollo tecnológico, la sostenibilidad y la equidad social.

En cuanto al impacto de la IA desde la esfera jurídica, social y económica, se han definido una serie de oportunidades, como también de desafíos, especialmente en lo que atiende a la responsabilidad civil y la gobernanza tecnológica. Durante los últimos años, se han logrado grandes avances, que permiten el desarrollo de actividades técnicas, que replican algunas características del ser humano, transformando los procesos del sector público y del sector privado.

En el escenario colombiano, este panorama de la implementación de la IA presenta grandes limitaciones, tal como lo plantean Cárdenas & Gómez, (2020), las disposiciones del Código Civil en materia de responsabilidad civil no son aplicables a aquellos daños o perjuicios que se presenten como consecuencia del uso de la IA (p.18).

Otro aspecto debatido, tiene que ver con la incorporación de la IA, en relación con los derechos fundamentales, planteándose la necesidad de que las políticas públicas sobre implementación de la IA armonicen con las disposiciones constitucionales, máxime en el respeto a la dignidad humana, la justicia y la igualdad, así como a los parámetros internacionales reconocido en la Convención Americana sobre Derechos Humanos.

Referente al manejo de la responsabilidad civil derivada de la IA, tanto en Colombia, como en otros países, se concretan algunos criterios, frente a las necesidades tecnológicas y económicas,

pero también desde la salvaguarda de los derechos fundamentales, la ética en el diseño y la regulación adaptable al cambio constante.

Se hace necesario también revisar que se ha investigado sobre la IA en la administración de justicia, según Suárez Manrique, De León Vargas y Luna Salas (2019), los autores proponen una tesis crítica basada en la reconstrucción dogmática del derecho a través de la tecnología, con el objetivo de modernizar y descongestionar el aparato jurisdiccional, expresan que es un desafío de orden constitucional, técnico y ético, que requiere ser analizado desde la perspectiva del derecho fundamental a la tutela judicial efectiva.

Desde la perspectiva de la IA como una herramienta que transforma el entorno jurídico al modificar los marcos de cognición y comunicación en los que el derecho se desenvuelve, para los autores, dicha transformación obliga a repensar el papel del derecho en un entorno digital, especialmente en lo que respecta a la eficiencia de la administración de justicia y el acceso a ella (Suárez Manrique et al., 2019, pp. 72–74).

Uno de los aportes más significativo de los autores en su investigación radica en la clasificación de las aplicaciones de la IA en el ámbito judicial, donde las agrupan en tres grandes dimensiones: los procedimientos judiciales, donde se busca automatizar etapas como la búsqueda de precedentes o la redacción de providencias; el análisis probatorio, que puede apoyarse en herramientas como la verificación automatizada de testimonios o autopsias virtuales; y la toma de decisiones, donde la IA funge como apoyo para ofrecer al juez diferentes alternativas de solución (Suárez Manrique et al., 2019, pp. 79–80).

Consideran que la IA no debe reemplazar al juez, sino asistirlo mediante la automatización de tareas repetitivas, la gestión inteligente de expedientes y la presentación de alternativas para la toma de decisiones. Esta tecnología, afirman, puede ser clave para transformar positivamente el

sistema judicial colombiano si se emplea como herramienta complementaria respetando principios como la dignidad humana y los derechos fundamentales (Suárez Manrique, De León Vargas & Luna Salas, 2019, pp. 72–81).

Continuando con la aplicación de la IA en la administración de justicia se trae a colación lo investigado por Manuel José Cepeda Espinosa y Guillermo Otálora Lozano (2020) sobre el debate de la incorporación de la IA en el ámbito judicial, pues según los autores presentan una reflexión equilibrada sobre el papel que puede jugar la IA en la transformación del sistema judicial. Los autores parte de la premisa que la IA deber ser un aliado del juez, no su reemplazo.

Lo autores identifican tres áreas claves donde la aplicación de la IA podría ser mas efectiva, en la gestión del conocimiento jurídico, el uso de la información judicial para diseñar políticas publicas mas acertada, y a la optimización del proceso judicial mediante la automatización de tareas repetitivas. Este enfoque permitiría que los jueces puedan concentrarse en lo verdaderamente complejo (Cepeda & Otálora, 2020, pp. 27-31).

Los autores también precisan que ninguna decisión que implique el ejercicio del juicio, especialmente aquellas que afectan derechos fundamentales, deberían quedar en manos de un algoritmo, por lo tanto, proponen hablar sobre “inteligencia artificial aumentada”, es decir, tecnologías que potencian las capacidades humanas sin sustituirlas (Cepeda & Otálora, 2020, p. 27-31).

los autores expresan que no son ingenuos en cuanto a los riesgos. Aceptan en términos inequívocos que los procedimientos de justicia con IA pueden conllevar graves problemas, si no siempre toman precauciones. Por ejemplo, sesgos discriminatorios o que los sistemas se vuelvan tan opacos que ni los propios jueces puedan explicar cómo llevo a esa conclusión. Por eso insisten

en que, además de la implementación técnica, es fundamental contar con un marco ético y legal solido que regula estas herramientas (Cepeda & Otálora, 2020, pp. 42-45).

En definitiva, Cepeda y Otálora no caen ni en el entusiasmo desbordado ni en el rechazo absoluto. Su propuesta busca abrir camino a una justicia más moderna, eficiente y equitativa, pero sin perder de vista la esencia humana del acto de juzgar. El documento no solo ofrece una hoja de ruta práctica para avanzar en esta dirección, sino que también plantea un llamado a la reflexión sobre los valores que deben guiar cualquier transformación tecnológica en un campo tan delicado como el judicial.

En ese contexto, Pere Simón Castellano (2021) plantea una postura crítica y matizada frente a la incorporación de sistema de IA en la administración de justicia. El autor hace una revisión detallada del marco legal europeo y experiencias comparadas que lo lleva a reconocer que la IA puede contribuir a mejorar la eficiencia, accesibilidad y la transparencia del sistema judicial, sin embargo, advierte que su implementación debe estar cuidadosamente regulada a fin de evitar vulnerar derechos fundamentales como la protección de datos, igualdad, derecho de defensa y el debido proceso (Simón Castellano, 2021, p. 11).

Uno de los ejes centrales del análisis en su artículo es que la IA no puede ni debe sustituir al Juez por mas sofisticados que sean los algoritmos, lo cual indica que cualquier tecnología basada en IA se debe concebir como una herramienta de apoyo a la labor del operador jurídico, no como reemplazo, a lo cual cita el artículo 117.3 de la constitución española (Simón Castellano, 2021, p. 12).

El autor en su análisis muestra una preocupación constante en la aplicación de la IA en la administración de justicia por la opacidad de sus algoritmos, lo que implica que su utilización sin

una regulación específica puede conllevar a reproducir sesgos discriminatorios si no se diseñan criterios éticos y jurídicos adecuados, entre los ejemplos que cita el autor menciona el sistema COMPASD en Estados Unidos o HART en el Reino Unido donde han demostrado como ciertos modelos predictivos utilizados en proceso penales pueden generar sesgos raciales o errores injustificables, lo cual pone en riesgo la igualdad ante la ley (Simón Castellano, 2021, pp. 8-9).

En cuanto al marco normativo vigente destaca que el reglamento general de protección de datos (RGPD de la Unión Europea contempla restricción al tratamiento automatizado de datos personas, sin embargo, las lagunas jurídicas y la falta de una normativa específica para la IA judicial dificultan una aplicación homogénea de garantías a nivel europeo (Simón Castellano, 2021, pp. 6-7).

El autor finalmente propone que la aplicación de la IA en el campo judicial debe basarse en principio como la transparencia, la explicabilidad, el control humano y la equidad y que su desarrollo debe ir acompañado de supervisión institucional independiente y participación de expertos en derecho en el diseño de los algoritmos (Simón Castellano, 2021, pp. 10-12).

### **3. Método**

La metodología adoptada en esta investigación tiene un enfoque cualitativo, con un alcance tanto exploratorio como descriptivo. El enfoque exploratorio se justifica por la novedad del tema a desarrollar, mientras que el enfoque descriptivo se emplea para presentar las principales características jurídicas del principio de precaución.

La investigación se centrará en examinar cómo se aplica el principio de precaución en la utilización de IA generativa en la toma de decisiones judiciales por un operador y cómo este limita

la responsabilidad del Estado en Colombia. Para abordar este tema, se empleará un enfoque cualitativo basado en el análisis de fuentes documentales.

Con este enfoque metodológico, se espera contribuir a la comprensión y aplicación del principio de precaución en el marco de la responsabilidad extracontractual del Estado colombiano.

#### **4. Responsabilidad Administrativa Extracontractual del Estado e IA Generativa**

El concepto de riesgo siempre está vinculado a la noción de responsabilidad. En este contexto, la responsabilidad puede surgir de diferentes ámbitos: fiscal, penal, contractual y extracontractual. En lo que respecta a la responsabilidad extracontractual, es fundamental partir del estatuto general vigente en Colombia, consagrado en el artículo 90 de la Constitución Política. Este artículo marca un punto de inflexión en la evolución de la responsabilidad estatal, diferenciando claramente la situación antes y después de la Constitución de 1991 (Corte Constitucional, Sentencia C-333, 1996). Antes de la promulgación de esta norma superior, no existía una disposición constitucional que atribuyera responsabilidad directa al Estado. Sin embargo, se aplicaba el artículo 8 de la Ley 153 de 1887, que permitía al operador judicial establecer responsabilidad a través de casos análogos.

La responsabilidad extracontractual del Estado en Colombia se enmarca inicialmente en el Código Civil, específicamente en el artículo 2341 y siguientes, que regulan esta materia (Codigo Civil, 1973). En un principio, se consideraba que la responsabilidad del Estado era indirecta. No obstante, con el desarrollo jurisprudencial, se estableció que dicha responsabilidad es directa, tal como lo establece el artículo 90 de la Constitución. Este artículo introduce dos elementos esenciales: el daño antijurídico y la imputación del daño (Constitucion Politica, 1991).

En Colombia, la responsabilidad extracontractual fue inicialmente competencia exclusiva de la jurisdicción ordinaria. Posteriormente, se compartió con la jurisdicción contencioso-administrativa y la Corte Suprema de Justicia. Con la expedición del Decreto Ley 528 de 1964, se estableció la responsabilidad del Estado bajo la competencia exclusiva de la jurisdicción contencioso-administrativa. Hasta la fecha, Colombia ha promulgado cuatro códigos contenciosos administrativos: la Ley 130 de 1913, la Ley 167 de 1941, el Decreto 01 de 1984 y la Ley 1437 de 2011.

El artículo 90 de la Constitución introduce dos conceptos clave: el daño antijurídico y la imputación del daño. Las primeras interpretaciones del Consejo de Estado (1991 y 1993), bajo la ponencia del magistrado Julio César Uribe Acosta, establecieron que la responsabilidad del Estado en Colombia se había objetivizado (Consejo de Estado, Sección III, Sentencia Exp. 6515, 1991). Esta postura fue declinada en la sentencia de unificación de la Sala Plena de la Sección Tercera del Consejo de Estado, con ponencia de Hernán Andrade Rincón, el 19 de abril de 2012. En dicha sentencia, se concluyó que el artículo 90 no establece ni privilegia un régimen de responsabilidad en particular, dejando al operador judicial la tarea de determinar, tras el estudio de las pruebas y el análisis del caso concreto, si se aplica un régimen objetivo o subjetivo (Sentencia Exp. 21359, 2013).

En Colombia, existen dos regímenes de responsabilidad: el régimen de responsabilidad subjetiva, basado en la falla probada, y el régimen de responsabilidad objetiva. Los elementos de la responsabilidad de la falla probada incluyen la falla del servicio, el daño y el nexo causal entre el hecho dañoso y el agente responsable. Por otro lado, en el régimen de responsabilidad objetiva, solo es necesario probar el daño y el nexo causal.

El daño es el elemento más importante y primordial en la responsabilidad extracontractual. Juan Carlos Henao lo define como la disminución de una circunstancia o situación favorable. Es decir, frente a las acciones u omisiones del Estado, se puede disminuir una situación favorable como consecuencia de un hecho dañoso. Cuando se incorpora el concepto de antijuridicidad al daño, es decir, el daño antijurídico, se establece que el Estado no solo responde por actos ilegales, sino también por actuaciones que, aun ajustadas a la legalidad, generan un daño, conocido como daño especial (Henao, 1998, p.317).

Finalmente, es necesario distinguir entre daño y perjuicio. Hernán Andrade Rincón define el daño como la afectación sufrida de manera física o material, mientras que el perjuicio es la consecuencia o reflejo de ese daño (Consejo de Estado, Sección III, Exp. 21294, 2011). En mi opinión, no necesariamente todos los daños materiales o físicos generan un perjuicio. Para complementar esta distinción, se puede decir que existe daño material, que a su vez puede ser un daño jurídico. El daño físico es el que afecta la integridad física de la persona, mientras que el daño jurídico no afecta físicamente al sujeto, como en el caso de la desvalorización de un bien inmueble, por la construcción de un aeropuerto que origina ruido generando una pérdida del valor comercial de los inmuebles cercanos.

En cuanto a las imputaciones subjetivas, se destacan la falla del servicio y la falla presunta del servicio. En la falla presunta, se traslada la carga de la prueba a la parte demandada, presumiendo que hubo una falla. El Consejo de Estado ha explicado que esta figura es común en la responsabilidad médica, donde el especialista, al encontrarse en una mejor posición para probar que su actuar fue diligente, asume la carga de la prueba, evitando que recaiga sobre el demandante (Consejo de Estado, Sección III, Sentencia Exp. 31182, 2014).

Antes de la expedición del Código General del Proceso (C.G.P.), la falla presunta tenía implicaciones graves, pero su tratamiento ha perdido su operatividad práctica en razón a que el estatuto procesal reguló la carga de la prueba en su artículo 167, que indica que a las partes incumbe probar el supuesto jurídico que las normas jurídicas persiguen, no obstante, atendiendo a las particularidades del caso concreto podrá invertirse la carga de la prueba.

Cuando se habla de la falla del servicio, se plantea que, más allá de los títulos jurídicos materiales, esta puede clasificarse según su origen en imputaciones jurídicas. Entre estas, se encuentran las de origen constitucional, como la expropiación por vía administrativa, y las de origen legal, como la establecidas en ley 270 de 1996 en el artículo 65 y siguientes, que abarcan situaciones como la privación injusta de la libertad, el defectuoso funcionamiento de administración de justicia y el error judicial. Adicionalmente, hay tres títulos de imputación cuyo origen es por vía jurisprudencia como la falla del servicio, el daño especial y el riesgo (Consejo de Estado, Sección III, Sentencia Exp. 16696, 2007).

Cuando se habla de la falla del servicio no hay definición como tal, si bien se mencionó antes que la falla es de origen jurisprudencial, cabe destacar que la ley 142 de 1994, en su artículo 136, establece la presunción de la falla en la prestación del servicio público. Según este artículo, cuando la empresa de servicios no preste de manera continua el servicio, se presumirá la existencia de una falla en la prestación, a lo cual el artículo 137 de la ley 142 de 1994 establece cuales son los deberes de reparación cuando han incurrido en esa falla.

Después de una breve explicación de las teorías de imputación subjetiva, es momento de desarrollar las teorías de la imputación objetiva, entre las cuales destacan el riesgo y el daño especial. La teoría del riesgo surgió en la Revolución Industrial inglesa en 1760, cuando se comenzó a utilizar el maquinismo, lo que provocó daños significativos a las personas debido al

uso de nuevas tecnologías. Esto originó la necesidad de establecer un sistema que contrarrestara dichos daños, dando lugar a la teoría del riesgo creado, que establece que quien crea el riesgo debe asumir sus consecuencias (Consejo de Estado, Sección III, Sentencia Exp. 18940, 2011).

Desde esta premisa, la teoría del riesgo sostiene que algunas actividades conllevan una alta probabilidad de generar un daño, y a medida que se intensifican esas actividades, también aumenta la probabilidad de que ocurra un hecho dañoso. En la década de los noventa, el Consejo de Estado, en su Sección Tercera, desarrolló tres subreglas relacionadas con el riesgo: riesgo alea, riesgo peligro y riesgo beneficio (Consejo de Estado, Sección III, Exp. 16530, 2008).

El Riesgo Peligro Se refiere al riesgo que surge de objetos peligrosos, métodos peligrosos o la ejecución de trabajos públicos en el caso de las armas de fuego o los vehículos automotores. El Riesgo Beneficio se da cuando una persona o entidad se beneficia de una actividad riesgosa. Un ejemplo cotidiano es el de las empresas prestadoras del servicio de energía eléctrica, que se benefician de la conducción de energía y, al mismo tiempo, generan un riesgo. En consecuencia, estas empresas son responsables de los daños que puedan derivarse de su actividad (Consejo de Estado, Sección III, Exp. 16530, 2008).

El Riesgo Alea: definido por el Consejo de Estado como las probabilidades derivadas del azar, este tipo de riesgo ha sido aplicado, por ejemplo, en casos de enfermedades intrahospitalarias, como cuando una persona contrae una enfermedad simplemente por visitar un centro médico (Consejo de Estado, Sección III, Exp. 16530, 2008).

El Consejo de Estado también ha examinado otras tipologías de riesgo, incluyendo los actos terroristas, que la corporación encuadra dentro del riesgo de conflicto armado, considerando que, aunque es un tipo de riesgo, no encaja en las subreglas mencionadas anteriormente (Consejo de Estado, Sección III, Sentencias 35874, 2016).

Por otro lado, el daño especial se refiere a un desequilibrio en las cargas públicas, donde una carga se considera anormal cuando excede las cargas que los ciudadanos están en el deber de soportar. Es importante señalar que, mientras la teoría del riesgo se fundamenta en la creación de un riesgo, el daño especial se basa en la existencia de un daño derivado de la actuación legítima del Estado. Sin embargo, en ambos casos, el Estado puede ser responsable de los daños generados.

#### **4.1 Inteligencia artificial generativa en el ámbito judicial**

El término "inteligencia artificial" se utilizó por primera vez en una conferencia académica celebrada en Dartmouth College en 1956. En ese seminario, los pioneros en la materia discutieron cómo desarrollar algoritmos que pudieran aprender de forma autónoma a partir del conocimiento existente, tal como lo hacen los humanos (Turing, 2010, p.22). Desde entonces, el desarrollo de la inteligencia artificial ha pasado por diversas etapas, enfrentándose a períodos de auge y estancamiento.

En los últimos años, el avance del "big data", el aprendizaje profundo y las redes neuronales ha impulsado la IA a convertirse en uno de los campos más populares de investigación. Esta tercera ola de desarrollo ha atraído la atención de diversas disciplinas, desde las ciencias naturales hasta las ciencias sociales, incluida la filosofía, la ética, la sociología y el derecho (Laney, 2001, p.1).

La inteligencia artificial ha sido un campo de estudio que ha evolucionado rápidamente desde mediados del siglo XX. Como ya se indicó uno de los primeros antecedentes se encuentran en los años 50, cuando Alan Turing y otros pioneros comenzaron a sentar las bases de lo que hoy conocemos como IA. Marvin Minsky, uno de los padres la definió como "la ciencia de construir máquinas para que hagan cosas que, si las hicieran los humanos, requerirían inteligencia" (Turing,

2010, p.22). Desde entonces, se ha ido integrándose en múltiples campos, desde la medicina hasta el sector empresarial, con capacidades cada vez más avanzadas para imitar el razonamiento humano.

En los últimos años, el desarrollo de la IA ha alcanzado niveles impresionantes, siendo capaz de realizar tareas especializadas que ni siquiera el ser humano puede ejecutar con la misma precisión. Esto ha llevado a que esta herramienta se encuentre en una amplia variedad de escenarios, desde robots quirúrgicos que realizan intervenciones médicas, hasta sistemas autónomos que toman decisiones sin intervención humana. Sin embargo, esta evolución también ha planteado desafíos éticos y legales, especialmente en relación con su potencial para cometer delitos cibernéticos (Martínez Quirante & Rodríguez, 2020, p.1).

La IA se clasifica en varios tipos, dependiendo de su complejidad y autonomía. Entre los principales se encuentran: IA Reactiva: Es el tipo más básico de inteligencia artificial. Solo responde a estímulos directos del entorno sin capacidad de aprendizaje o almacenamiento de experiencias previas. IA de Memoria Limitada: Este tipo de sistema puede tomar decisiones basadas en datos históricos limitados, pero no almacena experiencias a largo plazo (Hintze, 2016, p.1).

IA de Teoría de la Mente: es un concepto aún en desarrollo que se refiere a sistemas capaces de comprender pensamientos, emociones y expectativas humanas. Esta herramienta puede tener autoconciencia, este tipo de IA, también teórico, implica que la máquina tenga un nivel de autoconciencia y comprensión de sí misma, similar al de los humanos (Hintze, 2016, p.1).

Además de estos, se identifican cuatro tipos particulares de IA en función de su nivel de intervención y capacidad de decisión: IA Asistida: Colabora en la realización de tareas, acelerando

procesos mediante el uso de datos y algoritmos. IA Automatizada: realiza tareas rutinarias y administrativas sin intervención humana, como sucede en el sector empresarial (Hintze, 2016, p.1).

IA Aumentada: ayuda en la toma de decisiones basándose en el aprendizaje obtenido de interacciones previas. IA Autónoma: toma decisiones sin intervención humana, como los vehículos autónomos que operan en diversas partes del mundo (Hintze, 2016, p.1).

Ahora bien, en el ámbito del derecho, se ha generado un creciente interés en la responsabilidad de la inteligencia artificial. Los académicos del área han planteado preguntas sobre si los actos autónomos que infringen la ley cometidos por sistemas de IA, fuera del alcance de los programas diseñados y programados, deberían conllevar responsabilidad (Cairo Battistutti, 2011, p.143). Existen dos posiciones principales en este debate: una postura afirmativa que sostiene que la IA avanzada podría ser sujeta de responsabilidad penal, y una postura negativa que argumenta que solo los humanos, ya sea personas físicas o jurídicas, pueden ser responsables penalmente (Brenner, 2013, p.35).

Quienes defienden la postura afirmativa sugieren que, en el futuro, una IA avanzada o un "robot inteligente" que desarrolle autoconciencia y voluntad podría ser considerado responsable penalmente por sus acciones si estas causan daño social significativo. Esta perspectiva reconoce la posibilidad de que, en algún momento, la IA podría ser tratada como un nuevo tipo de sujeto penal, además de los individuos y las empresas (Cairo Battistutti, 2011, p.143).

Por otro lado, los defensores de la postura negativa argumentan que, en la actualidad, la IA carece de los elementos fundamentales para ser sujeta de responsabilidad penal. Señalan que la inteligencia artificial no tiene la autonomía necesaria para tomar decisiones morales o legales, ya que sus acciones siguen estando determinadas por los seres humanos que las diseñan y programan.

Además, la IA no posee la capacidad de autocontrol ni de intención racional, aspectos esenciales en la imputación penal (Brenner, 2013, p.35).

El debate sobre la responsabilidad penal de la IA no solo se limita a la esfera del derecho, sino que también aborda cuestiones filosóficas profundas sobre la naturaleza del conocimiento, la conciencia y el juicio humano. Los críticos de la postura afirmativa argumentan que, aunque la IA avanzada pueda parecer que toma decisiones de manera autónoma, en última instancia, sigue siendo una herramienta desarrollada por humanos y, por tanto, no debería ser considerada responsable penalmente (Brenner, 2013, p.35).

Este debate también se entrelaza con la distinción entre la inteligencia artificial débil y la inteligencia artificial fuerte. La IA débil se refiere a sistemas que realizan tareas específicas sin tener conciencia o voluntad propia, mientras que la IA fuerte, un concepto aún hipotético, se refiere a máquinas capaces de realizar todas las actividades humanas, incluyendo el pensamiento consciente y la toma de decisiones autónoma (Rodríguez Rodríguez, 2018, p.111).

Aunque la inteligencia artificial ha avanzado notablemente y se espera que continúe transformando muchos aspectos de la vida humana, la cuestión de su responsabilidad sigue siendo un tema de intenso debate. Mientras algunos abogan por que la IA avanzada podría asumir responsabilidad penal en el futuro, otros consideran que la IA nunca podrá alcanzar el nivel de autonomía y autoconciencia necesario para ello (Domiguez Peco, 2018, p.247).

Ahora bien, para comprender el marco en el que se inscribe este trabajo, así como los términos técnicos que implica, conviene en primer lugar ofrecer algunas definiciones que permitan entender el funcionamiento de un algoritmo de manera general. Esto nos permitirá comprender mejor la noción de la investigación. Luego, señalaremos y comentaremos algunos riesgos y

desafíos que surgen de aplicar estas herramientas de manera directa sin hacer ningún control humano significativo frente a las respuestas dadas por estas herramientas inteligentes.

Lo primero que hay que indicar es la definición y funcionamiento de estos algoritmos, pues este desarrollo ha permitido el avance en la inteligencia artificial, uno de ellos es big data, el cual se trata de métodos de procesamiento de datos masivos que permiten destacar la información relevante de un conjunto de datos recopilados a gran escala. La cantidad de datos procesados es tan inmensa que se habla de mega datos (Laney, 2001, p.1).

Estos algoritmos big data han permitido la creación de otros, que son un conjunto de instrucciones o un método que permite resolver un problema determinado, dentro de estos algunos pueden desarrollarse con funciones predictivas, es decir, que se especializan en la búsqueda de un dato particular y el registro de las condiciones ambientales de ese dato. Así, estos algoritmos pueden anticipar, analizando los datos proporcionados por los big data y los hechos nuevos, cuál es el desenlace más probable que ocurra en el futuro. Así es, por ejemplo, cómo funcionan las predicciones meteorológicas (Laney, 2001, p.1).

Ahora bien, dentro de estos algoritmos han impactado el mundo jurídico, desde 2016, ha crecido enormemente lo que se llama la era del big data jurídico o “algoritmos jurídicos”. Se trata del análisis de datos jurisprudenciales que permiten extraer información y crear predicciones jurídicas (Legalprod, 2024, p.1).

La inteligencia artificial en el ámbito de la justicia se conoce más comúnmente como justicia predictiva y puede definirse como el análisis de grandes cantidades de decisiones judiciales mediante tecnologías de inteligencia artificial con el fin de construir predicciones sobre el desenlace de los litigios. Dado que la máquina realiza un cálculo de probabilidad y no una

predicción real, sería más adecuado hablar de justicia previsible. Esta justicia predictiva consta de dos vertientes: una vertiente analítica y una vertiente predictiva (Belloso Matin, 2019, p.17).

Estas dos vertientes se diferencian únicamente por su finalidad. Efectivamente, la primera vertiente tiene como objetivo predecir el desenlace de litigios aún no resueltos. La segunda vertiente, por su parte, aspira a predecir el riesgo de reincidencia de un individuo o su peligrosidad. Esta vertiente predictiva puede emplearse no solo en el momento del juicio, es decir, al determinar la pena o al final del proceso otorgar una posible libertad condicional (Frosini, 2019, p.73).

Ya sea en la vertiente analítica o en la vertiente predictiva de esta justicia predictiva, es importante destacar que estos algoritmos funcionan de la misma manera. La idea es, por tanto, analizar decisiones jurisprudenciales anteriores para predecir lo que probablemente se dictará en un caso aún no resuelto, vertiente analítica, o calcular el riesgo de reincidencia de un individuo o su peligrosidad, vertiente predictiva.

Dado que su funcionamiento es similar, englobaremos ambas vertientes en nuestro estudio. Sin embargo, y únicamente en lo que respecta a la cuestión del retorno del pensamiento positivista, solo discutiremos los algoritmos predictivos que son el soporte de lo que se alimentan la IA Generativa o Chatsbots inteligentes, ya que no es tanto el algoritmo en sí lo que plantea interrogantes, sino su finalidad.

Los Riesgos y desafíos de esta justicia predictiva en el ámbito jurídico vas más allá de las implicaciones relacionadas con la compatibilidad o no de ciertos derechos fundamentales con el uso de la herramienta como el ChatGPT o Copilot, si bien, el uso de la tecnología ha logrado materializar una justicia más accesible respecto de la rapidez, el costo y la disponibilidad de la justicia.

Frente a la rapidez podemos indicar que el atraso judicial ha sido un tema sobre la mesa durante años. Los anteriores ministros de Justicia han intentado hacer la justicia más rápida, sin éxito, la lentitud de nuestra justicia sigue siendo un problema crucial en nuestros tribunales (Yepes Gómez, 2021, p.11). Aquí es donde las herramientas tecnológicas bien utilizadas podrían resultar interesantes, ya que algunos consideran que su uso podría permitir tratar más rápidamente lo que ya ha sido juzgado en numerosas ocasiones en casos similares, como la utilización de algoritmos predictivos. En ese sentido la carga de trabajo del juez se aliviaría significativamente, permitiéndole ser mucho más rápido gracias a todas las posibles soluciones al litigio que el algoritmo le proporcionaría.

Además, los abogados podrán utilizar estos algoritmos para calcular las probabilidades de ganar un juicio y, en consecuencia, disuadir a un cliente de proceder si las posibilidades de ganar son demasiado bajas. Los abogados tenderán a acompañar más a sus clientes hacia otras posibilidades, como los métodos alternativos de resolución de conflictos “MARC” (Congreso de la Republica, ley 2220, 2022). Así, habrá menos litigantes ante el juez, y este fenómeno, combinado con la rapidez en los juicios proporcionada por los algoritmos judiciales, permitirá un descongestionamiento considerable de nuestros tribunales.

Ahora bien, frente al costo del procedimiento, el razonamiento también sería establecer que, si los justiciables consideran que no tienen suficientes posibilidades de ganar un juicio, podrían dirigirse hacia los MARC y así evitar un juicio que les resultaría costoso. Además, los algoritmos judiciales permitirán la automatización de una serie de tareas, lo que beneficiará a una reducción del costo total de la justicia. A esto se suma el hecho de que es probable que se abandone la dimensión física del juicio. De este modo, la rama judicial ya no tendrá que alquilar parte del parque inmobiliario en el que actualmente se desarrollan los procedimientos. Todos estos ahorros

podrían generar una reducción en el monto de los gastos procesales, lo que permitiría una mayor accesibilidad a la justicia.

Finalmente, la disponibilidad, a diferencia del juez humano, el algoritmo podrá desempeñar su función de manera casi permanente. Podría imaginarse, con toda probabilidad, una plataforma que permita resolver litigios en línea. De esta manera, las partes interesadas podrán acceder a la justicia cuando lo deseen. Con todos estos elementos, nos parece realista afirmar que la Inteligencia Artificial permitirá efectivamente una mayor accesibilidad a la justicia.

Es fundamental desarrollar herramientas que impulsen la toma de decisiones y generar conocimiento académico que contextualice la inteligencia artificial (IA), la cual se considera parte de la cuarta revolución industrial. Aunque llevamos más de 20 años utilizando tecnología, las características actuales de la IA representan una verdadera revolución. A menudo se genera temor y se especula sobre la sustitución de empleos humanos por máquinas, cuando en realidad estas tecnologías deben verse como herramientas valiosas que potencian tanto la academia como el sector empresarial y el sistema judicial.

La IA permite avances significativos en tareas como la investigación, la conceptualización, la determinación de rutas de análisis y la prevención de la corrupción en los ámbitos económico, financiero y contractual, tanto a nivel nacional como global. Todas las áreas de actividad humana están impregnadas por estas tecnologías, y es esencial aprovecharlas de manera eficaz (Corvalán, 2018, p.301).

En el ámbito contractual, por ejemplo, herramientas tecnológicas como el SECOP permiten acceder de manera ágil a la información, eliminando la necesidad de trámites largos como solicitudes de derechos de petición (Decreto Ley 4170, 2011). No obstante, el uso de estas

tecnologías en la justicia y otras esferas debe realizarse bajo principios éticos, salvaguardando la confidencialidad y la privacidad de las personas.

El uso de herramientas tecnológicas con fines investigativos resulta esencial en el desarrollo de procesos constitucionales, penales y civiles. Estas herramientas permiten avances significativos, pero también plantean desafíos, como la posible vulneración de derechos de autor al utilizar información sin la debida autorización y cita (Aucejo & Ramón, 2023, p.13). Es crucial que la recopilación, almacenamiento y uso de datos se realice con el consentimiento informado de las personas involucradas, aplicando medidas de seguridad como el cifrado para evitar el uso indebido de la información (Aucejo & Ramón, 2023, p.13).

Un tema preocupante es el acceso a la información de menores, lo que demanda una regulación más estricta, especialmente en América Latina. Organismos como la CAF y la OCDE están apoyando a los estados en la creación de estructuras normativas que fijen límites adecuados al uso de la IA y tecnologías emergentes fiables (OCDE, 2022, p.1).

Otro desafío es la congestión judicial, agravada por el aumento de casos sin un incremento proporcional en los jueces y fiscales. Las herramientas digitales, implementadas tras la pandemia, han sido clave para mitigar este problema, como Pretoria en la Corte Constitucional, que facilita la identificación de casos de tutela y su revisión (Corte Constitucional, Boletín No. 128, 2020).

En el ámbito penal, Prisma, creada por la Fiscalía, ha sido útil para conectar casos relacionados con delitos sexuales y contratación pública (Fiscalía General de la Nación, 2018). La Contraloría, a través de DIARI, también utiliza herramientas tecnológicas para controlar la ejecución de contratos y prevenir la corrupción (Decreto Ley 2037, 2019).

#### **4.2 Avances de la legislación europea en IA.**

El Reglamento (UE) 2024/1689 caracteriza las aplicaciones de inteligencia artificial dependiendo del riesgo que significa en su utilización para los humanos o para el medio ambiente, se categorizan principalmente en dos, las que son aceptables, las que significa un riesgo, pero este es medible y debe estar registrado para su control, y las que son inaceptables que en algunos casos su utilización se puede dar bajo criterios excepcionales.

La reglamentación de la Unión Europea exige que las aplicaciones de inteligencia artificial (IA) sean diseñadas de manera responsable. Esto significa que, antes de lanzarlas al mercado, los desarrolladores deben cumplir con ciertos requisitos, entre los cuales se destaca el respeto a los derechos humanos, particularmente los derechos a la intimidad y privacidad (Parlamento Europeo y del Consejo, 2024, p.1).

La regulación no tiene como objetivo frenar la innovación, sino asegurar que cualquier aplicación sea probada exhaustivamente antes de su comercialización. Sin embargo, en el caso de las aplicaciones de procesamiento de lenguaje natural, como los ChatBots, estas no siempre pasan por pruebas exhaustivas. A menudo se lanzan a la red, y los usuarios las prueban asumiendo, bajo su propio albedrío, que tienen suficiente conocimiento para comprender su funcionamiento. Cabe destacar que estas aplicaciones como ChatGPT a veces son poco transparentes y pueden generar “alucinaciones” en un 15% de las respuestas, lo que compromete su confiabilidad (The New York Times, 2023, p.1).

Esta reglamentación está dirigida a los desarrolladores de IA para garantizar que las aplicaciones sean creadas de manera responsable, cumpliendo con la legislación vigente y respetando los derechos humanos y el medio ambiente. No se trata de detener los avances en

investigación, sino de asegurar que estos progresos se ajusten a los principios fundamentales de respeto a la dignidad y los derechos.

El reglamento de la Unión Europea clasifica las aplicaciones de IA en cuatro categorías según su nivel de riesgo: Riesgo mínimo, Estas aplicaciones pueden operar sin mayores restricciones. Riesgo medio, en este caso, se imponen ciertos límites, como el cumplimiento de estándares de transparencia. Por ejemplo, los ChatBots deben informar explícitamente a los usuarios que están interactuando con un sistema basado en IA y no con una persona (Parlamento Europeo y del Consejo, 2024, p.1).

Aplicaciones categorizadas en Riesgo alto están sujetas a criterios estrictos antes de ser autorizadas en la Unión Europea y las Aplicaciones inaceptables las cuales están prohibidas debido a los riesgos insalvables que conllevan (Parlamento Europeo y del Consejo, 2024, p.1).

Además, la reglamentación excluye algunas aplicaciones de IA de estas limitaciones, como aquellas que se utilizan exclusivamente con fines militares o de defensa, así como las destinadas a la investigación o innovación sin fines comerciales.

En el caso de ChatGPT, clasificado como de “riesgo medio o neutro”, debe cumplir con la reglamentación europea, especialmente en términos de transparencia. Estas aplicaciones han sido criticadas por infringir leyes de protección de derechos de autor, lo que las convierte en herramientas que operan fuera del marco legal en algunos casos (Parlamento Europeo y del Consejo, 2024, p.1).

Una de las soluciones propuestas para abordar este tipo de problemas es que las aplicaciones de IA paguen por el usufructo de los derechos de las personas cuyas investigaciones o creaciones están siendo aprovechadas sin compensación (Parlamento Europeo y del Consejo, 2024, p.1). Cada Estado miembro de la Unión Europea debe regular el uso de estas aplicaciones,

garantizando que los usuarios sean conscientes de que los resultados generados por ellas provienen de fuentes públicas, cuya veracidad no siempre está asegurada. Esto afecta directamente el derecho de las personas a recibir información precisa, un derecho consagrado en la Constitución Política de Colombia, que establece la obligación de que la información sea veraz e imparcial (Constitucion Politica, 1991).

Por ahora, la legislación de la Unión Europea es un marco general. Las regulaciones específicas deben seguir para definir con mayor precisión los límites y sanciones por incumplimiento. Hasta la fecha, no existe una ley que determine claramente si un contenido es verdadero o falso, pero es crucial que se regule la creación de contenido en redes, ya que ciertos datos verdaderos pueden ser utilizados para generar noticias o información falsa.

Ahora bien, el uso de datos biométricos está prohibido, salvo cuando sea necesario por razones de seguridad y bajo un estándar de emergencia, como en casos policiales, donde se pueden capturar los rostros de miles de personas con el objetivo de proteger a la sociedad. Esta excepción deberá ser regulada detalladamente, imponiendo controles estrictos, como la autorización judicial para permitir el uso de estas tecnologías, basándose en pruebas de razonabilidad y proporcionalidad y bajo circunstancias de necesidad urgente (Ley 1581, 2012).

Las Tecnologías como Pegasus ya están creadas y en uso en otros países. La cuestión es si deben permitirse su uso en un Estado Constitucional, donde la democracia participativa es esencial, en razón a que la utilización de estas sin control sería una invasión arbitraria a los derechos fundamentales lo que implica establecer límites para su uso, tarea crucial para la legislación doméstica (Amnistia Internacional, 2022, p.1).

Es bien sabido que la tecnología avanza más rápido que las leyes que la regulan. Por ello, el lanzamiento de aplicaciones al mercado debe realizarse de forma responsable, especialmente

cuando estas toman decisiones basadas en datos personales, sin prever claramente los riesgos legales a futuro. Además, las empresas que desarrollan estas tecnologías, con sus grandes recursos económicos, no siempre evalúan los riesgos a los que se puede enfrentar la humanidad debido a su desarrollo (Pont, Angostina Passera, & Castilla, 2022, p.10).

Uno de los principales problemas de las aplicaciones basadas en algoritmos de Deep Learning es su falta de transparencia. Esto implica que, aunque ya estén en uso, es casi imposible hacer completamente transparente el flujo de datos que manejan. Esto plantea un riesgo para los usuarios que interactúan con estas tecnologías (Gómez Llinás, 2021, p.3).

El reglamento de la Unión Europea busca darles a los ciudadanos herramientas para que comprendan que el uso de estas tecnologías está teniendo un impacto significativo en el mundo. No obstante, la efectividad de las regulaciones depende de la implementación de sanciones adecuadas. Si las sanciones son demasiado bajas, las empresas que desarrollan estas aplicaciones podrían no sentir un incentivo real para cumplir con las regulaciones debido a su poder económico.

El reglamento contempla dos tipos de sanciones: un porcentaje del volumen del negocio anual global de la empresa o un valor fijo determinado en millones de euros, eligiéndose el monto mayor según el tipo de infracción. Así, las aplicaciones de riesgo alto reciben las sanciones más severas, mientras que las aplicaciones de menor riesgo enfrentan sanciones más proporcionales (Parlamento Europeo y del Consejo, 2024, p.1).

Finalmente, la Unión Europea muestra especial preocupación por el uso de modelos de lenguaje natural en tareas gubernamentales y sanitarias, ya que consideran que estas aplicaciones no deben utilizarse cuando están en juego derechos fundamentales, como la vida o la libertad, dado que las decisiones tomadas por estos sistemas podrían comprometer gravemente los derechos de los individuos.

### 4.3 Marco ético y legal para la IA en Colombia

Primero, es esencial definir qué entendemos por ética. La consideramos una rama de la filosofía que orienta nuestra reflexión sobre los criterios que utilizamos para determinar lo que es bueno o malo, correcto o incorrecto, justo o injusto, todo ello dirigido hacia el bienestar en nuestra vida cotidiana. Si aplicamos estos principios éticos al ámbito judicial, entenderemos la ética judicial como una herramienta que guía a los profesionales del derecho a tomar decisiones más prudentes y razonadas, basadas en criterios bien establecidos sobre lo correcto, incorrecto, justo e injusto (De Zan, 2004, p.53).

Si codificamos estos principios éticos, dicho código servirá esencialmente como una guía y orientación para el desempeño de actividades en la labor jurisdiccional.

En ese sentido, las tecnologías emergentes presentan grandes oportunidades, pero también plantean significativos desafíos, particularmente en la impartición de justicia. Ya no es novedoso que diversas tecnologías se apliquen en este ámbito; por ejemplo, se utilizan buscadores electrónicos, se desarrollan tesauros, ontologías y sistemas expertos. Un caso dramático es el uso del sistema COMPAS en Estados Unidos, especialmente en el ámbito penal, que evalúa la probabilidad de reincidencia de delincuentes basándose en su historial criminal. Este sistema fue central en el caso de Estados Unidos vs. Loomis en 2016, donde se cuestionó si el uso de COMPAS vulneraba el derecho al debido proceso (p.25).

Este sistema utiliza algoritmos y modelos estadísticos de probabilidad para evaluar la posible reincidencia de delincuentes, basándose en su historial criminal. En el caso de Estados Unidos vs. Loomis en 2016, donde el Tribunal Superior de Wisconsin condenó a Loomis a más de seis años de prisión. Loomis solicitó una reconsideración de la sentencia, alegando que su derecho

al debido proceso fue vulnerado porque el juez basó su decisión en los resultados proporcionados por COMPAS. Sin embargo, el juez aclaró que su decisión habría sido la misma incluso sin haber consultado COMPAS, argumentando que lo utilizó simplemente como una herramienta complementaria. Este caso deja una incógnita sobre si realmente el juez utilizó COMPAS solo como una herramienta o si basó su decisión completamente en él, planteando un desafío ético que persiste desde entonces (Estado de Wisconsin Vs. Eric L. Loomis, 2016, p.20).

Ante estos riesgos, deseo revisar los potenciales beneficios de la inteligencia artificial (IA) en la justicia. La IA puede ser una herramienta crucial para los operadores judiciales, permitiéndoles procesar grandes volúmenes de datos y facilitar el acceso a la justicia. Este uso de la IA no solo podría potenciar derechos fundamentales como el acceso a la educación, la salud, la cultura y la información, sino que también presenta desafíos éticos significativos.

La implementación de la IA en la justicia implica riesgos relacionados con la privacidad, la protección de datos personales y la igualdad, particularmente en términos de sesgos potenciales que podrían llevar a decisiones discriminatorias. Además, la "caja negra" de la IA genera incertidumbres significativas sobre cómo se toman las decisiones, lo que implica desafíos en términos de transparencia y responsabilidad (Wayne Gregory, Henfridsson, Kaganer Evgeny, & Kyriakou , 2021, p.425).

Desde el punto de vista de la regulación, existe un debate sobre cuánto y cómo se debe regular la IA. Se han desarrollado diferentes enfoques, como los de la visión anglosajona y la Unión Europea. Desde 2018, se han hecho esfuerzos significativos en términos de principios éticos y regulaciones, como la Carta Ética Europea sobre el uso de la IA y la Declaración sobre Ética y Protección de Datos de la IA.

El Marco Ético para la Inteligencia Artificial en Colombia establece una serie de principios destinados a guiar el desarrollo y uso responsable de la IA, asegurando que la tecnología avance sin comprometer los valores éticos fundamentales ni los derechos individuales. Estos principios son vitales para la integración efectiva de la IA en diferentes sectores, proporcionando una base sólida para su implementación y operación (Guío, Tamayo, & Gomez, 2021, p.23).

Continuando con Guío, Tamayo & Gómez (2021) Se han identificado varios principios éticos fundamentales para el uso de la IA en la justicia: primero, el principio de Transparencia y Explicación requiere que los sistemas de IA sean abiertos acerca de su diseño, funcionamiento e impacto. La información proporcionada debe ser accesible y comprensible, permitiendo a los usuarios entender cómo interactúan con estos sistemas y cómo son afectados por sus decisiones. Es esencial que esta información sea adaptada a distintos contextos y audiencias para garantizar una comprensión adecuada, especialmente en aplicaciones consideradas de alto riesgo (p.25).

El principio de Privacidad enfatiza la importancia de respetar la intimidad de los individuos, protegiendo sus datos personales y evitando su uso no autorizado. Los sistemas deben permitir que los usuarios corrijan datos incorrectos o desactualizados, garantizando la precisión y la seguridad de la información personal.

En cuanto al Control Humano, Guío, Tamayo & Gómez (2021) expone que los sistemas de IA deben mantener un nivel de supervisión humana adecuado, ajustado al nivel de riesgo de la aplicación. Esto es crucial durante las fases iniciales de implementación y debe mantenerse conforme la tecnología evoluciona, asegurando que las decisiones críticas sean supervisadas adecuadamente (p.28).

Guío, Tamayo & Gómez en su obra indican que la seguridad se centra en proteger la integridad física y mental de los individuos, garantizando que la información personal esté segura

y que los sistemas no generen daños inadvertidos. Se requieren medidas rigurosas para proteger los datos y prevenir alteraciones que podrían comprometer tanto a individuos como al sistema en su conjunto (p.29).

Guío, Tamayo & Gómez frente a la Responsabilidad indican que se encuentra distribuida entre todos los actores involucrados en el diseño y operación de los sistemas de IA. Subraya que deben ser conscientes de los efectos y posibles daños que sus sistemas puedan causar. Este enfoque de responsabilidad compartida es fundamental para asegurar que todos los niveles de la cadena algorítmica sean conscientes y actúen en consecuencia (p.30).

Guío, Tamayo & Gómez frente al principio de No Discriminación busca prevenir resultados que sean perjudiciales o discriminatorios hacia grupos específicos, asegurando que los sistemas de IA funcionen de manera justa y equitativa. La implementación de medidas preventivas y correctivas es clave para eliminar los sesgos en los datos y algoritmos (p.30).

Es de resaltar que en estos avances tecnológicos se debe promover la inclusión como una participación de grupos históricamente marginados en todas las etapas de la IA, desde el diseño hasta la evaluación, garantizando que los sistemas sean accesibles y útiles para todos.

Por último, Guío, Tamayo y Gómez subraya la importancia de que la inteligencia artificial aporte un impacto positivo a la sociedad. Esto incluye la mejora de los servicios públicos y el fomento de una cultura de transformación digital. Asimismo, resulta fundamental que niños y adolescentes comprendan y se involucren activamente en el desarrollo de la IA, lo que les permitirá participar de manera significativa en la formulación de políticas y prácticas que moldearán su futuro (p.32).

Este marco ético no solo proporciona directrices para el desarrollo tecnológico, sino que también refleja un compromiso profundo con la protección y promoción de los derechos humanos en la era digital. Además, propongo agregar dos principios más:

1. Protección de los derechos humanos.
2. Supervisión y decisión humana.

Estos principios subrayan la necesidad de mantener un grado de supervisión humana y de garantizar que la IA no actúe con un nivel de autonomía que comprometa la justicia o los principios éticos.

La IA tiene el potencial de mitigar muchos de los riesgos asociados con los sesgos humanos en la toma de decisiones judiciales. Los principios de independencia, imparcialidad y objetividad, que han sido fundamentales en la ética judicial desde el primer código de ética del poder judicial de la federación en 2004, son especialmente relevantes en el contexto de la IA. Estos principios pueden ayudar a guiar el desarrollo y la implementación de tecnologías de IA en la justicia, asegurando que se mantenga el compromiso con la justicia y la equidad.

Recientemente el Consejo Superior de la Judicatura expidió el acuerdo PCSJA-12243 donde estableció lineamientos para el uso respetuoso, responsable, seguro y ético de la Inteligencia Artificial en la administración de justicia en Colombia. Este instrumento normativo busca garantizar que la adopción de tecnologías basadas en IA contribuya a mejorar el acceso, la eficiencia y transparencia judicial, sin comprometer los derechos fundamentales ni sustituir el juicio racional de los jueces (Consejo Superior de la Judicatura [CSJ], 2024).

Uno de los ejes centrales del acuerdo es la adopción de principios rectores que orientan el uso de la IA en la administración de justicia, entre ellos se destaca la primacía de los derechos

fundamentales, el respeto por la regulación ética, la supervisión humana, la necesidad de explicabilidad y transparencia de los razonamientos utilizados para adoptar una decisión judicial.

Además, el acuerdo trae consigo una prohibición expresa que la IA supla funciones inherentes al ejercicio judicial, como la valoración de pruebas, la motivación de providencias o la adopción de decisiones jurídicas (CSJ, 2024, arts. 3.1, 3.2, 3.6, 3.14 y 3.15).

En cuanto a los usos permitidos, el acuerdo diferencia entre aquellos orientados a la gestión administrativa, como la redacción asistida de oficios, programación de agendas, traducción de documentos y elaboración de presentaciones. Respecto a los usos judiciales no decisorios, como el apoyo en la consulta jurisprudencial, la clasificación de expedientes, el resumen de providencias y la transcripción de audiencias (CSJ, 2024, art. 4.1 y 4.2). estos usos están condicionados a una revisión detallada por parte del funcionario judicial, quien debe verificar la veracidad, completitud y utilidad de los productos generados por la herramienta (CSJ, 2024, art. 9).

Por otro lado, el acuerdo restringe el uso de herramientas de IA para funciones sustantivas, como la solución de caso, la interpretación de hechos y normas, o la motivación de decisiones judiciales. Prohíbe el uso de sistemas que recojan datos sensibles o personales sin control institucional, y se exige que todo uso de sistemas basados en IA generativa cuente con autorización expresa del Consejo Superior de la Judicatura (CSJ, 2024, arts. 5, 8.3, 8.4, 8.6).

El acuerdo también establece que los funcionarios deben realizar un análisis previo de idoneidad antes de usar cualquier herramienta de IA generativa, definiendo claramente el propósito, evaluando alternativas más seguras, conociendo los riesgos y limitaciones de la herramienta seleccionada. Igualmente, se exige que los usuarios se capaciten previamente y comprendan las implicaciones del uso inadecuado de estas tecnologías (CSJ, 2024, arts. 6 y 7).

El acuerdo representa un avance sustantivo hacia una justicia digital más eficiente, se concibe como una herramienta auxiliar de la administración de justicia, sin embargo, la aplicación de herramientas basados en IA se rija por criterios de legalidad, ética, derechos humanos y responsabilidad individual.

### **5. Análisis del Principio de Precaución en la Jurisprudencia del Consejo de Estado**

El principio de precaución debe entenderse, ante todo, como una medida de carácter proteccionista cuyo objetivo es guiar la conducta de las personas, tanto naturales como jurídicas, en prevenir y evitar daños al medio ambiente. Este principio cobra relevancia cuando se evidencian, fundamentan y motivan ciertos aspectos clave, tales como la certeza de la posible ocurrencia de un daño irreversible y la necesidad de limitar o prohibir actividades que generen un impacto ambiental negativo.

Es importante reconocer que la ciencia, al igual que otras disciplinas, tiene una historia y un proceso de construcción propio. Durante mucho tiempo, se mantuvo una diferenciación estricta entre el conocimiento científico y otros tipos de conocimiento, como el histórico o el sociológico. Sin embargo, hoy en día se ha reconocido la autonomía de ambas áreas, lo cual es esencial porque, aunque la ciencia ha emergido como un paradigma central en nuestra vida, también puede ser influenciada por intereses particulares. En ocasiones, estos intereses pueden oscurecer el verdadero objetivo de la ciencia, que es el bienestar general, y alinearse con fines económicos o sectoriales.

El filósofo de la ciencia Michael Serres ilustra cómo los avances científicos se han dado de maneras diversas, a veces por azar, otras por dedicación, y en ocasiones, incluso, desafiando las expectativas y el rigor del método científico. Un ejemplo que trae a colación este debate es el caso del plomo. A lo largo del siglo XX, era conocido que el plomo tenía efectos perjudiciales para la

salud humana. Sin embargo, empresas vinculadas a la industria de la pintura y los pigmentos financiaron a científicos que desacreditaban los estudios que revelaban estos efectos nocivos. Estos científicos argumentaban, con aparente rigor científico, que los estudios no eran concluyentes, que las muestras no eran lo suficientemente significativas o que existían otros estudios con resultados menos alarmantes (Serres, 1998, p.49).

Este ejemplo ilustra cómo el mismo rigor científico fue usado para cuestionar la evidencia clara de un riesgo para la salud humana. En situaciones como esta, se podría haber esperado hasta obtener estudios exhaustivos y representativos a nivel global, lo que habría retrasado la adopción de medidas preventivas. Sin embargo, el principio de precaución surge precisamente para actuar antes de que se logre una certeza absoluta, evitando que se deba esperar al último estudio que demuestre, con total seguridad, el daño potencial al medio ambiente o a la salud humana (Jáuregui, 2013, p.16).

El caso del plomo es emblemático. Según datos recientes, 143.000 personas mueren al año debido a la exposición al plomo, y la UNICEF revela que alrededor de 800.000 niños siguen siendo intoxicados por plomo presente en juguetes, pinturas y otros objetos cotidianos. Esto demuestra que la adopción del principio de precaución es fundamental para proteger la vida y la salud, incluso cuando la ciencia no ha alcanzado una certeza total sobre el nivel de riesgo (Fondo de las Naciones Unidas para la Infancia, UNICEF, 2020, p.1).

La Corte Constitucional recordó que el principio de precaución tiene sus raíces en Alemania, donde comenzó a tomar forma en 1971 con la legislación sobre protección ambiental (Corte Constitucional. Sentencia C-293, 2002). Posteriormente, en 1972, se consolidó con la Declaración de Estocolmo de las Naciones Unidas sobre el medio humano, donde se introdujo el concepto de desarrollo sostenible y se empezó a aplicar este principio de manera más formal

(ONU, 1972, p.1). En la Unión Europea, este principio ha dado lugar a la formulación de 11 principios fundamentales, entre los cuales destacan:

1. Protección de los derechos humanos.
2. Principio de acción preventiva.
3. Principio de corrección en la fuente.
4. Principio de “quien contamina paga”.
5. Principio de conservación y protección.
6. Principio de cooperación internacional.
7. Principio de prevención de daños transfronterizos.
8. Principio de responsabilidad.
9. Principio de evaluación de impacto ambiental.
10. Principio de participación ciudadana.
11. Principio de internacionalización de costos.

A partir de estos principios, surge una amplia gama de lineamientos que guían la política ambiental, desde la prevención hasta la cooperación (Union Europea, 1987, p.1). En la Declaración de Río de Janeiro de 1992 se recogen varios de estos principios, los cuales también se integran en la legislación colombiana, especialmente en la Constitución y en la Ley 99 de 1993. La necesidad de caracterizar y encontrar puntos comunes entre estos principios ha sido fundamental para hacerlos más accesibles y comprensibles. Entre los principios ambientales, podemos destacar dos tipos clave, estructurales y funcionales.

Principios estructurales, que ordenan y especifican el marco ambiental en su totalidad. Estos principios incluyen la globalidad, la horizontalidad, la sociabilidad y la sostenibilidad. Su propósito es recalcar que las acciones que afectan al medio ambiente no se limitan a una localidad

o país, sino que tienen repercusiones globales. De ahí el concepto de pensar global, actuar local (Organización de Naciones Unidas, ONU, 1992, p.1).

La horizontalidad se refiere a la interrelación entre los aspectos naturales, sociales y la ordenación del territorio, lo que es fundamental para garantizar una política ambiental integral. Además, la Asamblea General de las Naciones Unidas ha reconocido la “interdependencia de los derechos humanos y ambientales”, subrayando que estos principios deben ser entendidos no solo como pro hominem, sino como principios a favor de toda la humanidad, incluyendo la solidaridad con las generaciones futuras y la preservación de recursos naturales (Asamblea General de Naciones Unidas, 2013, p.15).

Principios funcionales, que ayudan a resolver tensiones entre derechos aparentemente en conflicto, como el derecho a la propiedad, el desarrollo económico y la protección ambiental. Entre estos principios destacan el de prevención y el de precaución. El principio de prevención busca anticipar y mitigar los daños conocidos, empleando herramientas legales como las evaluaciones de impacto ambiental, las licencias y los planes de manejo. El principio de precaución, por otro lado, se activa en situaciones de incertidumbre científica, como las que se dieron en la lucha para reducir el uso del plomo.

El principio de precaución fue introducido en la Conferencia del Mar del Norte (1987-1990) y luego se reafirmó en la Conferencia de las Naciones Unidas de 1992 y otros tratados internacionales como el Convenio sobre la Diversidad Biológica y el Convenio sobre el Cambio Climático. Este principio está consagrado explícitamente en diversos instrumentos internacionales y en la legislación colombiana, particularmente en el numeral 3 del artículo 3 de la ley 164 de 1994. Su esencia radica en la obligación de no ampararse en la falta de certeza científica como

justificación para posponer medidas eficaces y costo-efectivas que impidan la degradación del medio ambiente (Corte Constitucional, Sentencia C-339, 2002).

En este contexto, la Unión Europea ha abordado este tipo de situaciones desde 1996, como en el caso del Reino Unido y la Comisión Europea, donde se estableció que, ante dudas sobre la relación de una sustancia con el cáncer y sus efectos sobre la salud, las instituciones pueden adoptar medidas de protección sin tener que esperar a una plena confirmación científica del riesgo.

En este sentido, el principio de precaución busca evitar que la falta de certeza se utilice como excusa para trasladar las decisiones difíciles a futuras generaciones, quienes sufrirían las consecuencias irreversibles de la inacción. Como ya fue antes mencionado la aplicación de este principio es el caso del plomo.

Sin embargo, el principio de precaución establece que, aun en ausencia de certeza científica absoluta, es necesario adoptar medidas preventivas para evitar posibles daños graves e irreversibles al medio ambiente y a la salud (Congreso de la Republica, Ley 164, 1994).

En Colombia, aunque existen estudios que respaldan la necesidad de limitar el uso del plomo, las medidas regulatorias no se han implementado de manera efectiva (Ministerio de Salud y Protección Social, 2022, p.1). Esta inacción es precisamente lo que el principio de precaución busca evitar que se sigan usando sustancias tóxicas como el plomo en productos de uso diario, sin considerar las consecuencias a largo plazo. Por ello, fue imperativo que tanto las autoridades administrativas como las jurisdiccionales materializaron este principio y adoptando las medidas necesarias para proteger el medio ambiente y la salud pública, incluso en situaciones donde la certeza científica no es absoluta, fue así como se expidió inicialmente el Código Nacional de Recursos Naturales, Decreto 2811 de 1974, Luego la Constitución política de 1991 y por último la ley 2041 de 2020.

Por un lado, nos enfrentamos a una situación de incertidumbre y a la necesidad de realizar una evaluación científica del riesgo, es decir, contar con al menos algunos elementos que nos alerten sobre una posible afectación al medio ambiente o a la salud. Cuando existe la posibilidad de un daño grave e irreversible, es fundamental que se adopten medidas proporcionales, evaluadas a través de un juicio de proporcionalidad (Corte Constitucional, Sentencia C-703, 2010).

Estas medidas deben permitirnos ponderar hasta qué punto se puede continuar con una actividad o, en su defecto, qué acciones podemos tomar para evitar o mitigar los riesgos. Si el riesgo es mayor, la prohibición de dicha actividad podría ser necesaria. Además, es importante considerar la transparencia de las medidas y la inversión de la carga de la prueba.

No podemos esperar hasta que la extinción de especies, la pérdida de fuentes de agua o daños irreversibles a la salud se materialicen, como está ocurriendo en algunos de nuestros ríos, donde el mercurio utilizado en la explotación ilegal de oro ha generado graves daños ambientales. Este mercurio se transmite a través de la cadena alimenticia, afectando gravemente a las comunidades indígenas que consumen peces contaminados, e incluso transmitiéndose de madres a hijos a través de la leche materna (Jáuregui, 2013, p.16).

Este enfoque también ha sido respaldado por la jurisprudencia europea y la Corte Constitucional colombiana. En la sentencia C-595 de 2010, la Corte señaló que el principio de precaución debe aplicarse en favor del ambiente, bajo el criterio de *in dubio pro ambiente*, es decir, en caso de duda, debe prevalecer la protección del medio ambiente (Corte Constitucional, Sentencia C-339, 2002). De igual forma, en la sentencia C-703 de 2010, la Corte reafirmó que este principio, consagrado en la Constitución y en la Ley 99 de 1993, obliga a las autoridades a prevenir daños y riesgos para la vida, la salud y el medio ambiente.

La Corte también destacó en la sentencia C-449 de 2015 que este principio requiere una postura activa y de anticipación, con el objetivo de prever los riesgos medioambientales futuros y optimizar el entorno natural. En la T-154 de 2013, la Corte volvió a subrayar la importancia del principio *in dubio pro - natura*, enfatizando que es necesario tomar todas las medidas necesarias, aun en ausencia de certeza científica absoluta, frente a una amenaza grave. Además, se recordó que el principio de precaución se aplica cuando hay un daño o amenaza de daño grave e irreversible al medio ambiente o a la salud.

La Corte Constitucional también ha señalado que, ante la falta de certeza científica absoluta, no se puede exigir el máximo rigor de la ciencia para demostrar un riesgo, ya que los riesgos ambientales y de salud son mucho mayores. Esto quedó claro en la sentencia T-365 de 2017, en el caso de la vacuna contra el virus del papiloma humano, donde no existía certeza suficiente sobre los efectos negativos de la vacuna para justificar su prohibición. En lugar de prohibir la vacuna, se optó por evaluar sus beneficios frente a los posibles riesgos.

En cuanto a la aplicación del principio de precaución por el Consejo de Estado, la sala de lo contencioso administrativo, sección primera, proceso 2500-23-27-000-2001-90479-01 de fecha 28 de marzo de 2014 destacó cuatro ideas clave:

Fundamentación en la prudencia: Si hay riesgos y no existe certeza, lo más prudente es no permitir la actividad o hacerlo bajo condiciones más controladas, como en el caso de riesgos medioambientales, medicamentos, tratamientos médicos, nuevas tecnologías, etc. En estos casos, es preferible aplicar el principio de precaución.

Método de gestión de riesgos: El principio de precaución implica gestionar los riesgos de manera que, aun sin una prueba absoluta o una relación causa-efecto clara, se tomen medidas

cuando existan indicios serios de que una sustancia o actividad podría causar daños irreversibles para la salud o el medio ambiente.

Aplicación en un contexto de incertidumbre científica: Este principio se aplica cuando hay dudas sobre la comprensión del riesgo, permitiendo que se adopten decisiones administrativas o judiciales en favor de la protección del medio ambiente y la salud.

Intervención en actividades reguladas: Incluso si una actividad económica está reglamentada y cuenta con permisos, la autoridad administrativa o judicial puede intervenir para proteger la salud y el medio ambiente, aplicando el principio de precaución.

Este principio no responde exclusivamente a la existencia de peligro, sino que requiere al menos un mínimo de certeza, aunque sea insuficiente o incompleta, para adoptar las medidas necesarias. Un ejemplo relevante de su aplicación lo encontramos en la sentencia del 20 de febrero de 2014, donde el Consejo de Estado ordenó la suspensión de la explotación de carbón en el páramo de Pisba hasta que las autoridades ambientales definieran las áreas de protección (Consejo de Estado, Sentencia, 2013-00149-02, 2014).

Otros casos incluyen el auto del 12 de julio de 2018, en el que se protegió una quebrada bajo el principio de precaución debido a la posible contaminación (Consejo de Estado, Sección Primera, Rad. 2007-00292-00, 2018). y la sentencia del 17 de julio de 2018, donde se aplicó el mismo principio en relación con los campos electromagnéticos de las antenas de telefonía móvil cercanas a instituciones educativas (Consejo de Estado, Sección Primera, Rad. 2003-01265-01, 2008). Además, en una sentencia del 26 de noviembre de 2019, el Consejo de Estado reiteró la importancia de su aplicación para prevenir daños en la autorización de proyectos forestales (Consejo de Estado, Sala de Consulta, Rad. 2019-00117-00, 2019).

Estos ejemplos muestran cómo el Consejo de Estado ha venido aplicando el principio para proteger el medio ambiente y la salud pública, aun en contextos de incertidumbre científica.

El principio de precaución se encuentra plenamente incorporado en nuestro ordenamiento jurídico a nivel convencional y forma parte del bloque de constitucionalidad. Este principio es de suma importancia y tiene un carácter vinculante tanto para las decisiones de las autoridades administrativas como para las jurisdiccionales, como son las secretarías ambientales, las secretarías de salud, las corporaciones autónomas regionales y el Ministerio del Medio Ambiente. Además, debido a la interdependencia de los diferentes sectores, es esencial considerar su impacto en otras áreas como el ordenamiento territorial, la minería, el agua potable y la vivienda. El análisis del principio de precaución debe ser transversal y horizontal en todos estos campos.

Este principio es de carácter universal y está presente en numerosos instrumentos internacionales. Ha sido reconocido por tribunales internacionales, como la Corte Internacional de Justicia y los tribunales comunitarios europeos, así como a nivel local en Colombia. En el caso del Consejo de Estado, se ha aplicado en diversas áreas, como la simple nulidad, mediante medidas cautelares, en acciones populares y en casos de reparaciones directas. Un ejemplo reciente es su aplicación en la explotación de carbón en páramos, la explotación de oro y materiales aluviales, hidrocarburos, generación eléctrica y antenas de telefonía móvil.

Para la aplicación efectiva del principio de precaución, la Corte Constitucional, en la sentencia C-293 de 2002, estableció el cumplimiento de cinco elementos. Posteriormente, estos fueron retomados y detallados por el Consejo de Estado, Sección Tercera, en la providencia de Radicación Interna 57819 del 7 de julio de 2022, en la cual se identificaron de la siguiente manera:

1. Identificación de riesgos potenciales, respecto a los cuales existe incertidumbre sobre si se materializarán en el corto, mediano o largo plazo.

2. Los daños posibles deben ser graves, anormales e irreversibles.
3. En situaciones de incertidumbre, la administración debe suspender la actividad en cuestión o negar autorizaciones, concesiones, permisos o licencias.
4. No es necesario contar con todas las evidencias científicas, basta con indicios serios.
5. El principio invierte la carga de la prueba, es decir, quien realice la actividad debe demostrar que los riesgos son infundados o controlados.

Es importante destacar la diferencia entre el principio de precaución y el principio de prevención. La prevención se aplica cuando ya hay certeza de que una actividad genera daños, por lo que se busca mitigarlos mediante planes de manejo y recuperación. En cambio, la precaución se aplica cuando no existe certeza sobre los posibles daños o sus efectos a largo plazo. Un ejemplo es el caso del fracking, donde el Consejo de Estado, mediante la acción de nulidad de varias resoluciones del Ministerio de Minas, aplicó el principio de precaución debido a la falta de certeza sobre los efectos en las aguas subterráneas y el medio ambiente (Consejo de Estado, Sección Tercera, Rad. 57819, 2022).

La Corte Interamericana de Derechos Humanos ha sostenido que, en actividades con riesgos ambientales, las evaluaciones de impacto deben ser concertadas con las comunidades, garantizando el acceso a la información y la supervisión por parte de autoridades independientes (Corte Interamericana Derechos Humanos, Opinión Consultiva 23, 2017, p.22).

Un caso reciente es el uso del método de explotación a través del Fracking, el Consejo de Estado no fue ajeno a esto y emitió una decisión por la Sección Tercera, bajo la ponencia del doctor SÁCHICA, y ahora se cumple dos años de dicha decisión. En ella, la Sección Tercera aplicó el principio de precaución basándose en la ausencia de estudios concluyentes.

Los dictámenes periciales presentados por quienes objetaban las demandas señalaban, en primer lugar, la falta de certeza científica sobre los efectos de la actividad en cuestión. Mientras que, en algunos países, como Polonia, se han desarrollado estudios que sugieren ciertos impactos, en otros, como Argentina, los resultados aún son inciertos, y en otros lugares se ha optado por prohibir estas actividades.

Frente a esta incertidumbre, el principio de precaución fue aplicado de manera razonable, permitiendo que se realicen estudios adicionales bajo condiciones estrictas para medir los impactos reales. Esto permitió al Consejo de Estado tomar decisiones informadas que no solo benefician a un sector económico, sino que también tengan en cuenta el bienestar general del país.

### **5.1 El daño ambiental como escenario complejo en la regulación de tecnologías basadas en inteligencia artificial.**

El título resalta la complejidad inherente a la protección ambiental, un fenómeno que no se limita a una sola rama del derecho, sino que involucra múltiples disciplinas técnicas, científicas y sociales. Este escenario de decisión compleja se refiere a la necesidad de balancear entre la imposición de cargas y los impactos ambientales relevantes, especialmente cuando el Estado impone ciertas obligaciones a los ciudadanos. No todas las cargas pueden ser consideradas excesivas, y no todos los impactos ambientales son conocidos o controlados completamente por el Estado o reconocidos en la jurisprudencia.

El uso de tecnologías basadas en inteligencia artificial introduce un nuevo frente en la gestión del medio ambiente, debido a los potenciales riesgos que estas tecnologías pueden representar. El papel del Estado es fundamental en la regulación de estas tecnologías, y se debe

tener en cuenta tres elementos clave, impacto ambiental, prevención de daños y responsabilidad del Estado.

**Impactos ambientales:** Las tecnologías basadas en IA, al igual que cualquier actividad humana, generan impactos ambientales. Desde el uso de energía para la ejecución de algoritmos hasta la utilización de grandes infraestructuras de datos, todo tiene una repercusión sobre el medio ambiente (WIRED, 2023, p.1). Sin embargo, el ordenamiento jurídico solo reprocha aquellas afectaciones que son excesivas y no permitidas socialmente. En este contexto, el uso de IA puede ser responsable de daños no previstos si no se gestiona adecuadamente.

**Instrumentos de prevención de daños:** existen diversas herramientas de control administrativo, como los estudios de impacto y licencias ambientales, que ahora deben incluir el impacto de las tecnologías emergentes como la IA. El desarrollo de IA en sectores como la minería, la planificación territorial y los servicios públicos debe estar sujeto a estas medidas preventivas, evaluando de forma proactiva los posibles daños futuros.

**Responsabilidad del Estado:** en su rol de regulador y garante del bienestar público, el Estado es responsable de asegurar que las actividades basadas en IA no generen daños ambientales significativos. Esto incluye la adopción de medidas de control, monitoreo y compensación ante posibles afectaciones. La jurisprudencia ha reconocido que la omisión o negligencia del Estado en la prevención de daños le hace responsable, y lo mismo aplicaría en el caso de tecnologías emergentes como la IA (Constitución Política, 1991).

La jurisprudencia sobre responsabilidad del Estado por afectaciones ambientales es clara y establece que este puede ser responsable tanto por sus actos como por sus omisiones. En el contexto de la IA, esta responsabilidad también debe aplicarse a los impactos que las tecnologías puedan tener en el medio ambiente.

Un enfoque de responsabilidad para las tecnologías basadas en IA debe incluir el reconocimiento del daño ambiental puro, cuando la IA contribuye directamente a la degradación del ecosistema, como, por ejemplo, en la gestión de recursos naturales o la sobre explotación de recursos energéticos para alimentar algoritmos de alta complejidad (WIRED, 2023, p.1).

Así como también se debe considerar el daño ambiental impuro que consiste en que las afectaciones indirectas que la IA pueda generar sobre otros derechos, como la salud o la propiedad privada, debido a su aplicación en sectores críticos como la minería o la agricultura, donde sus decisiones automatizadas pueden no tener en cuenta todos los factores ambientales o humanos involucrados.

Un ejemplo ilustrativo es el uso de IA en la gestión de rellenos sanitarios. Si bien esta tecnología puede optimizar la disposición de residuos, también puede generar impactos ambientales negativos si no se maneja adecuadamente. La instalación de rellenos sanitarios ya implica una imposición de cargas sobre las comunidades cercanas, y el uso de IA para mejorar la eficiencia de estos rellenos no exime de analizar los posibles riesgos y daños ambientales.

El Estado debe garantizar que la implementación de IA en estas áreas se realice bajo estrictas medidas de control y compensación a las comunidades afectadas, y en caso de no cumplir con estos requisitos, la responsabilidad recae sobre el Estado.

## **5.2 El Principio de Precaución y su relación con la responsabilidad patrimonial del Estado.**

Desde un enfoque jurídico, el principio de precaución se ha consolidado como una directriz dispositiva orientada a la actuación ex ante frente a riesgos potenciales, sin que sea necesaria la certeza científica absoluta, si bien el principio fue aplicado en el ámbito del derecho ambiental, sin embargo, una vez afianzado ha adquirido un carácter transversal que incide en la estructura de la

responsabilidad patrimonial del Estado. Su consagración jurídica se encuentra en el artículo 191 del tratado de funcionamiento de la Unión Europea, así como en el ordenamiento colombiano, lo encontramos en el artículo 80 de la Ley 99 de 1993 y en reiterada jurisprudencia del Consejo de Estado (Castro Páez, 2021, p. 180; Osorio Alvis, 2021, p. 22).

En el contexto del sistema Interamericano de Derechos Humanos, aunque en principio el principio de precaución no ha sido convencionalizado expresamente, se ha planteado su integración al análisis de responsabilidad internacional del Estado ante omisiones frente a riesgos ambientales inciertos con normas internacionales ambientales (Castellanos Carreño & Castellanos Carreño, 2017, p. 227).

En el escenario de la responsabilidad extracontractual del Estado, este principio impone al Estado la obligación de adoptar medidas protectoras fundadas en la existencia de indicios de amenaza grave o irreversible, aun en contextos marcados por la incertidumbre científica (Castellanos Carreño & Castellanos Carreño, 2017, p. 229). La Corte Constitucional y el Consejo de Estado han interpretado que la omisión de tales medidas puede configurar una actuación antijurídica, susceptible de generar responsabilidad, incluso bajo régimen objetivo como el daño especial, en los que no se requiere demostrar culpa o falla en el servicio, sino únicamente un riesgo conocido y no gestionado adecuadamente (Osorio Alvis, 2021, p. 23).

El principio de precaución se articula como criterio normativo que permite evaluar la diligencia estatal en contextos de incertidumbre, como ocurrió durante la pandemia por COVID-19, donde las decisiones públicas debieron adoptarse sin certeza científica plena, pero sí con indicios suficientes de riesgo (Castro Páez, 2021, p. 185).

Esta lógica planteada por los tratadistas conlleva a que el principio de precaución desde una dimensión exclusivamente preventiva se extiende hacia una función atributiva de responsabilidad, al permitir imputar jurídicamente daños por omisión, sin que sea indispensable una prueba concluyente de causalidad. Un ejemplo de la anterior premisa sea da cuando la instalación de bases militares en zonas pobladas que deviene en objetivo militar de grupos armados ilegales, el Consejo de Estado ha reconocido la responsabilidad estatal bajo el título objetivo de daño especial (Consejo de Estado, 2012).

Desde el plano probatorio, su implementación se flexibiliza frente a la carga de la prueba, permitiendo al administrado alegar la existencia de un riesgo plausible no gestionado, lo cual representa una importante herramienta para la protección de derechos fundamentales como la vida, la salud o el ambiente (Castro Páez, 2021, p. 175).

En ese contexto el principio de precaución se ha consolidado como un eje normativo fundamental para la imputación de responsabilidad patrimonial del Estado en contextos de incertidumbre, obligando al aparato público a realizar una gestión diligente de los riesgos y a una ponderación adecuada de protección, proporcionalidad y prevención.

## **6. Criterios y Condiciones del Principio de Precaución en la Utilización de IA Generativa en Decisiones Judiciales.**

Este apartado examinará la compatibilidad de los algoritmos predictivos, como antecedente de la IA generativa, con las garantías institucionales y procesales que los jueces deben respetar imperativamente. En primer lugar, trataremos brevemente el caso del Juez que utilizó ChatGPT para motivar una sentencia, posteriormente abordaremos la imparcialidad y la independencia que

deben demostrar los jueces. Luego, examinaremos las garantías relacionadas con el juicio, discutiendo la motivación del fallo y la publicidad del procedimiento.

### **6.1 Impacto de la utilización de algoritmos predictivos en Decisiones Judiciales**

Entre las cualidades intrínsecas del juez podemos indicar independencia e imparcialidad, estos dos principios fundamentales están regidos por el artículo 8 del Convenio Americana de Derechos Humanos (CEDH) y el artículo 14 del Pacto Internacional de Derechos Civiles y Políticos. Estos dos principios están intrínsecamente vinculados, pero son distintos.

Además de los artículos citados, la independencia de los jueces también está garantizada por el artículo 228 de la Constitución Política. Puede definirse como la ausencia de subordinación a otros poderes. Se trata de un estatus que protege al juez de cualquier influencia externa o interna que pudiera afectar su decisión. El juez debe ejercer su función con total libertad y sin ninguna presión de ningún tipo (Corte Constitucional, Sentencia SU-174, 2021).

La Inteligencia Artificial - ChatGPT, por su parte, no tiene conciencia del lugar que ocupa en el “equilibrio de poderes” (Louis De Secondat, 1748, p.99). Es decir que no existe riesgo de que sea influenciado, por ejemplo, por los medios de comunicación. La única forma de garantizar la independencia del algoritmo es examinar cómo ha sido programado y quién es el autor de dicha programación.

Nuestra justicia actual enfrenta grandes dificultades estructurales que requieren inversión, por lo que parece poco probable que el Estado invierta por sí mismo en la creación de algoritmos judiciales (Corporación excelencia para la justicia, 2020, p.1). En este caso, estos últimos serían elaborados por el sector privado. El problema que surge es que esta concepción de algoritmos por el sector privado resulta incontrolable para el Estado. Por lo tanto, existiría el riesgo de una

privatización de la justicia. Desde este punto de vista, se podría cuestionar la independencia de estos algoritmos. Los creadores del algoritmo podrían, en el momento de su concepción, decidir sesgarlo, por ejemplo, para servir intereses financieros. Esto implicaría una falta de independencia del algoritmo desde su creación o durante alguna de sus actualizaciones.

Incluso como herramienta de ayuda a la toma de decisiones, la independencia del juez humano se vería comprometida, ya que se temería una insinuación por parte de estos a emitir una decisión contraria a las corrientes jurisprudenciales dominantes. El algoritmo tendría tal influencia sobre el juez que la independencia de este último podría verse potencialmente sesgada.

Si bien la IA de ChatGPT se puede alimentar de estos algoritmos de Big Data para llegar a generar textos e inclusive argumentar decisiones, estos no tienen la capacidad de oponerse a una posible actualización o de determinar si dicha actualización tiene como objetivo ejercer una influencia negativa. Por el contrario, el juez humano tiene la capacidad de reconocer una influencia ya sea positiva o negativa y de impugnar esa influencia que considere perjudicial. Debido a estos hechos, los jueces humanos parecen estar mejor capacitados para garantizar el principio de independencia que la Inteligencia Artificial.

Respecto de la “imparcialidad”, principio que consiste en la neutralidad absoluta del juez con respecto a las partes. Es una cualidad demostrada hacia las partes. Sin embargo, el juez es, ante todo, un ser humano que tiene una historia, valores y emociones que son inherentes a su persona y de las cuales no puede separarse completamente al juzgar un caso (De Zan, 2004, p.53). La IA de ChatGPT como una arquitectura de red neuronal que generan modelos predictivos se presentan aquí como garantes de la imparcialidad, ya que no se verían influenciados por prejuicios o emociones, a diferencia de los jueces humanos. Sin embargo, esta idea de imparcialidad absoluta de esta tecnología de IA debe ser relativizada.

El principio de imparcialidad se descompone en dos componentes, “la objetiva y la subjetiva”. La imparcialidad objetiva se puede definirse como factores objetivos, perceptibles, observados por las partes o el público, o conocidos por ellos. La idea es que cuando estas circunstancias externas son tales que existe la posibilidad de que el juez o el perito esté predispuesto, no importa si lo está realmente, ya que cualquier juez que se encuentre en tal situación debe apartarse en interés de la confianza del público en la administración de justicia (Corte Constitucional, Sentencia SU-174, 2021).

Las partes y el público deben estar convencidos de que el juez es imparcial, y esto se logra respetando el principio de transparencia. El proceso de creación del fallo debe ser accesible al público. En nuestra justicia actual se han implementado varias obligaciones, además de la obligación de imparcialidad, para consagrar esta transparencia de la justicia, como la publicidad del procedimiento y la motivación de la decisión. Estas dos garantías serán abordadas más a fondo posteriormente en el presente trabajo.

Hay que partir ChatGPT como herramienta de IA no tiene emociones y es indiferente a las partes y a su entorno. Sin embargo, como se explicó anteriormente, la transparencia de estos algoritmos es cuestionable debido a que sus creadores se escudan en el secreto de fabricación.

Por esta razón, el funcionamiento de esta arquitectura de red neuronal es demasiado opaco para las partes, y estas no pueden comprender el proceso de creación del fallo en lo que respecta a la publicidad del procedimiento ni el razonamiento que sigue y los algoritmos utilizados para llegar a una decisión concreta, la motivación del fallo. Sin esta transparencia en cuanto a la publicidad del procedimiento y la motivación de la providencia, es imposible para las partes establecer una apariencia de imparcialidad del sistema. Las partes y el público carecerán de elementos objetivos en los que basarse para confiar en la imparcialidad del juez.

Frente a la imparcialidad subjetiva, por su parte, puede definirse como la presunción de inocencia hasta que se demuestre lo contrario, exige que, en un caso en el que deba fallar, el juez no tenga ni prejuicios ni inclinación alguna, ni que tenga interés en el resultado del mismo. Esta cuestión de la neutralidad está estrechamente vinculada al respeto del principio de “igualdad y no discriminación”, que se desarrollará más adelante (Constitucion Politica, 1991).

Es importante recordar que el sistema denominado ChatGPT no son tan neutrales como parecen en razón a que los datos de donde se alimentan de manera aleatoria de opiniones, trabajos científicos en la red, conceptos derivados de la sociedad de la información en el ciberespacio, Big Data, algoritmos predictivos entre otros; además que siempre dependen de los prejuicios de sus creadores (Bowman, 2023, p.3). El sistema en sí mismo lo es, pero las reglas impuestas por los creadores no lo son. Así, como por ejemplo los algoritmos que busca información en un gran número de jurisprudencias anteriores para emitir su decisión, puede reproducir decisiones parciales y/o discriminatorias si las jurisprudencias analizadas lo eran, debido a las elecciones hechas por sus creadores. Además, el algoritmo no corregirá la parcialidad de las jurisprudencias, sino que la acentuará, a diferencia del juez humano, que puede tener en cuenta la posible parcialidad de las decisiones que analiza y corregirla.

En conclusión, podemos decir que la imparcialidad absoluta de esta arquitectura de ChatGPT es un mito y puede ser objeto de diversas críticas. Aunque algunas de estas críticas también se pueden dirigir a los jueces humanos, se puede pensar legítimamente que estos errores de imparcialidad se limitarán a unas pocas excepciones en los jueces humanos, mientras que se volverían sistémicos debido al fenómeno de uniformidad derivado de la alimentación de datos producidos por los algoritmos de consulta y análisis jurisprudencial generado por estos.

Frente a las cualidades intrínsecas del fallo, es decir la motivación y la publicidad se puede decir que la motivación del fallo está garantizada por el artículo 228 de la Constitución. También está implícitamente garantizada por el artículo 8 del Convención Americana de Derechos Humanos (CADH). En materia penal, dado el impacto que puede tener la pena sobre el procesado, posible privación de libertad, esta motivación debe ser más elaborada, debe ir más allá de la exigencia general de motivación prevista por el artículo 228 de la Constitución. Se habla de motivación especial de las decisiones penales artículo 446 de la ley 906 de 2004, en otros códigos se dispone el artículo 280 de la ley 1534 de 2012 y el artículo 187 de la ley del 1437 de 2011.

Se trata de una garantía para las partes contra la arbitrariedad del juez. La obligación de motivación del fallo consagra y extiende el principio de transparencia de la justicia, esta motivación debe permitir a las partes comprendan objetivamente la decisión del juez y este basado en elementos que se acerquen a una verdad material. Por lo tanto, las sentencias deben redactarse en un lenguaje claro, preciso y pertinente.

Para establecer una posible compatibilidad de los algoritmos predictivos como fuente de la arquitectura de IA con el principio de motivación, es necesario distinguir entre los casos judiciales denominados simples y los casos denominados complejos.

En los casos simples se caracteriza por la aplicación de una norma tan precisa que el margen de maniobra del juez es muy limitado. Estos casos corresponden a un silogismo judicial relativamente simple. Por ejemplo, en materia penal, algunas infracciones de tráfico, donde basta con constatar un exceso de velocidad, 80 kilómetros, en una zona escolar y aplicar la norma que sanciona dicho exceso.

Esto funcionará como un juez humano, ya que ambos deben limitarse a aplicar las normas preestablecidas correspondientes, sin margen de maniobra. Además, dado que el caso es simple,

este tipo de algoritmo es capaz de establecer las reglas en las que se ha basado para producir la decisión, así como las diferentes etapas de aplicación de dichas reglas. Por lo tanto, la motivación de los algoritmos para este tipo de caso no plantea problemas, siempre que esta sea comprensible para las partes.

Los casos complejos se caracterizan por la aplicación de reglas más abstractas, donde el juez dispone de un mayor margen de maniobra y debe equilibrar diferentes intereses. Es el caso, por ejemplo, cuando un juez debe considerar las particularidades del caso judicial en concreto para determinar si una conducta constituye o no una falta, ya que esta noción no está claramente definida en el texto legal, o cuando la ley autoriza explícitamente al juez a fallar en equidad.

Para estos casos, los sistemas de IA no pueden integrar directamente las reglas porque no son lo suficientemente precisas. El tipo de algoritmo utilizado en este tipo de caso, llamado red de redes neuronales artificiales, se basa en una gran cantidad de jurisprudencias, y su decisión se fundamentará en el análisis de esas jurisprudencias anteriores y similares al caso en cuestión.

Sin embargo, y a diferencia de los sistemas expertos, este algoritmo no puede explicar las diferentes etapas de su razonamiento ni las reglas utilizadas para llegar a la decisión. Simplemente realiza un cálculo de probabilidad basado en jurisprudencias anteriores relacionadas con el caso tratado.

Para los casos complejos, el razonamiento es, por tanto, totalmente opaco para las partes, y no se respeta el principio de motivación del fallo. Dado que la gran mayoría de los casos penales y administrativos son complejos y pertenecen al ámbito de la justicia distributiva, el algoritmo no podrá motivar su decisión en la mayoría de estos casos.

Frente a la publicidad del procedimiento está garantizada por el artículo 228 de la Constitución, así como por el artículo 8 del Convenio Europeo de Derechos Humanos (CADH).

Aquí también, al igual que con el principio de motivación del fallo, la publicidad del procedimiento permite garantizar la transparencia de la justicia. Permite que los procesados confíen en la justicia. Existen excepciones a este principio. De hecho, si las circunstancias excepcionales lo requieren, se puede decretar el juicio a puerta cerrada. La publicidad del procedimiento se divide en dos componentes, la publicidad del pronunciamiento y la publicidad de los debates.

En cuanto a la publicidad del pronunciamiento, las cosas son relativamente simples. La decisión puede pronunciarse válidamente a través de canales digitales (sitio web, etc.), y no es necesario que el pronunciamiento sea oral. Por lo tanto, la publicidad del pronunciamiento no plantea, en principio, ningún problema para este sistema de IA, ya que este es capaz de emitir su decisión públicamente a través de medios digitales.

En lo que respecta a la publicidad de los debates, la situación es más complicada, ya que en un escenario del juez electrónico esta es completamente suprimida, dado que no hay audiencia, pues lo que indica es que no se argumenta frente a la máquina. Por lo tanto, existe inevitablemente una contradicción entre principio de publicidad de los debates y la ausencia de debates inherentes a la inteligencia Artificial. Sin embargo, existen excepciones a la publicidad de los debates.

En los casos en que se pueda aplicar una excepción, el sistema autónomo podría juzgar con total validez no siendo necesaria la publicidad de los debates. Pero, dado que estas excepciones son muy limitadas, sería muy difícil aplicarlas a cada caso que la IA trate para que este pueda juzgar válidamente a puerta cerrada. Para los casos, que son mayoría, donde no se pueda exigir la excepción de juzgar a puerta cerrada, será obligatorio recurrir a un juez humano, con debates públicos. Por lo tanto, los algoritmos predictivos en el ámbito judicial plantearán un problema con la publicidad de los debates en la gran mayoría de los casos que trate, ya que el juicio a puerta cerrada no será válido.

## **6.2 Inteligencia Artificial y la violación de derechos fundamentales de las partes procesales**

En un contexto donde se requiere definir problemas y buscar soluciones de manera autónoma, la incertidumbre y el riesgo asociados a la tecnología han aumentado, lo que ha conllevado a que la aceptación de los riesgos tecnológicos se convierta en un tema crucial en el ámbito del derecho. En la medida que surjan situaciones de riesgo tecnológico no intencionadas, no previstas y coloquen en peligro derechos fundamentales, es el momento que surge el debate de cómo abordarlos y cuál sería la resolución al problema jurídico en el ordenamiento vigente al momento de su ocurrencia.

En este aparte se tratará sobre las consecuencias que la Inteligencia Artificial y algoritmos predictivos podría generar en los procesados. Examinaremos la compatibilidad de ciertos derechos fundamentales que enmarcan en el proceso penal y que pueden ser invocados por los procesados con los algoritmos avanzados predictivos y generativos. Luego, analizaremos un caso práctico que nos permitirá comprender los desafíos en la justicia actual y en los procesados de manera más concreta.

Abordamos el estudio de tres garantías fundamentales que la justicia debe asegurar a los procesados. Primero, discutiremos el principio de individualización de las penas, luego, abordaremos el principio de igualdad de armas. Finalmente, analizaremos el principio de igualdad y no discriminación.

El principio de individualización de las penas permite al juez adaptar la sanción de un condenado, así como sus modalidades de ejecución, para tener en cuenta la personalidad del autor de un delito o de las circunstancias de su ocurrencia. Este principio es aún más importante en materia penal debido a la gran cantidad de criterios que intervienen en la determinación de la pena,

algunos de ellos dispuestos en los artículos 59, 60 y 61 del Código Penal Colombiano. Se opone a la aplicación de penas automáticas, es decir, una pena sin adaptación a las circunstancias del delito y la personalidad del autor.

No obstante, si los algoritmos predictivos al considerar la jurisprudencia y ser fuente de herramientas de IA procederían a una generalización de la individualización de las penas, ya que esta no dependería de la intuición del juez. Según esta tesis, el algoritmo sería más objetivo al considerar todos los elementos que permiten la individualización.

Ahora bien, la IA generativa cuyos algoritmos no permitirían una mejor consideración de la individualidad de cada persona en razón a que cada ser humano es diferente y que ciertos criterios no pueden cuantificarse ni objetivarse, como la actitud del procesado o los eventos del pasado que permiten entenderlo mejor. La función del juez implica necesariamente una parte de subjetividad que permite adaptarse a la individualidad de cada caso, que el sistema IA no puede asumir completamente. Ciertos datos no pueden ser informatizados, y eso es lo que hace singular la labor del juez.

Finalmente, consideramos que la IA generativa y predictiva no garantiza una transparencia efectiva de la justicia. De hecho, como vimos anteriormente, los algoritmos no permiten un respeto suficiente de los diferentes componentes que consagran una justicia transparente. Sin embargo, esta transparencia es indispensable para respetar el principio de individualización de la pena, respaldado por la primera tesis. Por lo tanto, a la luz de estos elementos, nos parece más realista decir que la utilización de la IA de manera directa para adoptar una decisión sin control significativo humano, el Juez Penal, no permite un respeto suficiente del principio de individualización de las penas.

Por otro lado, el artículo 8 de la CADH define el principio de igualdad de armas como derivado del derecho a un juicio justo y como un equilibrio justo entre las partes, cada uno debe tener una oportunidad razonable de presentar su caso en condiciones que no lo coloquen en una situación de desventaja significativa en comparación con su o sus adversarios (Organización de Estados Americanos, 1969).

La falta de comunicación de pruebas a la defensa y el acceso limitado a su expediente o a otros documentos de interés público pueden constituir una violación del principio de igualdad de armas. La Corte Constitucional añade que el principio de igualdad de armas que tiene por objeto garantizar que el acusador y el acusado tengan a su alcance posibilidades reales y ciertas para ejercer sus derechos y las herramientas necesarias para situarse en un equilibrio de poderes y hacer respetar sus intereses (Corte Constitucional, Sentencia C - 127, 2011).

Como vimos anteriormente, la transparencia de los algoritmos es deficiente. Sin esta transparencia, es imposible para las partes comprender y tener acceso a todos los elementos de prueba y observaciones presentadas de manera que orienten la decisión del Juez Electrónico. Esta opacidad de los algoritmos, por tanto, no permite el respeto del principio de igualdad de armas.

Además, existe el riesgo de que las empresas privadas desarrollen herramientas informáticas que solo los más ricos puedan permitirse. Cuanto más adinerado sea un bufete o una persona, más podrá invertir en herramientas informáticas avanzadas. En este escenario, el procesado que no pueda permitirse este tipo de herramientas estaría en una situación de clara desventaja debido a su fragilidad económica, lo que va en contra del principio de igualdad de armas. Sin embargo, este tipo de problema no es nuevo ni exclusivo del desarrollo de la inteligencia artificial en el ámbito de la justicia. Además, el modo digital de resolución de litigios implica que

cada persona tenga el equipo adecuado, así como un conocimiento informático suficiente para utilizar estas herramientas.

Estas dificultades que puede enfrentar una de las partes no necesariamente constituyen una violación del principio de igualdad de armas, siempre que se garantice el acceso a un juez humano. En efecto, es el juez quien debe prestar especial atención a estas situaciones de desventaja significativa en cuanto al acceso o uso problemático de las tecnologías por una de las partes, para no favorecer a una parte sin respetar el principio de igualdad de armas. Por lo tanto, la IA generativa y predictiva en la rama judicial, por ahora, no puede resolver un caso por sí solo respetando este principio. Si el algoritmo juzga un caso en el que existe un claro desequilibrio entre las partes, será incapaz de prestar la atención necesaria a dicha desventaja.

Al igual que con otras garantías fundamentales estudiadas anteriormente como la individualización de la pena y la publicidad de los debates, los procesados podrán impugnar la decisión del juez electrónico mediante la organización de un recurso ante un juez humano. Existe aquí una contradicción entre la supuesta infalibilidad del algoritmo, que reemplazaría al juez humano por ser más eficiente, y la organización de un recurso ante este último. Si suponemos que el algoritmo es más eficiente que el juez humano, cual es la razón de organizar un recurso ante este, una incoherencia evidente. Además, esto generaría una carga adicional en el proceso judicial para obtener una decisión conforme a los derechos fundamentales exigidos en un juicio penal.

Frente al principio de igualdad y no discriminación está garantizado por los artículos 13 de la Constitución, el artículo 24 del CADH, así como el artículo 14.1 del Pacto Internacional de Derechos Civiles y Políticos. La discriminación puede ser directa o indirecta. Se dice que una discriminación es directa cuando la situación en la que una persona es tratada de manera menos favorable debido a su sexo, origen, estado de salud, u otros criterios, que otra persona que no lo

es, no lo ha sido o no lo sería en una situación comparable (Corte Constitucional, Sentencia T-909, 2011).

La discriminación indirecta, por su parte, se define como una medida neutral, pero que desfavorece particularmente a un grupo de personas en función de un criterio ilegal de discriminación, que no está objetivamente justificado por un fin legítimo y cuyos medios para alcanzar dicho fin no son necesarios ni adecuados (Corte Constitucional, Sentencia T-909, 2011). A pesar del mito de la neutralidad absoluta de los algoritmos, estos dos tipos de discriminación directa e indirecta podrían ser producidos o reproducidos a través de la IA.

Es importante recordar que los algoritmos que integran jurisprudencias anteriores y se basan en ellas, así como en hechos nuevos, para tomar decisiones. Sin embargo, como vimos anteriormente, el diseño del algoritmo no es neutral, ya que depende de las elecciones de sus creadores. Así, un diseñador con prejuicios puede, consciente o inconscientemente, incorporar esos prejuicios en el algoritmo. Este último reproducirá dichos prejuicios, e incluso los reforzará.

Este es el caso, por ejemplo, del software COMPAS en Estados Unidos. Este algoritmo fue diseñado para calcular el riesgo de reincidencia de los individuos. Sin embargo, calculaba un riesgo de reincidencia mucho más alto para los afroamericanos que para el resto de la población. Al analizar las jurisprudencias integradas por su creador, el algoritmo perpetuó los prejuicios raciales de Estados Unidos y estableció una correlación entre el color de la piel y un mayor riesgo de reincidencia (Guanche, 2023, p.1).

Además, es importante recordar que incluso la agregación de elementos aparentemente neutros puede, en la práctica, generar discriminación. Tomemos como ejemplo la dirección del domicilio en la nomenclatura urbana de una ciudad, que es un elemento totalmente neutral, pero que puede correlacionarse con zonas donde la criminalidad es más alta, donde hay mayor pobreza,

etc. El algoritmo, en este caso, podría tomar decisiones discriminatorias al establecer vínculos entre el código postal y la comisión de un delito, sin que esto sea intencional. Incluso si el algoritmo hubiera sido diseñado sin prejuicios, existiría un riesgo de discriminación.

Por lo tanto, existen grandes reservas sobre la capacidad de la IA, particularmente algoritmos generativos y predictivos para garantizar el respeto del principio de igualdad y no discriminación. También es cierto que el respeto absoluto de este principio tampoco está garantizado por los jueces humanos. Sin embargo, al igual que con la cuestión de la imparcialidad, podemos pensar legítimamente que las decisiones discriminatorias serían limitadas a unos pocos casos en los jueces humanos, mientras que se volverían sistémicas para los algoritmos, y estos últimos las reforzarían en lugar de eliminarlas.

### **6.3 Análisis del caso práctico: el caso Loomis vs. Wisconsin**

Los hechos ocurrieron la noche del 11 de febrero de 2013 en "La Crosse", una pequeña ciudad de Wisconsin, en los Estados Unidos. Esa noche, se produjo un tiroteo en el pequeño pueblo de Wisconsin, a raíz de esto se inició una persecución entre un vehículo policial y un vehículo conducido por Eric Loomis el cual terminó en un accidente. El señor Loomis fue arrestado por la policía. Sin embargo, no había ninguna prueba formal de que él fuera el responsable del tiroteo. A pesar de ello, el Estado de Wisconsin lo acusó de ser el culpable de dicho tiroteo. El señor Loomis negó formalmente los hechos, reconociendo únicamente el intento de fuga y la conducción de un vehículo robado.

Antes del juicio, el juez encargado del caso solicitó la redacción de un informe de Investigación Previa a la Sentencia. Este informe contenía la evaluación del riesgo de reincidencia del señor Loomis, basada en el resultado del software COMPAS, un algoritmo que permite calcular

el riesgo de reincidencia de un individuo y su peligrosidad; implementación del aspecto predictivo (Corte Suprema de Wisconsin, 2016).

En primera instancia, el señor Loomis fue condenado a 8 años y medio de prisión. Apeló ante la Corte de Apelaciones del Cuarto Distrito del Estado de Wisconsin, que también lo declaró culpable, pero redujo su condena a 6 años de prisión. La sentencia fue muy severa, ya que, en la determinación de la misma, el juez tuvo en cuenta el resultado del algoritmo COMPAS, que evaluaba una alta probabilidad de reincidencia en el caso del señor Loomis quien ya había sido condenado en 2002 por agresión sexual. Finalmente, tras su condena en apelación, el señor Loomis presentó una moción ante la Corte Suprema del Estado de Wisconsin para impugnar el uso del software en la determinación de su pena.

En esta moción presentada ante la Corte Suprema del Estado de Wisconsin, el señor Loomis solicitó que la Corte se pronunciara sobre si se había violado su derecho a un juicio justo, así como el principio de igualdad y no discriminación.

De lo anterior se procede Abordar varias de estas cuestiones, así como el principio de igualdad y no discriminación específicamente en el caso de Loomis. Esto nos permitirá poner en práctica el análisis teórico de estas garantías fundamentales estudiadas a lo largo de este trabajo.

Sea lo primero e indicar que los diseñadores del algoritmo COMPAS, escudándose en el secreto comercial, no revelaron el funcionamiento interno del algoritmo ni al juez, ni a las partes. El creador del algoritmo en este caso, la empresa Northpointe, consideró que el secreto comercial que había desarrollado debía ser protegido de sus competidores, quienes podrían apropiarse de él y explotarlo sin su autorización. Los intereses financieros en juego son enormes, y Northpointe, por lo tanto, no puede permitirse revelar el funcionamiento interno del algoritmo, ya que correría el riesgo de perder mucho dinero (Corte Suprema de Wisconsin, 2016).

Para justificar esta falta de transparencia, la empresa Northpointe también argumenta que, si los delincuentes tuvieran en su poder el manual de funcionamiento interno del algoritmo, manipularían sus respuestas para obtener un bajo riesgo de reincidencia. Esto haría que, en última instancia, el algoritmo sea ineficaz.

La falta de transparencia del algoritmo está perfectamente representada y asumida por la empresa Northpointe. Aunque los argumentos presentados por la empresa pueden ser comprensibles y aceptables, no cambia el hecho de que este principio fundamental, derivado del derecho a un juicio justo, no es respetado por el algoritmo COMPAS. El señor Loomis no podrá entender cómo ni por qué el algoritmo llegó a tal decisión, lo que constituye una violación de este componente del derecho a un juicio justo.

Además, el principio de igualdad de armas tampoco se respeta. De hecho, la opacidad del algoritmo resulta en la ocultación de pruebas determinantes para el resultado del litigio. Esta ocultación es, como se mencionó antes, contraria al principio de igualdad de armas. No hay manera para el acusado de impugnar ciertos elementos probatorios derivados de esta evaluación, y ni siquiera el juez puede explicar cómo el algoritmo llegó a esa decisión. La falta de transparencia del algoritmo genera una violación del principio de igualdad de armas, que también deriva del derecho a un juicio justo.

Para evaluar su riesgo de reincidencia, el señor Loomis tuvo que responder a un cuestionario de 137 preguntas. Todas las preguntas fueron diseñadas por los creadores del algoritmo COMPAS, y no por el juez encargado del caso. Dado que la elección de las preguntas no puede ser controlada por los jueces, existe claramente una privatización de la justicia y, por lo tanto, un riesgo de violación a la independencia de la justicia si la empresa privada decide sesgar el algoritmo en favor de sus propios intereses.

El juez, por supuesto, es libre de tomar decisiones, el algoritmo aquí es solo una herramienta de apoyo a la decisión, pero debe poder desvincularse con total tranquilidad del resultado proporcionado por el algoritmo, si lo considera prudente. Si esto no es posible, su juicio estaría parcialmente sesgado y su independencia podría verse comprometida.

En el formulario que tuvo que completar, el señor Loomis, por ejemplo, tuvo que responder preguntas relacionadas con su situación familiar y financiera. Estas preguntas pueden parecer neutrales, pero parece inevitable que el algoritmo establezca correlaciones entre las respuestas a estas preguntas y el riesgo de reincidencia.

Efectivamente, como se mencionó anteriormente, los algoritmos dependen siempre de las decisiones de sus creadores. En este caso, Northpointe tuvo que establecer, además de los criterios en los que se basaría para evaluar el riesgo de reincidencia, qué correlaciones se considerarían positivas, riesgo de reincidencia bajo, y qué correlaciones se considerarían negativas, riesgo de reincidencia más alto. De manera consciente o no, el creador va a integrar elecciones morales en el algoritmo, y el algoritmo reproducirá estas elecciones. Así, el algoritmo podría concluir, por ejemplo, que las personas con una situación financiera complicada tienen un mayor riesgo de reincidencia que una persona con estabilidad financiera.

Por lo tanto, podemos deducir de estos hechos que el algoritmo COMPAS no es imparcial y carece de objetividad. Sin intervención humana, no puede ser totalmente neutral y objetivo en los casos que trate.

Siguiendo con esta idea de neutralidad, la compatibilidad del algoritmo COMPAS con el principio de igualdad y no discriminación plantea interrogantes. En efecto, hemos visto que los algoritmos nunca son neutrales y que siempre dependen de los prejuicios de sus creadores.

Algunas personas se tomaron el tiempo de analizar los resultados proporcionados por el algoritmo COMPAS en comparación con la tasa real de reincidencia observada durante un período de dos años. El resultado es claro: el algoritmo COMPAS calcula un riesgo más alto de reincidencia para los afroamericanos que para el resto de la población estadounidense.

En su cálculo de reincidencia, el algoritmo COMPAS reproduce los prejuicios raciales que han estado arraigados en la sociedad estadounidense durante años. A diferencia de un juez humano, no podrá desvincularse de ellos. Debido a su falta de neutralidad, el algoritmo COMPAS no permite, en este caso particular, respetar el principio de igualdad y no discriminación.

Como quedo expuesto en este análisis, podemos afirmar que este caso demuestra una serie de problemas que generan los algoritmos judiciales en relación con el respeto de las garantías fundamentales del proceso penal. Este estudio casuístico nos ha permitido observar cómo, de manera concreta y práctica, estos problemas, abordados de forma teórica a lo largo de este trabajo, se articulan con la justicia penal. Indiscutiblemente, en este caso existen deficiencias algorítmicas que no permiten una administración efectiva de la justicia.

Lo anterior se debe a la postura que se adopta el país frente a los riesgos tecnológicos que para ellos no existen si no está confirmada, lo que implica la utilización de la tecnología en beneficio de la economía y otras áreas. Esta perspectiva se fundamenta en que la gestión del riesgo se hace de manera reactiva en lugar de proactiva, adoptando el principio de que, si los componentes, formas y características ecológicas de una nueva tecnología son similares a los de tecnología existente, se debe prescribir de manera reactiva una vez se haya demostrado el riesgo, lo que no estaría acorde con el principio de precaución que se viene desarrollando en esta investigación.

#### 6.4 Análisis del Caso del Juez laboral de fecha 30 de enero de 2023

Ahora bien, procederemos abordar el caso reciente donde un juez humano utilizó ChatGPT en un fallo judicial, si bien hemos expuesto que la inteligencia artificial puede llegar a ser una herramienta fundamental en la administración de justicia, como se ha visto en casos recientes, donde jueces han consultado herramientas como ChatGPT para resolver cuestiones sobre derechos fundamentales. Sin embargo, es necesario seguir ajustando el uso de estas tecnologías para asegurar que su aplicación respete los derechos y garantías fundamentales (Juez Laboral del Circuito de Cartagena, 2023).

En este caso particular, el juez laboral de Cartagena utilizó ChatGPT para resolver tres preguntas relacionadas con el acceso a tratamiento gratuito para un menor con autismo. Aunque la herramienta ofreció respuestas afirmativas, no brindó una solución definitiva al caso. El papel del juez, más allá de recibir apoyo de estas herramientas tecnológicas, es realizar un análisis profundo de los antecedentes y justificar su decisión conforme a la ley.

El uso de inteligencia artificial en la toma de decisiones judiciales ha generado debates éticos, ya que algunos temen que los jueces deleguen su responsabilidad en estas herramientas. El problema no radica en el uso de la IA, sino en la falta de un análisis independiente por parte del juez, quien debe contrastar la información proporcionada y desarrollar su propia argumentación. En este caso, el juez simplemente transcribió las respuestas de ChatGPT sin un análisis adicional, lo que ha generado críticas, incluso por parte de la Defensoría del Pueblo, que solicitó la revisión de la sentencia.

Este caso ilustra los límites de la IA en el ámbito judicial, ya que, al ser alimentada con información programada por humanos, puede carecer de actualización y ofrecer respuestas incompletas o desactualizadas. La evolución constante del derecho, como lo demuestra el Consejo

de Estado en su jurisprudencia sobre imputación objetiva y subjetiva, subraya la necesidad de que los jueces hagan un análisis continuo y profundo, y no dependan exclusivamente de herramientas tecnológicas.

El caso fue revisado por la Corte Constitucional, la cual exhortó a los jueces de la República a evaluar el uso adecuado de herramientas tecnológicas como ChatGPT y otras basadas en inteligencia artificial (IA). La Corte les instó a aplicar las mejores prácticas, respetar criterios éticos y observar los mandatos superiores, garantizando así los derechos fundamentales, especialmente el debido proceso. Además, recalcó la importancia de asegurar la independencia y autonomía judiciales como garantías indispensables para la vigencia del Estado Social de Derecho y la democracia (Corte Constitucional, Sentencia T - 324, 2024).

El principio de transparencia, que deriva del derecho a un juicio justo consagrado por el artículo 8 del Convenio Americana de Derechos Humanos (CADH), puede definirse como el carácter observable y verificable del proceso judicial. El principio de transparencia también implica el conocimiento del funcionamiento de las herramientas de inteligencia Artificial, particularmente su algoritmo.

En la motivación del fallo, el juez no está obligado a establecer las razones íntimas que lo llevaron a tomar determinada decisión. Partiendo de este postulado, los algoritmos judiciales parecen más transparentes que los jueces humanos, sin embargo, en la práctica, los creadores de estos algoritmos que desarrollan IA como los ChatGPT se escudan en el secreto de fabricación. Esta transparencia algorítmica es indispensable porque, como afirma Jonker & Roger (2024), el algoritmo depende de las decisiones conscientes o inconscientes del creador del sistema, las cuales son menos transparentes ya que generalmente se ocultan detrás de la herramienta. En otras

palabras, el creador del algoritmo ha introducido, de manera consciente o no, ciertos prejuicios en su máquina (Jonker & Rogers, 2024, p.1).

Por lo tanto, la comprensión del funcionamiento interno de un algoritmo es fundamental para entender la decisión que ha tomado y, así, poder eventualmente impugnarla. De lo contrario, no existe ninguna posibilidad de comprender los medios por los cuales se llegó a una decisión X en un caso Y, lo cual es precisamente contrario al principio de transparencia.

Como se explicó anteriormente, los avances tecnológicos se perfeccionan cada día. La vertiente de la Inteligencia Artificial en la justicia implica la adopción de decisiones de información que circula en la web, sin embargo, esta información en algunas ocasiones no tiene fundamento científico y solo son apreciaciones u opiniones en diferentes contextos, lo que implica un alto riesgo a la hora de motivar una sentencia con información generada por la herramienta ChatGPT.

El derecho hoy en día tiene claramente un carácter evolutivo para poder enfrentar y adaptarse a los cambios de la sociedad. El rol creador de la función del juez no debe ser subestimado. A veces, gracias a los jueces, el legislador se da cuenta de que normatividad debe cambiar y evolucionar, o surgen ciertos principios generales del derecho como el estado de necesidad, por ejemplo, es una creación jurisprudencial.

Este carácter evolutivo y el rol del juez se ven amenazados por la inteligencia artificial generativa y algoritmos predictivos. En efecto, la herramienta de IA o el algoritmo producirá una decisión estadísticamente satisfactoria en la mayoría de los casos, pero no se adaptará a situaciones que, a veces, son muy diferentes para una misma infracción. Existe un gran riesgo de repetición, lo que impediría la evolución de la jurisprudencia y, por tanto, del derecho.

La decisión producida por la IA será puramente matemática, cuando la esencia misma del contencioso administrativo y el penal reside en la riqueza de los criterios que influyen en la determinación del juicio, algunos de los cuales no pueden ser integrados por la máquina, como la actitud del procesado frente a la justicia, eventos pasados significativos, etc. Es la consideración de todos estos criterios, a veces subjetivos, lo que permite que la jurisprudencia evolucione.

Por lo tanto, la intervención humana nos parece aquí indispensable, ya que esta uniformización jurisprudencial que podría causar la utilización de ChatGPT llevaría a unas decisiones que no se ajustan a derecho y la utilización de información desactualizada sin ninguna trazabilidad podría colocar en riesgo la seguridad jurídica.

Si bien hay algoritmos predictivos que puede ser otra herramienta de ayuda al juez, sin embargo, su utilización sin filtros puede llevar a que el derecho se estático en razón a que el algoritmo no podrá desvincularse de las jurisprudencias que analiza para tomar una decisión, a diferencia del juez humano. El algoritmo podrá ser, como mucho, una herramienta de ayuda a la decisión, siempre que el juez humano tenga la capacidad de separarse de la decisión del algoritmo si considera que esta no es la mejor.

Resultado de lo anterior, la Corte Constitucional emitió la sentencia T-323 de 2024 donde marco un hito jurisprudencial en la regulación del uso de herramientas de inteligencia artificial en la administración de justicia. En el caso de estudio ya fue expuesto el juez de segunda instancia utilizó la herramienta ChatGPT 3.5 como apoyo argumentativo en su decisión judicial, lo que motivó a la alta corporación a pronunciarse sobre los límites y condiciones de uso de IA en la judicatura.

La Corte Constitucional en su análisis expreso que el uso de la IA generativa puede ser admisible como herramienta complementaria, siempre y cuando no sustituya el juicio racional del

operador jurídico, además reconoció que el juez de segunda instancia utilizó la IA para extender sus argumentos, pero sin delegar la decisión judicial a la herramienta tecnológica, la cual considera que fue un uso legítimo (Corte Constitucional, Sentencia T-323, 2024).

A partir del análisis que realizó la Corte Constitucional fijó criterios orientadores para el usos de IA en el proceso judicial, entre los cuales destacan la primacía del juicio humano, la transparencia respecto al uso de estas herramientas, la verificación rigurosa de la información generada por la IA y la protección de los derechos fundamentales, particularmente el derecho a la intimidad, el habeas data y el debido proceso, principios que buscan garantizar que la implementación herramientas basadas en IA no derive en una vulneración de garantías esenciales para los ciudadanos (Corte Constitucional, Sentencia T-323, 2024).

Asimismo, la Corte señaló límites al uso de la IA en decisiones judiciales, advirtiendo que su utilización es inadecuada cuando reemplaza funciones de raciocinio propia del juez, cuando omite la verificación de la veracidad y suficiencia de la información suministrada por la herramienta, o cuando se produce un impacto negativo en derechos fundamentales. Por lo tanto, cualquier apoyo tecnológico en la justicia debe estar sujeto a control humano, rendición de cuentas y su uso informado, prudente y documentado (Corte Constitucional, Sentencia T-323, 2024).

## **6.5 Antecedentes y dogmática de la responsabilidad extracontractual del Estado en el uso de Inteligencia artificial: riesgos y el principio de Precaución.**

La jurisprudencia colombiana en materia de responsabilidad extracontractual del Estado ha reconocido dos enfoques clave: la falla del servicio y el riesgo creado. Estas doctrinas son aplicables a la IA, ya que la implementación de estas tecnologías implica tanto la posibilidad de fallas en su uso como la creación de nuevos riesgos inherentes.

La teoría del riesgo, derivada de la revolución industrial, establece que quien crea un riesgo debe asumir sus consecuencias. Esto es especialmente relevante para las tecnologías de IA, que pueden generar daños significativos debido a la alta probabilidad de error en los algoritmos o en la toma de decisiones automatizadas. El Consejo de Estado ha desarrollado subreglas relacionadas con el riesgo, como el riesgo-beneficio, que aplica cuando una entidad se beneficia de una actividad riesgosa. Este principio puede aplicarse a empresas tecnológicas que implementan IA para obtener ganancias, pero que, al mismo tiempo, generan riesgos para los usuarios y el entorno.

El principio de precaución se ajusta perfectamente a la regulación de la IA. Al igual que en el daño ambiental, donde no es necesario esperar a que el daño sea evidente para actuar, en el caso de la IA, el Estado debe intervenir de manera preventiva cuando existan indicios serios de que una tecnología puede generar daños graves e irreversibles. La Unión Europea, a través de su marco regulador, ya impone límites estrictos a las aplicaciones de IA consideradas de riesgo alto, exigiendo pruebas exhaustivas antes de su uso en la sociedad. Del mismo modo, las tecnologías clasificadas como inaceptables están prohibidas debido a los riesgos insalvables que representan.

El concepto de riesgo está intrínsecamente vinculado a la noción de responsabilidad. En el contexto de la responsabilidad extracontractual del Estado, consagrada en el artículo 90 de la Constitución Política de Colombia, el Estado es responsable de los daños antijurídicos causados a los ciudadanos, incluso cuando estos provienen de actuaciones legítimas del Estado. Este marco también se aplica al uso de tecnologías emergentes como la inteligencia artificial (IA), donde el principio de precaución juega un papel esencial para mitigar los riesgos asociados a su implementación.

El principio de precaución, originado en la protección ambiental, se traslada al ámbito tecnológico para gestionar los riesgos que la IA puede generar. La IA, especialmente en sectores

como la salud, la justicia, y la gestión de datos personales, presenta incertidumbres y potenciales riesgos que, aunque no completamente conocidos, podrían tener consecuencias graves y difíciles de revertir. Ante estos escenarios de incertidumbre, el principio de precaución se convierte en una herramienta clave para que el Estado adopte medidas preventivas, aun en ausencia de certeza científica plena sobre los posibles daños.

A medida que la IA evoluciona y se vuelve más autónoma, los riesgos asociados a su uso también aumentan. Uno de los mayores desafíos es la posibilidad de que pueda cometer delitos de manera independiente, especialmente en el ámbito cibernético. Por ejemplo, se han reportado casos de IA utilizadas para hackear sistemas de seguridad y cometer fraudes a un nivel que supera las capacidades de los humanos (WIRED, 2023, p.1).

La posibilidad que la IA, en su afán por emular las capacidades humanas, cometas delitos sin intervención directa de una persona. Esto ha llevado a propuestas de reconocer a la IA como una persona artificial para poder atribuirle responsabilidad legal. Este riesgo no es teórico; ya han ocurrido incidentes en los que sistemas autónomos tomaron decisiones que resultaron en daños, como el caso de vehículos autónomos involucrados en accidentes (Gañán, 2019, p.1).

Otro riesgo clave es la posibilidad de que la IA sea utilizada para manipular o engañar a seres humanos. Un ejemplo de esto es el sistema de IA de Google que, en 2018, demostró su capacidad para mantener conversaciones que los humanos no podían distinguir de las reales. Este tipo de situaciones plantea dilemas sobre el control que se debe ejercer sobre la IA, para evitar que sea utilizada de manera maliciosa (La Vanguardia, 2021, p.1)..

La evolución de la IA ha traído consigo grandes avances tecnológicos, pero también ha abierto una nueva frontera de desafíos éticos y legales. La capacidad de aprendizaje y decisión

autónoma de estas máquinas requiere una urgente regulación, tanto para proteger a los usuarios como para evitar que la IA sea utilizada para fines delictivos.

El Estado tiene el deber de proteger a sus ciudadanos de los riesgos generados por el uso de tecnologías basadas en IA. Al igual que ocurre con el daño ambiental, el uso de IA puede generar riesgos que afecten derechos fundamentales, como la privacidad, la seguridad y la igualdad. Estos riesgos no solo afectan a individuos, sino también al orden social y a la confianza en el sistema de justicia y otros servicios públicos.

El uso de algoritmos en áreas como la salud pública, la toma de decisiones judiciales, o la seguridad puede traer grandes beneficios, pero también conlleva riesgos. La falta de transparencia en los algoritmos de IA, combinada con su capacidad para tomar decisiones automatizadas, puede generar consecuencias no previstas y difíciles de controlar. En este sentido, la responsabilidad del Estado no solo implica reaccionar ante los daños ya causados, sino anticipar y prevenir dichos daños mediante regulaciones adecuadas.

Como fue expuesto en acápite anterior, el reglamento de la Unión Europea sobre IA introduce una clasificación de las aplicaciones de IA según su nivel de riesgo: riesgo mínimo, medio, alto e inaceptable. Las aplicaciones de riesgo medio, como los Chatbots, algoritmos predictivos y otras tecnologías de procesamiento de lenguaje natural, deben cumplir con normas de transparencia, informando claramente a los usuarios que están interactuando con un sistema de IA y no con una persona. Este tipo de regulación puede servir como modelo para que el Estado busque mitigar los riesgos de la IA.

## 6.6 Teorías de imputación y el principio de precaución en el uso de IA

Lo primero que debemos reconocer es que la tecnología ha adquirido una importancia creciente como mecanismo de acceso a la justicia. Un ejemplo claro de esto fue la pandemia, que obligó al sistema judicial a superar los obstáculos impuestos por el confinamiento, donde la tecnología jugó un papel crucial.

Hoy en día, la tecnología es una herramienta poderosa en el ámbito judicial, ya que permite gestionar procesos, avanzar en trámites y optimizar la actividad procesal. Mediante el uso de herramientas tecnológicas, es posible buscar jurisprudencia y doctrina de manera más eficiente, facilitando así la toma de decisiones más acertadas y, en última instancia, asegurando un mejor acceso a la administración de justicia.

Ahora bien, los algoritmos es un sistema ordenado de procesos que permite realizar cálculos y llegar a soluciones ante problemas. Lo primero que hace un algoritmo es analizar la información disponible para ofrecer respuestas a preguntas o resolver problemas que se le plantean. Estos sistemas procesan grandes volúmenes de información, y en muchos casos, también toman decisiones o monitorean personas a través de sus dispositivos móviles.

Incluso, los algoritmos pueden combinar los criterios proporcionados por el usuario para, por ejemplo, crear perfiles en el ámbito de relaciones personales. En este contexto, se transgrede la privacidad porque, implícitamente, estamos buscando asistencia. El siguiente paso en este proceso es lo que llamamos inteligencia artificial.

Gómez Llinás (2021) expreso que la IA es un sistema mediante el cual una máquina aprende de manera similar a los seres humanos: a partir de experiencias, errores y aciertos, acumulando conocimiento para mejorar sus decisiones. En esencia, la IA es un proceso de

optimización, que busca utilizar los recursos disponibles de manera eficiente para alcanzar un resultado óptimo (p.3).

Por lo tanto, la inteligencia artificial tiene como objetivo optimizar los procesos. Se considera uno de los mayores inventos de la humanidad, y se prevé que para el año 2029, con un 50% de probabilidad, la IA podrá igualar o incluso superar la capacidad humana para tomar decisiones, lo que la convertiría en un invento aún más eficiente que las contribuciones humanas previas (León Serrano, 2017, p.61).

La diferencia fundamental entre los seres humanos y la IA es que los humanos contamos con la capacidad de emocionarnos en el momento de tomar decisiones, lo cual añade un elemento de subjetividad. Por el contrario, la IA toma decisiones basándose exclusivamente en la optimización de procesos, sin dejarse influir por emociones.

Un ejemplo ilustrativo son los coches autónomos, que deben tomar decisiones basadas en la evaluación de riesgos en la carretera, optimizando sus acciones en tiempo real. Sin embargo, aunque estos sistemas son eficientes en términos de optimización, no siempre consideran los aspectos morales o éticos que rodean las decisiones humanas (León Serrano, 2017, p.61).

La toma de decisiones humanas suele asociarse al utilitarismo, es decir, las personas eligen la opción más útil, lo que, en palabras del propio Bentham (1998), es “un principio que aprueba o rechaza las acciones según aumenten o disminuyan la felicidad de los demás contra cualquier acción” (Bentham, 1781, p.14). Sin embargo, la cuestión no es si la IA tomará el control en la toma de decisiones, sino cómo queremos que la IA tome decisiones en situaciones que involucren dilemas éticos o que puedan afectar derechos fundamentales.

Es importante tener en cuenta que, aunque la IA es ya una realidad y una herramienta útil para la toma de decisiones, se debe garantizar que su escala de valores sea lo más similar posible

a la de los seres humanos. En ese contexto, lo primero es comprender cómo funciona la IA y cómo nos gustaría que tomara decisiones en escenarios complejos.

En ese sentido, las alucinaciones que pueden presentar los ChatBots implicaría un riesgo, este se puede encuadrar dentro del marco de la teoría del riesgo creado. Las alucinaciones en los ChatBots se refieren a respuestas incorrectas, incoherentes o fabricadas, que, aunque parecen lógicas o veraces, carecen de base en hechos reales. Este fenómeno puede generar riesgos significativos, particularmente en contextos sensibles como la salud, la justicia o la toma de decisiones públicas.

Este riesgo puede categorizarse según el usuario, el proveedor o el diseñador del sistema. Para el usuario consiste en que se puede identificar un riesgo de información errónea, que encaja en la categoría de riesgo peligro debido a las alucinaciones de los ChatBots, que pueden proporcionar información incorrecta o engañosa. Esto puede inducir a los usuarios a tomar decisiones basadas en datos falsos o inexactos. Por ejemplo, en un contexto médico, un ChatBot podría ofrecer recomendaciones equivocadas, comprometiendo la salud del usuario. Este tipo de riesgo proviene de la tecnología en sí, ya sea por errores en su programación o en la manera en que procesa la información, lo que lo convierte en un riesgo inherente al uso de estas herramientas.

Frente al Riesgo para el proveedor o programador: Se presenta un riesgo de confianza injustificada, que se encuadra en el concepto de riesgo-beneficio. Las empresas o entidades que desarrollan y utilizan ChatBots se benefician de la automatización y la eficiencia que estas herramientas proporcionan. Sin embargo, también generan un riesgo para los usuarios que confían en la exactitud de las respuestas. En este sentido, el riesgo-beneficio implica que las entidades creadoras o implementadoras de ChatBots deben asumir la responsabilidad por los posibles daños que puedan derivarse de la dependencia de estas herramientas.

También se puede dar el Riesgo Alea o de azar para el usuario, en razón a que se puede identificarse un riesgo aleatorio o riesgo Alea, dado que las alucinaciones de los ChatBots son impredecibles. El riesgo de recibir una respuesta incorrecta es completamente aleatorio, y puede variar según el contexto, la consulta y la calidad de los datos que maneja el sistema. Este tipo de riesgo es difícil de prever, ya que las alucinaciones pueden ocurrir sin un patrón claro y sin advertencia previa de que el sistema está fallando.

En ese contexto el Principio de Precaución juega un papel importante dado que estas tecnologías aún presentan riesgos no totalmente comprendidos y los efectos de sus errores pueden ser graves, el principio de precaución debe aplicarse. Esto implica que, aun sin certeza absoluta sobre cuándo y cómo pueden ocurrir estas alucinaciones, es necesario que los desarrolladores, reguladores y usuarios adopten medidas preventivas. Estas medidas pueden incluir la supervisión constante del uso de ChatBots, la limitación de su implementación en áreas críticas y la obligación de informar a los usuarios sobre los posibles errores y su naturaleza.

Las alucinaciones en los ChatBots crean un riesgo peligroso y de confianza injustificada, donde los desarrolladores y usuarios deben ser conscientes de las limitaciones de estas tecnologías, aplicando medidas de precaución para minimizar los daños potenciales que puedan derivarse de la información errónea generada por estos sistemas.

El tipo de riesgo que puede generarse al adoptar una decisión judicial basada únicamente en información generada por un ChatBot inteligente podría denominarse Riesgo de Decisión Automatizada Inexacta dado que la falta de fundamento Jurídico, Riesgo Peligro, en razón a que las fuentes de donde toman información para sustentar una decisión judicial suelen no ser precisas ni rigurosas, como antes fue estudiado. Si se adopta una decisión basada únicamente en la información generada por un ChatBot, se corre el riesgo de que la información sea incorrecta o

carezca de una base legal adecuada, lo que podría afectar la justicia del caso y los derechos de las partes involucradas.

El riesgo de confianza injustificada, riesgo beneficio, consiste en este caso en que los jueces o abogados pueden confiar erróneamente en la precisión y objetividad del ChatBot, y en algoritmos predictivos ignorando que estos sistemas pueden cometer errores alucinaciones, sistematizar jurisprudencia que ha cambiado, no ser capaces de interpretar adecuadamente los matices legales, los precedentes o la complejidad de los casos judiciales.

Además de configurarse también el riesgo de irresponsabilidad jurídica, riesgo alea, toda vez que las decisiones judiciales basadas en información automatizada generan un riesgo de azar, ya que las alucinaciones de los ChatBots son impredecibles. Si el juez o la parte procesal no verifican la veracidad y precisión de la información, la decisión puede estar sujeta a errores graves, comprometiendo el debido proceso y el acceso a la justicia.

El Principio de Precaución en el contexto judicial es crucial para evitar decisiones basadas en información no verificada proveniente de herramientas tecnológicas. Las cortes deben asegurarse de que cualquier información generada por IA sea rigurosamente revisada y complementada con análisis humano, evitando que una decisión judicial se fundamente exclusivamente en datos automatizados.

En ese sentido el Riesgo de Decisión Automatizada Inexacta surge cuando una decisión judicial se adopta sin validar la precisión y veracidad de la información generada por un ChatBot, lo que puede comprometer los derechos y la justicia en el proceso.

### **6.7 Aplicación del principio de precaución en la IA**

A medida que la sociedad moderna es designada como una sociedad de riesgo, los incidentes relacionados con la tecnología están ocurriendo con frecuencia, pues algunos de los ejemplos fueron expuestos al inicio de este trabajo, lo que conlleva a un aumento de la discusión sobre los riesgos tecnológicos. Hasta ahora, las discusiones sobre definición de la naturaleza de los riesgos tecnológicos se centran sobre la definición de la naturaleza, el control y la mitigación (Ulrich, 1998, p.233).

Una de las características más destacadas del riesgo tecnológico es que hay muy poca información confiable, aunado a esto, la inexistencia de disposiciones regulatorias claras sobre la inteligencia artificial lo que origina que por ahora se tiene que gestionar el riesgo producido y solo se da con el afianzamiento de la tecnología en la sociedad.

El principio de precaución es esencial cuando se trata de tecnologías emergentes como la IA, especialmente debido a la incertidumbre sobre sus impactos a largo plazo. Como ya fue expuesto al inicio de esta investigación, el principio establece que, aun en ausencia de certeza científica, si hay indicios serios de que una tecnología puede generar daños graves e irreversibles, deben adoptarse medidas para prevenir dichos daños.

En el caso de la IA, esto significa que el Estado debe evaluar y regular su uso en sectores donde los impactos ambientales puedan ser significativos. No se puede esperar a tener certeza absoluta sobre los riesgos antes de actuar; el daño podría ser irreversible para cuando los efectos sean evidentes. El principio de precaución ofrece una vía para detener o regular el uso de tecnologías en situaciones de incertidumbre, permitiendo un enfoque más consciente y preventivo.

En ese contexto la gestión de tecnologías basadas en IA en relación con el medio ambiente requiere un enfoque interdisciplinario que abarque no solo aspectos legales, sino también científicos y técnicos. No deben adoptarse fórmulas generales para medir los impactos de la IA en el medio ambiente. En su lugar, deben utilizarse enfoques equitativos y restauradores que consideren los contextos específicos de cada caso.

El Estado tiene la responsabilidad de adoptar políticas más conscientes y fundamentadas en el principio de precaución, para evitar daños ambientales irreversibles causados por la IA, anticipando los riesgos antes de que se materialicen.

Como ya fue expuesto el principio de precaución se viene analizando desde un enfoque donde la introducción de la tecnología debido a que la seguridad no está confirmada y representa una amenaza para los derechos fundamentales se debe adoptar un enfoque preventivo, incluso si no se ha llegado a una conclusión clara sobre la relación de causalidad.

Bajo esta premisa y frente a lo que se ha desarrollado sobre la gestión del riesgo y tomado como marco general la clasificación del riesgo de la inteligencia artificial contenido en la resolución del Parlamento europeo, proponiendo en esta investigación clasificar el riesgo en función de la incertidumbre del conocimiento y la posibilidad de conflicto.

*Tipo I:* aquí tanto la incertidumbre del conocimiento como la posibilidad de conflicto son bajas lo que significa que hay un consenso claro sobre el problema y se pueden encontrar soluciones técnicas fácilmente. Son tecnologías bien establecidas, como algoritmos bien definidos, y no generan conflicto éticos o sociales significativos, ya que usan principalmente para mejorar la experiencia del usuario, plataforma de streaming como Netflix o Spotify.

*Tipo II:* en este caso, la incertidumbre del conocimiento es alta, pero la posibilidad de conflicto es baja. Aunque hay un acuerdo sobre la definición del problema, el conocimiento es

insuficiente. Estos sistemas enfrentan incertidumbre debido a la falta de datos médicos adecuados o comprensión completa de las enfermedades, pero no generan desacuerdo en términos éticos sociales debido al propósito el cual es claro. Ejemplo el diagnóstico médico asistido por IA.

*Tipo III:* aquí, aunque la información sobre los riesgos es clara, el proceso para llegar a un consenso es conflictivo. Aunque las soluciones son evidentes, la falta de acuerdo sobre cómo definir el problema y qué solución elegir puede llevar a la necesidad de imponer decisiones o facilitar discusiones para alcanzar un consenso. Un ejemplo es: el reconocimiento facial en espacios públicos.

*Tipo IV:* en este caso, tanto la incertidumbre del conocimiento como la posibilidad de conflictos son altas. Esto significa que no solo hay falta de claridad sobre los riesgos, sino que también hay desacuerdos significativos sobre cómo definir y evaluar esos riesgos. En este escenario no hay métodos claros de toma de decisiones o control, y la única forma de superar estos riesgos es a través de la acumulación de conocimiento y el establecimiento de un consenso. El ejemplo es la inteligencia artificial fuerte en razón que estos algoritmos plantean riesgos desconocidos por cuanto no se ha desarrollado plenamente, y su impacto ético, social y económicos es bastante controvertido.

Para garantizar la seguridad de la información y abordar de manera eficiente los riesgos tecnológicos, es indispensable combinar el desarrollo con enfoques metodológicos sólidos, la utilización de herramientas de análisis de riesgos que ofrezcan resultados confiables y que se puedan adaptar a las condiciones específicas y la colaboración entre expertos, instituciones públicas y el sector privado bajo un enfoque continuo en investigación y desarrollo.

Si bien, ya se clasificó el riesgo se parte para el diseño de estrategias adaptativas para cada tipo de riesgos identificados y se desarrollan estrategias específicas, como puede ser para el riesgo

tipo I se puede desarrollar guías normativas basadas en estándares técnicos existentes, supervisión limitada a través de auditorías tecnológicas periódicas como puede ser normas de transparencia y privacidad en algoritmos de recomendación. En Colombia se tiene un marco ético para la aplicación de la IA como suplemento a este tipo de riesgo.

Cuando se habla de riesgo tipo II el objetivo es buscar reducir la incertidumbre del conocimiento a través de fomentar la investigación colaborativa para cerrar las brechas de conocimiento, implementar regulaciones temporales o provisionales hasta que se acumule más información; obligar a los desarrolladores a compartir datos y resultados para mejorar la comprensión técnica del sistema. Un ejemplo puede ser disposiciones legales que exijan validación clínica por una autoridad que haga parte del ministerio de las TIC a fin de que mediante un diagnóstico al sistema basado en IA de su aprobación.

En el riesgo tipo III el objetivo por lograr es facilitar el consenso social mediante la creación de espacios de dialogo participativo para involucrar a todas las partes interesadas o actores claves como la sociedad civil, comisión del congreso, expertos, autoridades y el sector privado; establecer un marco ético y principios rectores para la protección los derechos fundamentales de las personas. Un ejemplo es un control previo ante el juez de control de garantías para el uso de reconocimiento facial en espacios públicos.

Frente al riesgo tipo IV el objetivo es acumular conocimiento y construir consenso a largo plazo el cual se puede llevar a cabo mediante el fomento de la investigación interdisciplinaria y los proyectos piloto para explorar usos seguros, crear organismos nacionales adscrito a una red de apoyo internacional que se especialicen en el monitoreo y evaluación de riesgos de esta tecnología emergente. Asimismo, adoptar un enfoque precautorio, restringiendo su implementación hasta que

exista mayor claridad sobre sus implicaciones. Normas que propicien la investigación y desarrollo responsable de la inteligencia artificial fuerte.

De esta manera el principio de precaución se desarrolla como eje esencial en el uso de la IA. Cuando una tecnología presenta riesgos potenciales que podrían afectar gravemente a los derechos fundamentales o al medio ambiente, el Estado debe adoptar una metodología como la antes desarrollada, comenzado por ubicar la tecnología en un tipo de riesgos y desarrollar el objetivo propuesto y adoptar algunas de las medidas preventivas expuesta en cada una de ellas, además de exigir evaluaciones de impacto ético, restricciones en el uso de datos sensibles y, en casos extremos, prohibir su uso.

En el caso de Chatbots y otras IA basadas en algoritmos Deep Learning, inteligencia artificial fuerte, pues es claro que la falta de transparencia y el potencial para generar errores, conocidos como alucinaciones en los modelos de lenguaje natural, que representan riesgos que deben ser gestionados adecuadamente. El principio de precaución sugiere que, ante la falta de certeza científica sobre los efectos a largo plazo de estas tecnologías, el Estado debe establecer límites claros, imponiendo obligaciones de transparencia y protección de datos, así como sanciones proporcionales para su incumplimiento.

En ese sentido el principio de precaución es una herramienta esencial para gestionar los riesgos derivados del uso de tecnologías basadas en IA, dado que permite anticiparse a los posibles daños, aun cuando no haya certeza científica completa sobre su ocurrencia.

La regulación del Estado en torno a la IA debe basarse en la responsabilidad objetiva, siguiendo el modelo europeo que clasifica las aplicaciones de IA según su nivel de riesgo y establece límites claros para su implementación. El daño causado por la IA puede ser similar al daño ambiental en cuanto a su naturaleza difusa y difícil de revertir, por lo que el Estado debe

garantizar la transparencia, control y responsabilidad en el uso de estas tecnologías, siempre buscando el bienestar colectivo y la protección de los derechos fundamentales.

De esta manera, la dogmática del riesgo, unida al principio de precaución, proporciona un marco sólido para regular las tecnologías emergentes y garantizar que el avance tecnológico no se realice a expensas del bienestar de la sociedad y el medio ambiente.

## **7. Conclusiones**

La evolución y aplicación del principio de precaución en Colombia se ha venido desarrollando a través de la jurisprudencia colombiana, especialmente a partir de la sentencia C-988/2004, consolidándolo como una herramienta para gestionar el riesgo en contexto de incertidumbre. Este principio permite a los jueces adoptar medidas preventivas, incluso en ausencia de certeza científica, para evitar daños graves e irreversibles, lo que implica la necesidad de incorporarlo en la administración de justicia frente a los riesgos que afecten los derechos fundamentales al utilizar sistemas basados en IA.

La legislación de la Unión Europea emitida en junio de 2024 ha logrado avances significativos y límites en la regulación de la IA generativa, estableciendo estándares para garantizar su responsabilidad y ética. Se destacan prácticas como la obligación de transparencia en los algoritmos, la protección de los derechos de los usuarios y la implementación de marcos de auditoría para evitar sesgos y errores. Estas regulaciones representan un modelo efectivo para equilibrar innovación y protección de derechos en la administración de justicia.

En el contexto colombiano, la aplicación del principio de precaución en el uso de IA generativa por parte de operadores judiciales contribuye a limitar la responsabilidad extracontractual del Estado. Esto se logra mediante la adopción de medidas preventivas razonables

y demostrando que las decisiones se tomaron con base en información disponibles y metodología rigurosa. Este enfoque refuerza la diligencia estatal de mitigar los riesgos inherentes al uso de tecnologías avanzadas.

En una perspectiva futura, la IA podría, como mucho, ser una herramienta de apoyo a la decisión de los jueces humanos, pero nunca podrán reemplazarlos completamente. En efecto, existe una parte de subjetividad inherente a la función de juez que un sistema u algoritmo no puede asumir. Sin embargo, aunque en teoría la Comisión Europea para la Eficiencia de la Justicia establece que las herramientas de ayuda a la decisión judicial deben ser concebidas y percibidas como un apoyo auxiliar al proceso de decisión del juez, facilitando su trabajo y no como una imposición, en la práctica, los jueces que utilicen el ChatGPT como herramienta de apoyo a la decisión encontrarán dificultades para separarse del resultado proporcionado por este, fenómeno conocido como el efecto performativo.

## Referencias

- Amnistía Internacional. (29 de Abril de 2022, p.1). *Caso Pegasus (resumen): El escándalo del espionaje masivo*. Obtenido de <https://www.es.amnesty.org/en-que-estamos/blog/historia/articulo/pegasus-espionaje-masivo/>
- Artigas, C. (2001, p.11). *El principio precautorio en el derecho y la política internacional. Serie Recursos naturales e infraestructura*. Cepal. Obtenido de <https://hdl.handle.net/11362/6377>
- Asamblea General de Naciones Unidas. (2013, p.15). Informe del Experto independiente sobre la cuestión de las obligaciones de derechos humanos relacionadas con el disfrute de un medio ambiente sin riesgos, limpio, saludable y sostenible John H Knox. (pág. 102). New York: UN.org. Obtenido de <https://documents.un.org/doc/undoc/gen/g13/192/14/pdf/g1319214.pdf>
- Asamblea Nacional Constituyente. (1991, p.1).
- Aucejo, E. A., & Ramón, F. (28 de Abril de 2023, p.13). Inteligencia Artificial: Chat GPT Versus la Ley y El Derecho. Jaque al derecho de la propiedad intelectual. *Revista de Educación y Derecho*, 1-21. doi:ORCID: <https://orcid.org/0000-0001-5688-1482>
- Belloso Matin, N. (06 de 12 de 2019, p.17). ALGORITMOS PREDICTIVOS AL SERVICIO DE LA JUSTICIA: ¿UNA NUEVA FORMA DE MINIMIZAR EL RIESGO Y LA INCERTIDUMBRE? *Revista de Facultad de Minería de Datos*, 22(43), 1-31. Recuperado el 5 de 10 de 2024, de <https://periodicos.pucminas.br/index.php/Direito/article/view/20780/16029>

Bentham, J. (1781, p.14). *Introduction to the Principles of Morals and Legislation*. Londres:

Batoche Book Kichener. Obtenido de  
<https://historyofeconomicthought.mcmaster.ca/bentham/morals.pdf>

Bowman, S. R. (2023, p.3). Eight Things to Know about Large Language Models. *Anthopic, P.B,C.*

Obtenido de <https://arxiv.org/pdf/2304.00612>

Brenner, S. (2013, p.35). *HUMANS AND HUMANS+: TECHNOLOGICAL ENHANCEMENT*

(Vol. 19). Boston: Boston University. Obtenido de file:///C:/Users/User/Downloads/ssrn-2360756.pdf

Cairo Battistutti, P. (2011, p.143). *El Hombre Artificial*. Alfaomega.

Cárdenas, G. A., & Gómez, G. (2020, p.15). *RESPONSABILIDAD CIVIL EXTRACONTRACTUAL*

*DE LA INTELIGENCIA ARTIFICIAL EN EL RÉGIMEN JURÍDICO COLOMBIANO*  
*¿NECESIDAD DE UN CAMBIO NORMATIVO?* Pontificia Universidad Javeriana.

Obtenido de  
<https://repository.javeriana.edu.co/bitstream/handle/10554/51579/Trabajo%20de%20Grado%20Responsabilidad%20Civil%20Extracontractual%20de%20la%20Inteligencia%20Artificial.pdf?sequence=1&isAllowed=y>

Castellanos Carreño, A., & Castellanos Carreño, D. (2017). Proceso de convencionalización del principio de precaución y de prevención en el marco del Sistema Interamericano: Reto y perspectiva.

Revista Republicana, (23), 215-234.  
<https://doi.org/10.21017/Rev.Repub.2017.v23.a37>

Castro Páez, A. F. (2021). Responsabilidad patrimonial y COVID-19: El principio de precaución como título de imputación. *Revista de Derecho Público*, (47), 173–197. Universidad Externado de Colombia.

Centro Cibernético de la Policía. (2023, p.1). Bogotá. Obtenido de [https://caivirtual.policia.gov.co/sites/default/files/observatorio/Balance%20anual%202023\\_0.pdf](https://caivirtual.policia.gov.co/sites/default/files/observatorio/Balance%20anual%202023_0.pdf)

Cepeda Espinosa, M. J., & Otálora Lozano, G. (2020). Modernización de la administración de justicia a través de la inteligencia artificial. Bogotá D. C.: [s. n.].

Colmenares, R. O. (2024, p.1). *Retos en la modernización de la justicia con la implementación de Inteligencia Artificial (IA) generativa en la decisión judicial*. Universidad Externado de Colombia. Obtenido de <https://blogrevistaderechoestado.uexternado.edu.co/2024/07/24/retos-en-la-modernizacion-de-la-justicia-con-la-implementacion-de-inteligencia-artificial-ia-generativa-en-la-decision-judicial/>

Congreso de la República de Colombia, Ley 84 (1973).

Congreso de la Republica Ley 1474. (2011).

congreso de la Republica Ley 83. (1993).

Congreso de la Republica, Ley 1523. (2012, p.1). Gaceta Oficial.

Congreso de la Republica, Ley 164. (1994).

Congreso de la Republica, ley 2220. (2022). Estatuto de Conciliación .

Congreso de la Republica, Ley 489. (1998).

Congreso, Ley 1581. (2012).

Consejo de Estado, Sala de Consulta, Rad. 2019-00117-00, 11001-03-06-000-2019-00117-00(C)  
(26 de 11 de 2019).

Consejo de Estado, Sección III, Exp. 16530 (26 de Marzo de 2008).

Consejo de Estado, Sección III, Exp. 21294 (07 de Julio de 2011).

Consejo de Estado, Sección III, Sentencia Exp. 16696 (03 de Mayo de 2007).

Consejo de Estado, Sección III, Sentencia Exp. 18940 (26 de Enero de 2011).

Consejo de Estado, Sección III, Sentencia Exp. 31182 (13 de Noviembre de 2014).

Consejo de Estado, Sección III, Sentencia Exp. 6515 (31 de Octubre de 1991).

Consejo de Estado, Seccion III, Sentencias 35874 (02 de Mayo de 2016).

Consejo de Estado, Seccion Primera, Rad. 2003-01265-01, 41001-23-31-000-2003-01265-01(AP)  
(17 de 7 de 2008).

Consejo de Estado, Seccion Primera, Rad. 2007-00292-00, 11001-03-24-000-2007-00292-00 (12  
de 7 de 2018).

Consejo de Estado, Seccion Tercera, Rad. 57819, 11001-03-26-000-2016-00140-00 (7 de 7 de  
2022).

Consejo de Estado, Sentencia (27 de Julio de 1947, p.46). Obtenido de [https://sidn.ramajudicial.gov.co/SIDN//DOCTRINA/TEXTOS\\_COMPLETOS/ANTOLOGIAFINAL/SECCION\\_TERCERA/SECCION\\_TERCERA\\_TOMO\\_B/CE-SCA-1947-07-29.pdf](https://sidn.ramajudicial.gov.co/SIDN//DOCTRINA/TEXTOS_COMPLETOS/ANTOLOGIAFINAL/SECCION_TERCERA/SECCION_TERCERA_TOMO_B/CE-SCA-1947-07-29.pdf)

Consejo de Estado, Sentencia, 2013-00149-02, 15001-23-33-000-2013-00149-02 (20 de 02 de 2014). Obtenido de [https://www.consejodeestado.gov.co/documentos/boletines/142/AC/15001-23-33-000-2013-00149-02\(AP\).pdf](https://www.consejodeestado.gov.co/documentos/boletines/142/AC/15001-23-33-000-2013-00149-02(AP).pdf)

Consejo de Estado, Sala de lo Contencioso Administrativo, Sección Tercera, Subsección B. (2012, 29 de octubre). Radicación n.º 25000-23-26-000-1993-08632-01 (18472).

Constitucion Politica (1991, Art. 13).

Constitución Política (1991, Art. 90).

Constitucion Politica (1991, p.3).

Contaduría General de la Nación. (2023, p.14). *Litigios y demandas en contra del Estado*. Bogotá. Obtenido de <https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwim5ubm1OaKAxULfDABHS0sOEYQFnoECBYQAw&url=https%3A%2F%2Fwww.contaduria.gov.co%2Fdocuments%2F20127%2F6084011%2FIEBC%2BLitigios%2B%2526%2Bdemandas%2Ben%2Bcontra%2Bdel%2B>

Consejo Superior de la Judicatura. (2024, 16 de diciembre). Acuerdo PCSJA24-12243: Por el cual se adoptan lineamientos para el uso y aprovechamiento respetuoso, responsable, seguro y ético de la inteligencia artificial en la Rama Judicial.  
<https://procesojudicial.ramajudicial.gov.co/FirmaElectronica>

Corporación excelencia para la justicia. (18 de Abril de 2020, p.1). Obtenido de <https://cej.org.co/sala-de-prensa/articulos-de-prensa/mas-jueces-podrian-ayudar-a-mitigar-la-congestion-judicial/>

Corte Constitucional de Colombia Sentencia C-703 de 2010 (Magistrado Ponente:GABRIEL EDUARDO MENDOZA MARTELO). Obtenido de <https://www.corteconstitucional.gov.co/relatoria/2010/c-703-10.htm>

Corte Constitucional de Colombia, Sentencia T-323 de 2024 (M.P. Juan Carlos Cortés González). Obtenido de <https://www.corteconstitucional.gov.co/relatoria/2024/T-323-24.htm>

Corte Constitucional, Sentencia C - 127 (02 de Marzo de 2011).

Corte Constitucional, Sentencia C-333 (1996).

Corte Constitucional, Sentencia C-339 (7 de 5 de 2002). Obtenido de <https://www.corteconstitucional.gov.co/Relatoria/2002/C-339-02.htm>

Corte Constitucional, Sentencia C-339, D-3767 (7 de Mayo de 2002). Obtenido de <https://www.alcaldiabogota.gov.co/sisjur/normas/Normal.jsp?i=82830&dt=S>

Corte Constitucional, Sentencia C-703, D-8019 (6 de 9 de 2010). Obtenido de <https://www.corteconstitucional.gov.co/relatoria/2010/c-703-10.htm>

Corte Constitucional, Sentencia SU-174, T-8.013.629 (3 de 06 de 2021). Obtenido de <https://www.corteconstitucional.gov.co/Relatoria/2021/SU174-21.htm>

Corte Constitucional, Sentencia T-909, T-3102855 (01 de Diciembre de 2011).

Corte Constitucional. Sentencia C-293, D-3748 (23 de 4 de 2002). Obtenido de <https://www.corteconstitucional.gov.co/relatoria/2002/c-293-02.htm>

Corte Constitucional. (2024). Sentencia T-323 de 2024. Magistrado ponente: Jorge Enrique Ibáñez Najar. <https://www.corteconstitucional.gov.co/relatoria/2024/T-323-24.htm>

Corte IDH, Caso Palamara Iribarne Vs Chile (22 de 11 de 2005).

Corte Interamericana Derechos Humanos, Opinión Consultiva 23. (2017, p.22). Opinión Consultiva 23 sobre Medio Ambiente y Derechos Humanos., (pág. 20). Obtenido de [http://corteidh.or.cr/docs/opiniones/seriea\\_23\\_esp.pdf](http://corteidh.or.cr/docs/opiniones/seriea_23_esp.pdf)

Corte Suprema de Wisconsin. (07 de Julio de 2016). Estado de Wisconsin Vs. Eric L. Loomis No. 2015AP157-CR. Obtenido de <https://www.courts.ca.gov/documents/BTB24-2L-3.pdf>

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

De Zan, J. (2004, p.53). *La ética, los derechos y la Justicia*. Montevideo: Fundación Konrad. Obtenido de <https://www.corteidh.or.cr/tablas/23356.pdf>

Departamento Nacional de Planeación. (Mayo de 2021, p.3). *dnp.gov.co*. Obtenido de [https://colaboracion.dnp.gov.co/CDT/PND/Barco\\_Polits\\_Modernizacion\\_Admon\\_Pub.pdf](https://colaboracion.dnp.gov.co/CDT/PND/Barco_Polits_Modernizacion_Admon_Pub.pdf)

Domiguez Peco, E. (2018, p.247). *Derecho de los Robots*. Madrid: Wolters Kluwer España, S.A.

Obtenido de

<https://sistemabibliotecario.scjn.gov.mx/sisbib/2018/000294735/000294735.pdf>

Escuela Judicial “Rodrigo Lara Bonilla”. (2024). *Decisión innovadora: SENTENCIA T-323 DE 2024, LA INTELIGENCIA ARTIFICIAL (IA) NO PUEDE SUSTITUIR AL JUEZ EN LA TOMA DE DECISIONES JUDICIALES*. Obtenido de

<https://escuelajudicial.ramajudicial.gov.co/noticia/decision-innovadora-sentencia-t-323-de-2024-la-inteligencia-artificial-ia-no-puede>

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

Fondo de las Naciones Unidas para la Infancia, UNICEF. (30 de 07 de 2020, p.1). *UNICEF.ORG*.

Obtenido de <https://www.unicef.org/es/comunicados-prensa/un-tercio-de-los-niños-del-mundo-está-intoxicado-por-plomo-según-un-nuevo>

Frosini, V. (2019, p.73). *Cibernetica, Derecho y Sociedad*. (C. Salguero Talavera, & R. Soriano Diaz, Trads.) Santiago de Chile: Ediciones Jurídicas Olejnik.

Gañán, H. (01 de Enero de 2019, p.1). Un Tesla Autónomo atropella a un robot ruso y se da a la fuga. Obtenido de [https://www.elplural.com/leequid/omg/un-tesla-autonomo-atropella-a-un-robot-ruso-y-se-da-a-la-fuga\\_209152102](https://www.elplural.com/leequid/omg/un-tesla-autonomo-atropella-a-un-robot-ruso-y-se-da-a-la-fuga_209152102)

García de Enterría , E., & Fernández , T. R. (1999, p.353). *Curso de Derecho Administrativo*. Madrid, España: Civitas.

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

<https://www.umng.edu.co/documents/20127/0/EL+IMPACTO+DE+LA+INTELIGENCIA+ARTIFICIAL.pdf/8007b6ca-5b02-b7f1-4a64-4a27ac3a9060?t=1639080191820>

Gómez Llinás, D. A. (06 de Diciembre de 2021, p.3). Obtenido de

<https://www.umng.edu.co/documents/20127/0/EL+IMPACTO+DE+LA+INTELIGENCIA+ARTIFICIAL.pdf/8007b6ca-5b02-b7f1-4a64-4a27ac3a9060?t=1639080191820>

Granja, A. H. (2017, p.17). *“Riesgos ambientales y principio de precaución: una perspectiva*.

Guanche, J. C. (2023, p.1). *La historia del algoritmo. Los “fallos” de la Inteligencia Artificial*.

UNESCO. Obtenido de <https://www.unesco.org/es/articulos/la-historia-del-algoritmo-los-fallos-de-la-inteligencia-artificial>

Guerra, M. D. (2022, p.15). *Constitución e Inteligencia Artificial en proceso*. Universidad Libre - Cúcuta. Obtenido de

<https://www.unilibrecucuta.edu.co/portal/images/investigacion/pdf/librocongreso/LIBRO-CONSTITUCION-E-INTELIGENCIA-ARTIFICIAL-EN-EL-PROCESO.pdf>

Guío, E. A., Tamayo, U. E., & Gomez, A. P. (2021, p.23). *Marco Ético para la Inteligencia Artificial en Colombia* (Version 1 ed.). Bogotá. Obtenido de

<https://minciencias.gov.co/sites/default/files/marco-etico-ia-colombia-2021.pdf>

Henao, P. J. (1998, p.317). *El Daño: Análisis Comparativo de la responsabilidad Extracontractual del estado en Derecho Colombiano y Frances*. Bogotá: Universidad Externado.

Henríquez, R. C. (2014, p.1). *Modelando el Crecimineto de Ciudades Medias*. Santiago:

Universidad Católica de Chile. Obtenido de

[https://books.google.com.co/books?id=lgP7CAAAQBAJ&pg=PA34&lpg=PA34&dq=Primavera+Silenciosa"+de+Rachel+Carson+y+el+informe+"Los+límites+del+crecimiento"&source=bl&ots=cGLMXIKmyt&sig=ACfU3U3BYiNOaLfsehnG\\_Yk80MxDUE60iA&hl=es-419&sa=X&ved=2ahUKEwiy9N3nvNKGAXU](https://books.google.com.co/books?id=lgP7CAAAQBAJ&pg=PA34&lpg=PA34&dq=Primavera+Silenciosa)

Herrera, S. . (2024). *Resumen de la Sentencia T-323 de 2024 de la Corte Constitucional de*

*Colombia sobre el uso de IA por jueces de la República*. Universidad Externado de Colombia. Obtenido de <https://propintel.uexternado.edu.co/resumen-de-la-sentencia-t-323-de-2024-de-la-corte-constitucional-de-colombia-sobre-el-uso-de-ia-por-jueces-de-la-republica/>

Hidalgo, O. (2024). *Incorporación del principio de precaución en la responsabilidad frente a la*

*amenaza de daño a los trabajadores*. Universidad Externado de Colombia. Obtenido de <https://bdigital.uexternado.edu.co/server/api/core/bitstreams/0f49d98f-d80c-4600-9d09-57e43bc21228/content>

Hintze, A. (14 de Noviembre de 2016, p.1). *Theconversation.com*. Obtenido de

<https://theconversation.com/understanding-the-four-types-of-ai-from-reactive-robots-to-self-aware-beings-67616>

Jáuregui, M. . (2013, p.16). La construcción histórica del principio de precaución como respuesta

al desarrollo científico y tecnológico. *Dilemata*, 1-19. Obtenido de <https://www.dilemata.net/revista/index.php/dilemata/article/view/188/229>

Jiménez, L. (2024, p.37). *Inteligencia Artificial: responsabilidad contractual y extracontractua.*

Lloreda Camacho. Obtenido de <https://lloedacamacho.com/inteligencia-artificial-responsabilidad-contractual-y-extracontractual/>

Jonas, H. (1990, p.25). *El Principio de Responsabilidad.* (J. E. De Siqueira, Trad.) Obtenido de

[https://www.academia.edu/17837021/El\\_principio\\_Responsabilidad\\_de\\_Hans\\_Jonas](https://www.academia.edu/17837021/El_principio_Responsabilidad_de_Hans_Jonas)

Jonker, A., & Rogers, J. (2024, p.1). *¿Que es el sesgo algoritmico.* IBM. Obtenido de

[https://www.ibm.com/mx-es/think/topics/algorithmic-](https://www.ibm.com/mx-es/think/topics/algorithmic-bias#:~:text=Jonker%2C%20Julie%20Rogers-)

[bias#:~:text=Jonker%2C%20Julie%20Rogers-](https://www.ibm.com/mx-es/think/topics/algorithmic-bias#:~:text=Jonker%2C%20Julie%20Rogers-)

[,¿Qué%20es%20el%20sesgo%20algorítmico%3F, raciales%20y%20de%20género%20existentes.](https://www.ibm.com/mx-es/think/topics/algorithmic-bias#:~:text=Jonker%2C%20Julie%20Rogers-)

La Vanguardia. (28 de Diciembre de 2021, p.1). Alexa pide a una niña que ponga una moneda en

el enchufe. pág. 2. Obtenido de

<https://www.lavanguardia.com/tecnologia/20211228/7957447/alexa-reto-viral-tiktok-moneda-enchufe-pmv.html>

Lagadec, P. (1984, p.72). *La Civilizacion del riesgo.* Madrid: MAPFRE.

Laney, D. (21 de Febrero de 2001, p.1). *3D data management: Contrilling data volumen, velocity*

*and variety.* Obtenido de <http://blogs.gartner.com/doug-laney/files/2012/01/ad949-3D-Data-Management-Controlling-Data-Volume-Velocity- and-Variety.pdf>

Legalprod. (28 de 02 de 2024, p.1). *Legalprod.* Obtenido de

<https://www.legalprod.com/es/algoritmos-juridicos/>

León Serrano, G. (2017, p.61). Situación y perspectivas de las tecnologías y aplicaciones de inteligencia artificial. *Instituto Español de Documentos Estrategicos*, 39-65.

Loperena, R. D. (1998). *Los Principios del Derecho Ambiental*. Madrid, España: Civitas.

Louis De Secondat, C. (1748, p.99). *La sepracion de poderes*. (C. Fernández Muñoz, Trad.) Barcelona, Barcelona, España: Pagina Indomita. Obtenido de <http://montesquieu.ens-lyon.f>

Lozano, D. (2024). *Inteligencia artificial en el derecho penal, una discusión sobre su uso en el sistema jurídico colombiano*. Universidad Externado de Colombia. Obtenido de <https://www.uexternado.edu.co/departamento-de-derecho-penal-y-criminologia/inteligencia-artificial-en-el-derecho-penal-una-discusion-sobre-su-uso-en-el-sistema-juridico-colombiano/>

Martínez Quirante, R., & Rodríguez, J. (04 de Mayo de 2020, p.1). *Revistaidees*. Obtenido de <https://revistaidees.cat/es/el-lado-oscuro-de-la-inteligencia-artificial/>

Ministerio de Salud y Proteccion Social. (2022, p.1). *Informe sobre riesgos del plomo*. Bogotá. Obtenido de <https://www.minsalud.gov.co/sites/rid/Lists/BibliotecaDigital/RIDE/VS/PP/SA/riesgos-plomo.pdf>

Miró Llinares, F. (2018). INTELIGENCIA ARTIFICIAL Y JUSTICIA PENAL: MAS ALLA DE LOS RESULTADOS LESIVOS CAUSADO POR ROBOTS. *Revista de Derecho Penal y criminología*, 87-130. Recuperado el 10 de 09 de 2024, de <https://revistas.uned.es/index.php/RDPC/article/view/26446/20937>

Monsalve Mantilla, M. D. (2021, P.19). Animales silvestres y derecho procesal constitucional.

*DIXI*, 24(1), 1-24. doi:<https://doi.org/10.16925/2357-5891.2022.01.03>

Morales, C. (2021, p.20). El impacto de la inteligencia artificial. *ADVOCATUS*. Obtenido de

<file:///C:/Users/USUARIO/Downloads/5117-Texto%20del%20art%C3%ADculo-18860-1-10-20210325.pdf>

NORTHPOINTE. (2015). *Practitioner's Guide to COMPAS Core Northpointe Inc*. Obtenido de

<https://archive.epic.org/algorithmic-transparency/crim-justice/EPIC-16-06-23-WI-FOIA-201600805-COMPASPractitionerGuide.pdf>

OCDE. (11 de 2022, p.1). *APROVECHANDO EL PODER DE LA IA Y LAS TECNOLOGIAS EMERGENTES*. Obtenido de

[https://www.oecd.org/content/dam/oecd/es/publications/reports/2022/11/harnessing-the-power-of-ai-and-emerging-technologies\\_c74e020c/6e76bc18-es.pdf](https://www.oecd.org/content/dam/oecd/es/publications/reports/2022/11/harnessing-the-power-of-ai-and-emerging-technologies_c74e020c/6e76bc18-es.pdf)

ONU. (1972, p.1). Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura.

Convenio para la Protección del Patrimonio Mundial, Cultural y natural., (págs. 1-89). Estocolmo. Obtenido de

<https://documents.un.org/doc/undoc/gen/n73/039/07/pdf/n7303907.pdf>

Organizacion de Estados Americanos. (1969). *Convencion Americana de Derechos Humanos*. Art.

8. San Jose de Costarrica. Obtenido de [https://www.oas.org/dil/esp/1969\\_Convenci%C3%B3n\\_Americana\\_sobre\\_Derechos\\_Humanos.pdf](https://www.oas.org/dil/esp/1969_Convenci%C3%B3n_Americana_sobre_Derechos_Humanos.pdf)

Organización de Naciones Unidas. (1992, p.1). Declaración de Rio sobre el Medio Ambiente y el Desarrollo. Rio de Janeiro. Obtenido de <https://www.un.org/spanish/esa/sustdev/agenda21/riodeclaration.htm>

Organización de Naciones Unidas, ONU. (1992, p.1). Declaración de Rio sobre el Medio Ambiente y el Desarrollo. Rio de Janeiro. Obtenido de <https://www.un.org/spanish/esa/sustdev/agenda21/riodeclaration.htm>

Ortiz, F. A., & Ortiz, F. S. (2024, p.28). Responsabilidad civil en la era digital: Daños causados por inteligencia artificial. *BLOG-OPINAN LOS ESTUDIANTES*. Obtenido de <https://geneticayderecho.uexternado.edu.co/responsabilidad-civil-en-la-era-digital-danos-causados-por-inteligencia-artificial/>

Osorio Alvis, M. A. (2021). Una aproximación a la articulación del derecho internacional humanitario y el juicio de responsabilidad extracontractual del Estado: análisis del principio de distinción por ataque, incursiones o toma guerrillera a una población en la jurisprudencia del Consejo de Estado de Colombia. Universidad Externado de Colombia.

Parlamento Europeo y del Consejo. (13 de 06 de 2024, p.1). *Unión Europea*. Obtenido de [https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=OJ%3AL\\_202401689](https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=OJ%3AL_202401689)

Pont, A., Angostina Passera, M., & Castilla, K. (2022, p.10). *Impactos de las Nuevas Tecnologías en los Derechos Humanos*. Barcelona: Open Society Foundations. Obtenido de <https://www.ohchr.org/sites/default/files/documents/issues/digitalage/cfis/tech-standards/subm-standard-setting-digital-space-new-technologies-csos-idhc-4-annex.pdf>

Robledo, P. (14 de 2 de 2024, p.15). El Estado Enfrenta mas de 353.000 proceso judiciales cuyas pretensiones sumas cerca de 603 billoes de pesos. Ambito Jurídico . Recuperado el 12 de 05 de 2024, de <https://www.ambitojuridico.com/noticias/invitado/administrativo-y-contratacion/el-estado-enfrenta-mas-de-353000-procesos>

Rodríguez Rodríguez, P. (2018, p.111). *Inteligencia Artificial: Cómo cambiará al mundo y tu vida*. (J. Rizzo Tortuero , Trad.) Deusto.

Rodríguez, M. L., Morales, K. d., Chapa, A. d., & Zambrano, D. J. (2024). Impacto de Herramientas de IA Generativa en la Motivación y Satisfacción de Estudiantes de Nivel Superior de la Facultad de Ciencias y Tecnologías de la Información. *Ciencia Latina Revista Científica Multidisciplinar*.

Sentencia Exp. 21359 (13 de Marzo de 2013).

Serres, M. (1998, p.49). Muertes. (M. Gómez, & L. Paláu , Edits.) *Extension Cultural Universidad Nacional*, 47-55. Obtenido de [https://medellin.unal.edu.co/revista-extension-cultural/images/revista/rec48/REC\\_48-45-53.pdf](https://medellin.unal.edu.co/revista-extension-cultural/images/revista/rec48/REC_48-45-53.pdf)

Soto, C. K. (2018). *El principio de precaución en el sistema de solución de diferencias*. Universidad de Chile.

Steele, K. (2006, p.21). The precautionary principle: a new approach to public decision-making. *Law, Probability and Risk*, 19-31.

Simón Castellano, P. (2021). Inteligencia artificial y administración de justicia: ¿Quo vadis, justitia? IDP. Revista de Internet, Derecho y Política, (33), 1–18. Universitat Oberta de Catalunya. <https://idp.uoc.edu>

Suárez Manrique, W. Y., De León Vargas, G. I., & Luna Salas, F. (2019). Inteligencia artificial y su aplicación en la administración de justicia. Revista Vía Iuris, 11(21), 71–83. <https://revistas.libertadores.edu.co/index.php/ViaIuris/article/view/862>

The New York Times. (9 de 11 de 2023, p.1). ¿Los chatbots inventan? Un estudio indica que más de lo que creíamos.

Turing, A. (2010, p.22). Maquinaria Computacional e Inteligencia. 1-22. (C. Fuentes Barassi, Trad.) Obtenido de <http://xamanek.izt.uam.mx/map/cursos/Turing-Pensar.pdf>

Ulrich , B. (1998, p.233). *La Sociedad del Riesgo, Hacia una nueva modernidad*. (J. Navarro, D. Jimenez , & M. R. Borrás, Trads.) Buenos Aires: Paidós Iberica S.A. Obtenido de <https://www.gub.uy/sistema-nacional-emergencias/sites/sistema-nacional-emergencias/files/documentos/publicaciones/La%2Bsociedad%2Bdel%2Briesgo%2Bhacia%2Buna%2Bnueva%2Bmodernidad%20-BECK.pdf>

Union Europea. (1987, p.1). ACTA UNICA EUROPEA. (pág. 28). Luxemburgo: Diario Oficial de las Comunidades Europeas. Obtenido de <https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=LEGISSUM%3Axy0027>

Union Europea. (3 de Marzo de 2010, p.86). Tratado de Funcionamiento de la union Europea. Boletín Oficial. Obtenido de [http://data.europa.eu/eli/treaty/tfeu\\_2016/art\\_191/oj](http://data.europa.eu/eli/treaty/tfeu_2016/art_191/oj)

Wayne Gregory, R., Henfridsson, O., Kaganer Evgeny, & Kyriakou , H. (2021, p.425). Data Network Effects for Creating User Value. 46, 421-430. doi:<https://doi.org/10.5465/amr.2019.0178>

WIRED. (1 de 05 de 2023, p.1). *El inesperado uso de agua que exige ChatGPT y su impacto para el planeta*. Obtenido de <https://es.wired.com/articulos/el-inesperado-uso-de-agua-que-exige-chatgpt-y-su-impacto-para-el-planeta>

Yepes Gómez, F. (24 de 12 de 2021, p.11). La mora judicial, ¿un problema de sistema procesal? *DIXI*, 24(1), 1-24. Obtenido de <https://doi.org/10.16925/2357-5891.2022.01.07>