

LÍMITES DEL DERECHO PENAL FRENTE A LA RESPONSABILIDAD DE PERSONAS JURÍDICAS EN ESCENARIOS DE USO DE INTELIGENCIA ARTIFICIAL Y POSIBLES CONSECUENCIAS JURÍDICAS APLICABLES EN COLOMBIA.

Paola Pacheco¹

Resumen

Se analizan en la presente investigación los límites del derecho penal colombiano frente a la intervención de las personas jurídicas en escenarios de uso de inteligencia artificial dentro de entornos empresariales; el estudio parte de la inexistencia de un régimen de responsabilidad penal directa para las personas jurídicas en Colombia y además explora cómo el uso de las nuevas tecnologías ha venido generando dificultades para identificar responsables individuales cuando intervienen sistemas automatizados en procesos empresariales con relevancia jurídica.

Se identifican distintas consecuencias jurídicas aplicables a las organizaciones, partiendo del análisis normativo, jurisprudencial y doctrinal, especialmente desde ámbitos administrativos y preventivos; de esta misma manera se desarrollan criterios jurídicos relacionados con el beneficio obtenido por la organización, el control organizacional, el deber de prevención y la trazabilidad tecnológica, los cuales permiten profundizar en la intervención de las personas jurídicas en escenarios donde se utilizan herramientas de inteligencia artificial.

Al cierre se concluye que aunque el derecho penal colombiano mantiene una estructura que

¹ Abogada, candidata a magister en Derecho Penal y Procesal Penal

se fundamenta en la responsabilidad del individuo, el ordenamiento jurídico sí tiene mecanismos que permiten reaccionar frente a actuaciones empresariales mediadas por tecnologías automatizadas; pero también es posible ver una clara necesidad de fortalecer herramientas de supervisión, control y prevención frente a los riesgos derivados del uso de inteligencia artificial en el ámbito empresarial².

Palabras clave

Inteligencia artificial; personas jurídicas; derecho penal; responsabilidad empresarial; consecuencias jurídicas; control organizacional; trazabilidad tecnológica.

Abstract

This research analyzes the limits of Colombian criminal law regarding the intervention of legal entities in scenarios involving the use of artificial intelligence within business environments; the study is based on the absence of a direct criminal liability regime for legal entities in Colombia and examines how new technological dynamics have created difficulties in identifying individual responsibility when automated systems participate in business processes with legal relevance.

Through a normative, jurisprudential, and doctrinal analysis, the research identifies different legal consequences applicable to organizations, particularly from administrative, regulatory, and preventive perspectives; likewise, it develops legal criteria related to organizational

² **Nota sobre el uso de inteligencia artificial.** En la elaboración de este trabajo se utilizó inteligencia artificial como herramienta de asistencia académica, con una participación aproximada del 20%, exclusivamente para apoyar procesos de búsqueda de información, organización de ideas, revisión de estilo y mejora de la redacción; el análisis jurídico, la selección y verificación de las fuentes, la construcción de la argumentación, las conclusiones y el contenido final fueron desarrollados, revisados y validados por la autora, quien asume la responsabilidad integral sobre el trabajo presentado.

benefit, organizational control, duty of prevention, and technological traceability, which make it possible to examine the involvement of legal entities in scenarios where artificial intelligence tools are used.

The research concludes that, although Colombian criminal law continues to be structured around individual liability, the legal system already contains mechanisms capable of responding to business conduct mediated by automated technologies; nevertheless, the study also highlights the need to strengthen supervision, control, and prevention mechanisms regarding the risks associated with the use of artificial intelligence in business activities.

Keywords

Artificial intelligence; legal entities; criminal law; corporate liability; legal consequences; organizational control; technological traceability.

TABLA DE CONTENIDO

I. INTRODUCCIÓN

1. MARCO NORMATIVO, JURISPRUDENCIAL Y DOCTRINAL EXISTENTE EN COLOMBIA CON RELACIÓN A LAS CONSECUENCIAS JURÍDICAS APLICABLES A LAS PERSONAS JURÍDICAS.

1.1 Marco normativo de la responsabilidad de las personas jurídicas en Colombia en escenarios de uso de inteligencia artificial

1.2 Capítulo 2; marco doctrinal de la responsabilidad de las personas jurídicas en Colombia en escenarios de uso de inteligencia artificial

1.3 Capítulo 3; marco Jurisprudencial de la responsabilidad de las personas jurídicas en

Colombia en escenarios de uso de inteligencia artificial

2. CONCEPTO Y LOS USOS DE LA INTELIGENCIA ARTIFICIAL, SU IMPLEMENTACIÓN EN ENTORNOS EMPRESARIALES Y LOS POSIBLES ESCENARIOS EN LOS QUE PUEDE INTERVENIR EN ACTUACIONES CON RELEVANCIA JURÍDICA.

2.1; concepto de inteligencia artificial

2.2 Implementación y funcionamiento de la inteligencia artificial en entornos empresariales

2.3 3; escenarios prácticos de uso de la inteligencia artificial con relevancia jurídica en entornos empresariales.

3. LÍMITES DEL DERECHO PENAL COLOMBIANO FRENTE A LAS PERSONAS JURÍDICAS EN ESCENARIOS DE USO DE INTELIGENCIA ARTIFICIAL Y CRITERIOS PARA SU VINCULACIÓN JURÍDICA.

3.1. Límites del derecho penal colombiano frente a la responsabilidad de las personas jurídicas.

3.2. Criterios jurídicos para vincular a las personas jurídicas en escenarios de uso de inteligencia artificial

3.3. Aplicación de criterios jurídicos frente a la intervención de personas jurídicas en escenarios de inteligencia artificial en Colombia.

CONCLUSIONES

BIBLIOGRAFÍA

I. INTRODUCCIÓN

En Colombia aún no existe un régimen de responsabilidad penal directa para las personas jurídicas, lo que ha generado múltiples discusiones frente a la manera en que el derecho penal debe responder cuando una empresa participa o se beneficia de una conducta ilícita; y aunque el ordenamiento jurídico contempla algunas consecuencias administrativas y procesales para las organizaciones, la estructura tradicional del sistema penal continúa enfocada principalmente en la responsabilidad individual de las personas naturales.

Esta discusión es fundamental si se tiene en cuenta el uso cada vez más frecuente de sistemas de inteligencia artificial dentro de las empresas; actualmente, muchas decisiones relacionadas con atención al cliente, análisis de datos, otorgamiento de créditos, selección de personal o estrategias comerciales son desarrolladas mediante herramientas

automatizadas que operan con cierto grado de autonomía; en estos escenarios, no siempre resulta sencillo establecer quién adoptó realmente una decisión o hasta dónde llega el control humano sobre el sistema utilizado (OECD, 2019).

Lo mencionado anteriormente plantea un problema jurídico importante, especialmente cuando el uso de estas tecnologías da lugar a afectaciones de derechos, fraudes, vulneraciones de datos personales u otras actuaciones con relevancia jurídica; en ese contexto, nace la necesidad de analizar cuáles son los límites del derecho penal colombiano frente a la intervención de las personas jurídicas en este tipo de escenarios y si las consecuencias jurídicas actualmente previstas resultan suficientes frente a las nuevas dinámicas empresariales mediadas por inteligencia artificial (Prieto, 2022).

En efecto, el desarrollo de las actividades empresariales y la globalización han permitido la aparición de nuevas formas de criminalidad, en las cuales las personas jurídicas participan, directa o indirectamente, en la afectación de bienes jurídicos protegidos por el legislador; frente a ello, distintos sectores doctrinales han advertido que el ordenamiento jurídico colombiano presenta vacíos en esta materia, particularmente frente a la manera en que el derecho penal debe responder cuando las conductas se desarrollan dentro de estructuras empresariales complejas (Petro-González, Mosquera & Torres, 2014).

Desde un nivel normativo, aunque no existe una regulación expresa de responsabilidad penal para personas jurídicas, sí se han establecido mecanismos que permiten imponer consecuencias jurídicas relevantes; De manera pues que el artículo 91 de la Ley 906 de 2004 contempla la posibilidad de suspender o cancelar la personería jurídica cuando ésta haya sido utilizada para la comisión de delitos; de esta misma manera normas como la Ley 1778 de 2016 y la Ley 1474 de

2011 desarrollan mecanismos sancionatorios principalmente en lo que se refiere a corrupción, lo que evidencia ciertos avances, aunque todavía insuficientes frente a las nuevas dinámicas empresariales y tecnológicas.

A lo mencionado anteriormente se suma el desarrollo tecnológico y el uso cada vez más frecuente de sistemas de inteligencia artificial en entornos corporativos; actualmente, muchas empresas implementan herramientas automatizadas para el análisis de datos, atención de usuarios, contratación de personal, seguridad financiera y toma de decisiones comerciales; aunque estas tecnologías han optimizado múltiples procesos, también han generado escenarios en los que resulta más complejo identificar quién adopta realmente una decisión o hasta dónde llega el control humano sobre el sistema utilizado.

En consecuencia, la implementación de inteligencia artificial dentro de estructuras empresariales plantea nuevos desafíos para el derecho penal, particularmente porque los criterios tradicionales de imputación resultan limitados frente a escenarios donde intervienen sistemas automatizados con cierto grado de autonomía (Del Rosal, 2023); así, la problemática no solo gira en torno a la inexistencia de responsabilidad penal directa para las personas jurídicas, sino también alrededor de los límites del derecho penal colombiano y de la suficiencia de las consecuencias jurídicas actualmente previstas para responder a estas nuevas realidades tecnológicas y empresariales; lo mencionado anteriormente nos llevó a plantearnos como pregunta problema el determinar: ¿Cuáles son los límites del derecho penal frente a la responsabilidad de personas jurídicas en escenarios de uso de inteligencia artificial y posibles consecuencias jurídicas aplicables en Colombia?

Para responder a la pregunta anterior nos propusimos como objetivo general: analizar cuáles son los límites del derecho penal frente a la responsabilidad de personas jurídicas en escenarios de uso de inteligencia artificial y posibles consecuencias jurídicas aplicables en Colombia; y como objetivos específicos: i; analizar el marco normativo, jurisprudencial y doctrinal existente en Colombia Con relación a la responsabilidad penal y consecuencias jurídicas aplicables a las personas jurídicas. ii; examinar el concepto y los usos de la inteligencia artificial, su implementación en entornos empresariales y los posibles escenarios en los que puede actuar con relevancia jurídica; y iii; determinar los posibles límites del derecho penal colombiano frente a las personas jurídicas en escenarios de uso de inteligencia artificial y criterios para su vinculación jurídica.

La presente investigación se despliega en el marco del programa de Maestría en Derecho Penal y Procesal Penal, y se desarrolla bajo una estrategia metodológica que comprende: tipo de investigación básica jurídica, método lógico cualitativo, las técnicas de recolección de datos de investigación documental, de carácter informativo, expositivo y crítico y el enfoque de la investigación cualitativo analítico; la investigación es de tipo básica jurídica, en la medida en que busca analizar un problema jurídico a partir de la interpretación del desarrollo normativo, jurisprudencial y doctrinal relacionado con la responsabilidad penal de las personas jurídicas en Colombia; se desarrollará bajo un modelo descriptivo y explicativo, en tanto que se identificarán y analizarán los referentes legales, jurisprudenciales y doctrinales sobre la materia, con el fin de comprender las dificultades existentes para atribuir responsabilidad en el marco jurídico vigente; de esta misma manera se tendrá en cuenta el contexto actual, de manera especial en lo relacionado con el uso de

las tecnologías de inteligencia artificial en entornos empresariales, lo que permitirá examinar su incidencia en la aplicación de los criterios jurídicos tradicionales.

Se destaca también que se empleará el método lógico-cualitativo, a partir del cual se analizarán e interpretarán las normas, conceptos y criterios jurídicos relacionados con la responsabilidad penal de las personas jurídicas en Colombia; mediante este método, se busca entonces comprender cómo el marco jurídico vigente puede aplicarse a escenarios en los que interviene la inteligencia artificial en el ámbito empresarial; el enfoque de la investigación es cualitativo analítico, en tanto que se basa en el análisis e interpretación de normas jurídicas, jurisprudencia y algunos planteamientos doctrinales relacionados con la responsabilidad de las personas jurídicas en Colombia; a partir de este enfoque, se examinarán las principales dificultades que existen para atribuir responsabilidad a las personas jurídicas, teniendo en cuenta principios del derecho penal como el *societas delinquere non potest*, entre otros.

Como resultado de lo mencionado anteriormente, la presente investigación se estructura en tres partes principales; en la primera, correspondiente a la introducción, se desarrolla el problema de investigación, su planteamiento, la pregunta problema, la hipótesis, los objetivos, la justificación y la metodología empleada, incluyendo el tipo de investigación, el método, las técnicas de recolección de la información y el enfoque adoptado; en la segunda parte, denominada resultados de la investigación, se abordará el estudio del tema a partir de tres títulos; en el primer título se analizará el desarrollo normativo, jurisprudencial y doctrinal relacionado con la responsabilidad de las personas jurídicas en Colombia; en el segundo título se contextualizará el problema de investigación a partir del análisis de escenarios en los que interviene la inteligencia artificial en entornos empresariales; Para dar

cierre en el tercer título se realizará un análisis orientado a establecer criterios jurídicos que permitan examinar la posible atribución de responsabilidad a las personas jurídicas en estos escenarios, conforme al marco jurídico vigente; en la tercera parte se presentarán las conclusiones, en las cuales se dará respuesta a la pregunta problema, se verificará la hipótesis planteada y se evaluará el cumplimiento de los objetivos de la investigación.

1. MARCO NORMATIVO, JURISPRUDENCIAL Y DOCTRINAL EXISTENTE EN COLOMBIA CON RELACIÓN A LAS CONSECUENCIAS JURÍDICAS APLICABLES A LAS PERSONAS JURÍDICAS.

1.1 Marco normativo de la responsabilidad de las personas jurídicas en Colombia en escenarios de uso de inteligencia artificial

El derecho penal En Colombia, ha estado (por tradición) orientado hacia la responsabilidad de las personas naturales, en atención a su capacidad de actuar con conciencia y voluntad; este enfoque ha limitado la posibilidad de atribuir responsabilidad penal directa a las personas jurídicas, en tanto que estas no cuentan con una voluntad propia en los términos exigidos por la teoría clásica del delito, definido como una acción humana típica, antijurídica y culpable; pero el uso cada vez más frecuente de sistemas de inteligencia artificial dentro de las empresas ha generado nuevos escenarios en los que muchas decisiones y actuaciones con relevancia jurídica ya no dependen exclusivamente de una persona natural identificable, lo que ha reabierto la discusión sobre los límites del derecho penal frente a la intervención de las organizaciones en este tipo de contextos.

Pero el ordenamiento jurídico colombiano ha previsto algunas figuras que permiten vincular a las personas jurídicas cuando estas se ven involucradas en la comisión de conductas ilícitas, sin que ello implique necesariamente la intervención del derecho penal o

la atribución de responsabilidad penal directa; con relación a lo mencionado anteriormente, una de las disposiciones más relevantes se encuentra en el artículo 91 de la Ley 906 de 2004, el cual permite la suspensión o cancelación de la personería jurídica cuando existan motivos fundados para inferir que ha sido utilizada para el desarrollo de actividades delictivas (Congreso de la República, 2004); este tipo de medidas adquiere especial relevancia en escenarios donde las actividades empresariales son desarrolladas mediante herramientas tecnológicas o sistemas automatizados que pueden incidir en actuaciones con consecuencias jurídicas.

Aplicar el artículo 91 de la Ley 906 de 2004 exige la verificación de presupuestos jurídicos específicos que impiden considerar la suspensión o cancelación de la personería jurídica como una consecuencia automática derivada de la investigación penal; primero la norma exige la existencia de motivos fundados para inferir que la persona jurídica ha sido utilizada, total o parcialmente, para la realización de actividades delictivas; este estándar supone la existencia de elementos objetivos que permitan establecer una relación razonable entre la organización y la conducta investigada, sin que resulte suficiente la simple vinculación de alguno de sus integrantes a un proceso penal; la decisión judicial debe sustentarse en elementos probatorios que permitan concluir, de manera preliminar, que la estructura empresarial fue instrumentalizada para facilitar o encubrir la comisión del delito (Silva, 2008).

Esta exigencia desde lo dogmático responde al principio de responsabilidad personal que caracteriza al derecho penal contemporáneo; la doctrina ha expresado que las consecuencias jurídicas dirigidas contra una persona jurídica únicamente encuentran justificación cuando existe una vinculación suficientemente acreditada entre el

funcionamiento de la organización y la actividad ilícita desarrollada, evitando que la sola existencia de un delito cometido por uno de sus integrantes produzca automáticamente efectos sobre toda la empresa; de manera pues que el análisis debe dirigirse a establecer si la organización fue utilizada como instrumento para la realización de actividades ilícitas o si las condiciones de su funcionamiento facilitaron de manera relevante la producción del resultado (Bacigalupo, 2016).

El artículo 91 hace una diferencia entre las dos medidas con alcances distintos; la suspensión de la personería jurídica posee un carácter temporal y busca impedir que la organización continúe desarrollando actividades mientras avanza el proceso penal, especialmente cuando existe riesgo de que siga siendo utilizada para la comisión de conductas ilícitas; por otro lado la cancelación constituye una medida de mayor intensidad, aplicable únicamente cuando las circunstancias del caso pone en evidencian que la persona jurídica ha sido utilizada de manera permanente o predominante como instrumento para la realización de actividades delictivas; en ambos casos, la decisión exige una valoración judicial motivada que respete plenamente las garantías propias del debido proceso (Gómez, 2016).

Se ha precisado desde la jurisprudencia colombiana que estas medidas poseen naturaleza cautelar y preventiva, por lo que no constituyen una pena en sentido estricto ni implican el reconocimiento de una responsabilidad penal autónoma de la persona jurídica; su finalidad consiste en evitar que la organización continúe siendo utilizada para la ejecución de actividades ilícitas durante el desarrollo del proceso penal, preservando simultáneamente los principios de legalidad, proporcionalidad y debido proceso que rigen toda actuación judicial; en consecuencia, la suspensión o cancelación de la personería jurídica no

reemplaza la responsabilidad penal de las personas naturales eventualmente involucradas, sino que constituye una respuesta jurídica excepcional dirigida a proteger el orden jurídico frente a organizaciones cuya actividad ha servido como medio para la comisión de delitos (Del Rosal, 2023).

Estos requisitos adquieren una importancia aún mayor cuando las organizaciones incorporan sistemas de inteligencia artificial dentro de sus procesos empresariales; la utilización de herramientas automatizadas no elimina la necesidad de acreditar que la empresa ejercía dirección, supervisión o control sobre dichos sistemas, ni exonera al juez de demostrar que la organización fue utilizada para la realización de actividades ilícitas; por el contrario, la creciente complejidad tecnológica exige una valoración aún más rigurosa acerca de la existencia de mecanismos efectivos de control, de los programas de cumplimiento implementados y del grado de intervención de la organización en los resultados producidos mediante inteligencia artificial, evitando atribuciones automáticas incompatibles con los principios estructurales del derecho penal (Januário, 2023).

Así, el artículo 91 de la Ley 906 de 2004 constituye una de las principales herramientas jurídicas previstas por el ordenamiento colombiano para reaccionar frente a la utilización indebida de personas jurídicas en actividades ilícitas; pero su aplicación se encuentra condicionada al cumplimiento de estrictos requisitos materiales y procesales que ponen en evidencia que el legislador colombiano optó por establecer consecuencias jurídicas excepcionales para las organizaciones, sin llegar a reconocer un régimen general de responsabilidad penal directa para las personas jurídicas (Prieto, 2022).

Aunque esta medida no constituye una sanción penal en sentido estricto, sí representa una consecuencia jurídica importante que afecta directamente a la persona jurídica, lo que

evidencia que el ordenamiento jurídico colombiano contempla mecanismos de reacción frente a la intervención de las empresas en conductas ilícitas, aun cuando dichas respuestas no se desarrollen necesariamente desde la esfera penal (Tolosa, 2015).

En el ámbito administrativo se han desarrollado normas orientadas a sancionar a las personas jurídicas, de manera especial en lo que se refiere a corrupción; la Ley 1778 de 2016, por la cual se dictan normas sobre la responsabilidad de las personas jurídicas por actos de corrupción transnacional, establece un régimen sancionatorio para las empresas involucradas en actos de soborno transnacional, permitiendo la imposición de multas, inhabilidades y otras medidas que afectan su funcionamiento (Congreso de la República, 2016); aunque esta regulación no fue creada específicamente para escenarios de inteligencia artificial, sí depone en evidencia que el ordenamiento jurídico colombiano ha venido ampliando los mecanismos de control frente a conductas desarrolladas dentro de estructuras empresariales complejas.

De esta misma manera la Ley 1474 de 2011, orientada a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública, y la Ley 2195 de 2022, que adopta medidas en lo que se refiere a transparencia, prevención y lucha contra la corrupción, han fortalecido los mecanismos de prevención y control, promoviendo la implementación de programas de cumplimiento (compliance) en las organizaciones, con el fin de evitar la comisión de conductas ilícitas (Congreso de la República, 2011; 2022); este tipo de herramientas adquiere una importancia particular en escenarios donde las empresas utilizan sistemas automatizados o tecnologías de inteligencia artificial, en tanto que refuerzan el deber de supervisión y control sobre las actividades desarrolladas dentro de la organización (FATF, 2021).

A su vez, la Superintendencia de Industria y Comercio, mediante la Circular Externa No. 002 del 21 de agosto de 2024, estableció lineamientos sobre el uso de la inteligencia artificial en entornos empresariales, dada la importancia de garantizar la transparencia, el control y la supervisión en la implementación de estas tecnologías; estas directrices advierten que las empresas no pueden desligarse de las decisiones que se adopten a través de sistemas automatizados, sino que mantienen el deber de vigilancia sobre su funcionamiento.

Tal regulación también guarda relación con el régimen de protección de datos personales, en la medida en que refuerza obligaciones ya previstas en la Ley 1581 de 2012, de manera especial en lo relacionado con el tratamiento adecuado de la información y la responsabilidad de quienes la administran; dicha ley establece en su artículo 23 un régimen sancionatorio aplicable a entidades de naturaleza privada, que incluye multas de carácter personal e institucional, la suspensión de las actividades relacionadas con el tratamiento de datos, el cierre temporal de las operaciones e incluso el cierre inmediato y definitivo de las actividades que involucren dicho tratamiento; aunque estas medidas pertenecen principalmente al ámbito administrativo, reflejan que el ordenamiento jurídico sí contempla consecuencias relevantes frente a actuaciones empresariales desarrolladas mediante tecnologías que puedan afectar derechos de terceros.

La Superintendencia de Industria y Comercio, mediante la Circular Externa 01 de 2025, fijó una serie de lineamientos sobre el tratamiento de datos personales en servicios financieros digitales, de manera especial en aquellos que funcionan a través de aplicaciones tecnológicas; esta circular pone especial atención en el uso de herramientas automatizadas, indicando que el manejo de la información debe respetar principios como la finalidad, la minimización de datos y el consentimiento informado; además, establece que las personas

tienen derecho a recibir una explicación clara cuando una decisión automatizada les afecte, aspecto que adquiere relevancia en escenarios como la aprobación de créditos o servicios financieros.

También establece reglas estrictas para el uso de datos sensibles, como los biométricos, reforzando la necesidad de proteger la información de los usuarios en entornos digitales; aunque esta circular no regula directamente la responsabilidad penal de las empresas, sí empieza a fijar límites y deberes frente al uso de herramientas automatizadas, lo que evidencia que el ordenamiento jurídico colombiano ha comenzado a adaptarse progresivamente a estos nuevos escenarios tecnológicos.

En lo que refiere a inteligencia artificial se han venido implementando políticas orientadas a promover su desarrollo y utilización responsable; muestra de ello es el CONPES 4144 de 2025, mediante el cual se establecen lineamientos de política pública dirigidos a fomentar el desarrollo, uso y adopción responsable de estas tecnologías en el país; este documento no crea obligaciones penales ni regula directamente la responsabilidad jurídica de las empresas, pero sí reconoce la necesidad de implementar principios como la transparencia, la ética y la supervisión en el uso de la inteligencia artificial.

Este tipo de iniciativas muestran que el país ha comenzado a adaptarse a los retos que trae consigo la inteligencia artificial en el ámbito empresarial; pero todavía persisten vacíos frente a la manera en que deben abordarse las consecuencias jurídicas derivadas de actuaciones desarrolladas mediante sistemas automatizados, de manera especial en el ámbito penal, donde continúan existiendo límites frente a la atribución de responsabilidad a las personas jurídicas (OECD, 2019).

En Colombia también se han presentado iniciativas legislativas orientadas a regular la

inteligencia artificial, como el Proyecto de Ley 043-2025S, el cual busca impulsar el desarrollo y uso de la inteligencia artificial en Colombia, promoviendo el conocimiento, la infraestructura tecnológica y la innovación, con el fin de fortalecer la economía y la competitividad del país, bajo un enfoque ético, inclusivo y responsable, que garantice el respeto de los derechos fundamentales dentro del marco jurídico vigente (Cámara de representantes de Colombia, 2024); aunque esta iniciativa aún se encuentra en trámite, su presentación evidencia el interés del legislador en avanzar hacia la regulación de la inteligencia artificial y en responder a los desafíos jurídicos que su implementación plantea en distintos ámbitos, particularmente en escenarios empresariales donde el uso de tecnologías automatizadas puede generar consecuencias con relevancia jurídica.

Las corrientes doctrinales examinadas permiten advertir que la discusión contemporánea ya no se centra en determinar si las personas jurídicas pueden participar en la realización de conductas con relevancia penal, sino en establecer cuál es el fundamento jurídico que justificaría su eventual responsabilidad; mientras la hetero-rresponsabilidad mantiene el protagonismo de la actuación de las personas naturales que reafirman a la organización, la autorresponsabilidad desplaza el análisis hacia los defectos de organización, los mecanismos de control y los deberes de supervisión empresarial; ambas construcciones aportan herramientas útiles para comprender la criminalidad empresarial; pero ninguna resulta plenamente trasladable al ordenamiento colombiano, debido a que este continúa estructurado sobre el principio de responsabilidad penal individual y no reconoce un régimen general de responsabilidad penal para las personas jurídicas (Gómez, 2016).

Esta investigación adopta entonces una posición intermedia; se considera que los desarrollos doctrinales sobre organización empresarial, cumplimiento normativo y control

interno constituyen referentes útiles para interpretar las consecuencias jurídicas actualmente previstas en el ordenamiento colombiano, de manera especial en escenarios de utilización de inteligencia artificial; no obstante, también es posible dar cierre con la idea de que dichos avances no justifican, por sí solos, la incorporación inmediata de un modelo de responsabilidad penal empresarial, pues ello exigiría una reforma legislativa integral que armonizara dicha transformación con los principios de legalidad, culpabilidad, personalidad de la pena y ultima ratio que orientan el derecho penal colombiano (Silva, 2008).

1.2 Marco doctrinal de la responsabilidad de las personas jurídicas en Colombia en escenarios de uso de inteligencia artificial

La discusión doctrinal sobre la responsabilidad penal de las personas jurídicas constituye uno de los debates más relevantes de la dogmática penal contemporánea; durante gran parte del desarrollo histórico del derecho penal predominó la máxima *societas delinquere non potest*, según la cual únicamente las personas naturales podían ser sujetos de responsabilidad penal, al considerarse que solo ellas poseen capacidad de acción, culpabilidad y conciencia de la ilicitud. Bajo esta concepción, las personas jurídicas eran entendidas como construcciones normativas incapaces de realizar una conducta típica en sentido penal, razón por la cual cualquier consecuencia jurídica derivada de una actuación empresarial debía recaer exclusivamente sobre las personas naturales que actuaban en su nombre (Silva, 2008).

Pero el crecimiento de las estructuras empresariales, la complejidad de las organizaciones económicas y la aparición de nuevas formas de criminalidad corporativa llevaron a replantear progresivamente esta concepción clásica; la doctrina comenzó a advertir que

numerosos delitos económicos, financieros, ambientales y de corrupción no podían explicarse únicamente desde la actuación aislada de una persona natural, sino que respondían a decisiones adoptadas dentro de organizaciones complejas cuya estructura interna favorecía o facilitaba la producción de resultados ilícitos; esta realidad impulsó el desarrollo de nuevas construcciones dogmáticas orientadas a explicar la posible intervención de las personas jurídicas en la comisión de conductas con relevancia penal (Silva, 2008).

Partiendo de esta mirada, el debate dejó de centrarse exclusivamente en determinar si una persona jurídica posee voluntad propia y pasó a concentrarse en establecer cuáles son los fundamentos jurídicos que permitirían atribuirle responsabilidad sin desconocer los principios tradicionales del derecho penal; en consecuencia, la doctrina contemporánea comenzó a construir modelos de imputación que buscan responder a las particularidades de la criminalidad empresarial, caracterizada por la división funcional del trabajo, la descentralización en la toma de decisiones y la existencia de complejas estructuras organizacionales que dificultan la clara identificación de un único responsable individual (Bacigalupo, 2016).

Entonces, la evolución doctrinal ha evidenciado que la discusión sobre la responsabilidad de las personas jurídicas no responde únicamente a una necesidad de política criminal, sino también a la transformación de los escenarios donde actualmente se producen numerosas conductas lesivas para bienes jurídicos de especial importancia; la empresa moderna ya no constituye únicamente un espacio donde actúan personas naturales, sino una organización dotada de procedimientos internos, sistemas de control, modelos de gestión y mecanismos de decisión que pueden incidir directamente en la producción de riesgos jurídicamente

relevantes; por ello, buena parte de la doctrina penal contemporánea considera que el análisis debe desplazarse desde la conducta individual hacia el funcionamiento mismo de la organización cuando este facilite o propicie la comisión de hechos ilícitos (Gómez, 2016).

Esta es una evolución que también ha sido impulsada por el desarrollo tecnológico y la creciente incorporación de sistemas automatizados dentro de las organizaciones; actualmente, numerosas decisiones empresariales relacionadas con procesos de contratación, evaluación de riesgos, segmentación de clientes, tratamiento de datos personales o gestión financiera son adoptadas mediante herramientas de inteligencia artificial, circunstancia que complejiza aún más la clara identificación del sujeto que materialmente interviene en la producción del resultado; en estos escenarios, la doctrina advierte que las categorías tradicionales de imputación penal enfrentan importantes desafíos, debido a que las decisiones dejan de depender exclusivamente de una actuación humana directa y pasan a desarrollarse mediante procesos organizacionales mediados por tecnologías de creciente autonomía funcional (Prieto, 2022).

Pero el reconocimiento de estos nuevos escenarios no implica aceptar automáticamente la responsabilidad penal de las personas jurídicas; por el contrario, buena parte de la doctrina expresa de manera vehemente que cualquier modelo de atribución debe respetar los principios estructurales del derecho penal, especialmente la culpabilidad, la legalidad y la personalidad de la pena; de ahí que el debate contemporáneo no gire únicamente alrededor de la conveniencia de sancionar penalmente a las organizaciones, sino de determinar cuáles son los fundamentos dogmáticos que permitirían justificar dicha responsabilidad sin afectar las garantías que caracterizan al Estado social y democrático de derecho (Silva,

2008).

Sobre esta base se desarrollaron dos grandes modelos doctrinales que han orientado la discusión contemporánea: la heterorresponsabilidad y la autorresponsabilidad de las personas jurídicas; ambos buscan explicar la intervención de las organizaciones en la criminalidad empresarial desde fundamentos distintos, convirtiéndose en el punto de partida para comprender las diferentes respuestas adoptadas por los ordenamientos jurídicos contemporáneos frente a este fenómeno (Gómez, 2016).

La primera de estas construcciones corresponde al modelo de heter-orresponsabilidad, el cual parte de la idea de que la persona jurídica no desarrolla una conducta penalmente relevante por sí misma, sino a través de las personas naturales que integran su estructura organizacional. Bajo este enfoque, la actuación de administradores, reafirmanes legales, directivos o empleados puede proyectar sus efectos jurídicos sobre la organización cuando dichas actuaciones se ejecutan dentro del ámbito funcional de la empresa y persiguen un beneficio para esta; en consecuencia, la responsabilidad atribuida a la persona jurídica no deriva de una culpabilidad propia, sino de la actuación de quienes exteriorizan su voluntad mediante el ejercicio de funciones de dirección, administración o representación (Bacigalupo, 2016).

Este es un modelo que conserva la estructura clásica del derecho penal, pues mantiene como centro de imputación a la persona natural y considera que la organización únicamente constituye el contexto dentro del cual se desarrolla la conducta punible; de esta forma, la empresa no reemplaza al autor material del delito, sino que puede verse afectada por determinadas consecuencias jurídicas derivadas del comportamiento de quienes actúan en su nombre; precisamente por ello, esta construcción ha tenido una importante acogida

en diversos ordenamientos jurídicos, en tanto que permite extender determinadas consecuencias hacia la organización sin romper completamente con los principios tradicionales de culpabilidad personal que caracterizan al derecho penal continental (Silva, 2008).

Pero la doctrina también ha identificado importantes limitaciones en este modelo. Una de las principales críticas radica en que la responsabilidad de la organización continúa dependiendo de la identificación previa de una persona natural responsable, circunstancia que resulta especialmente problemática cuando la conducta nace de decisiones colectivas, procesos altamente descentralizados o estructuras empresariales donde las funciones se encuentran distribuidas entre múltiples órganos de dirección; en estos casos, la complejidad organizacional dificulta establecer quién adoptó realmente la decisión que produjo el resultado lesivo, reduciendo considerablemente la eficacia del modelo tradicional de imputación (Gómez, 2016).

Estas son dificultades que se intensifican con la incorporación de tecnologías de inteligencia artificial dentro de las organizaciones; actualmente, numerosos procesos empresariales funcionan mediante algoritmos capaces de realizar análisis, formular recomendaciones o ejecutar decisiones previamente parametrizadas por la empresa; aunque estos sistemas no poseen voluntad jurídica propia, sí participan activamente en procesos cuya ejecución antes dependía exclusivamente de la intervención humana; como consecuencia, la clara identificación del sujeto responsable deja de ser una tarea sencilla y obliga a replantear el análisis desde la forma como la organización diseñó, implementó y supervisó el funcionamiento de estas herramientas tecnológicas (Prieto, 2022).

Justamente como respuesta a estas limitaciones nace el modelo de autorresponsabilidad de

las personas jurídicas; a diferencia del enfoque anterior, esta construcción expresa de manera vehemente que el fundamento de la responsabilidad no debe buscarse exclusivamente en la conducta individual de una persona natural, sino también en la existencia de defectos propios de organización que permitan o favorezcan la realización de conductas ilícitas; partiendo de esta mirada, el reproche jurídico no se dirige únicamente contra quien ejecuta materialmente la conducta, sino contra la propia organización cuando incumple los deberes de estructuración, vigilancia, supervisión y prevención que le corresponden dentro de su actividad económica (Gómez, 2016).

Bajo esta concepción, la empresa deja de entenderse como un simple escenario donde ocurren los hechos y pasa a ser considerada un verdadero centro de generación de riesgos jurídicamente relevantes; el elemento central ya no reside únicamente en la actuación de un empleado o directivo, sino en la existencia de fallas organizacionales que hacen posible la comisión del ilícito; en consecuencia, aspectos como la cultura de cumplimiento, los mecanismos internos de control, los sistemas de supervisión y la adecuada gestión de riesgos adquieren una importancia determinante para evaluar la actuación de la organización desde una perspectiva jurídico-penal (Del Rosal, 2023).

Este cambio de enfoque resulta especialmente significativo en escenarios donde interviene la inteligencia artificial; la utilización de herramientas automatizadas no elimina la obligación de dirección y vigilancia que corresponde a la organización, sino que incrementa la necesidad de establecer procedimientos eficaces de supervisión, auditoría y control tecnológico; De manera pues que la doctrina reciente expresa de manera vehemente que la inteligencia artificial no constituye un sujeto responsable, pero sí un elemento que obliga a redefinir los criterios mediante los cuales se examina la actuación

empresarial frente a los riesgos derivados de su implementación; en consecuencia, la verdadera discusión ya no consiste únicamente en determinar quién ejecutó materialmente una determinada decisión, sino en establecer si la organización creó, gestionó y controló adecuadamente los riesgos asociados al funcionamiento de estos sistemas (Januário, 2023). Ambos modelos reflejan la evolución de la dogmática penal frente a la transformación de las organizaciones empresariales; mientras la heterorresponsabilidad continúa vinculando la responsabilidad de la empresa a las actuaciones de las personas naturales que la reafirman, la autorresponsabilidad desplaza el análisis hacia la propia estructura organizacional y los mecanismos internos de control; esta evolución doctrinal constituye uno de los principales referentes para comprender el debate contemporáneo sobre la responsabilidad de las personas jurídicas y permite contextualizar adecuadamente la discusión que actualmente enfrenta el derecho colombiano frente a la utilización de sistemas de inteligencia artificial en el ámbito empresarial.

En torno a lo mencionado anteriormente, se han desarrollado diferentes orientaciones para explicar la posible vinculación de las personas jurídicas. Una de ellas plantea que la responsabilidad puede derivarse de las actuaciones de sus directivos o reafirmantes, lo cual significa que no existe una responsabilidad penal propia sobre la persona jurídica, en tanto que quienes actúan lo hacen en nombre de la organización; esta postura, también llamada teoría de “irresponsabilidad penal”, ha tenido una amplia aceptación dentro del derecho penal.

La criminalidad empresarial dentro de este enfoque puede estudiarse a partir de figuras como la cláusula del actuar por otro, la teoría de la autoría mediata en aparatos organizados de poder, la responsabilidad por omisión cuando se ostenta una posición de garante, así

como la responsabilidad derivada de decisiones adoptadas por órganos colegiados, como las juntas directivas; estas figuras adquieren relevancia en escenarios empresariales donde las decisiones son ejecutadas mediante estructuras organizadas o sistemas tecnológicos que dificultan identificar de manera directa a una persona responsable; es de resaltar que, en los supuestos de criminalidad organizada, la estructura empresarial puede servir como medio para la realización de conductas ilícitas; estas figuras jurídicas facilitan una comprensión en torno al hecho de cómo, a pesar de que la organización tiene un papel importante en el resultado, la responsabilidad penal continúa recayendo sobre personas naturales (Mosquera & Torres, 2014).

El modelo de heterorresponsabilidad parte de la idea de que la empresa no actúa por sí sola, sino a través de las personas que la integran, como sus directivos y empleados; aplicando esta perspectiva, si las actuaciones de estas personas generan efectos jurídicos en otros ámbitos de la empresa, también deberían tener consecuencias en el campo jurídico; es decir, lo que hacen quienes reafirman a la empresa se entiende como una manifestación de la voluntad de la misma corporación; esta postura adquiere especial interés en escenarios donde las empresas utilizan herramientas automatizadas o sistemas de inteligencia artificial dentro de sus procesos, en tanto que muchas decisiones continúan dependiendo de la supervisión, programación o control ejercido por personas vinculadas a la organización.

Desde este enfoque, no se sanciona a la persona jurídica por un comportamiento propio, sino por las conductas realizadas por quienes actúan en su nombre o en su beneficio; este modelo ha sido acogido en algunos ordenamientos jurídicos, como el francés o el inglés, donde es posible reconocer que la empresa responde por los actos de sus integrantes cuando estos buscan terminarla favoreciéndola.

Pero esta postura también ha sido objeto de críticas; por un lado, se expresa que la responsabilidad de la empresa termina dependiendo necesariamente de identificar a una persona natural concreta, lo que puede limitar su aplicación; por otro lado se cuestiona que este modelo puede acercarse a formas de responsabilidad objetiva, en la medida en que el reproche no recae directamente sobre una actuación propia de la persona jurídica, sino sobre hechos ajenos que se le atribuyen (Petro-González, Mosquera & Torres, 2014).

El modelo de autorresponsabilidad plantea una idea distinta: la empresa puede responder no solo por lo que hacen sus integrantes, sino también por fallas propias en su forma de funcionamiento; es decir, la infracción no se origina únicamente en una persona natural, sino en la manera en que está organizada la empresa para el desarrollo de sus actividades.

Lo mencionado anteriormente es muy importante en escenarios donde las organizaciones implementan sistemas de inteligencia artificial para el desarrollo de actividades empresariales, en tanto que la ausencia de controles adecuados sobre estas herramientas puede facilitar afectaciones a derechos o bienes jurídicos.

Desde este enfoque, la persona jurídica puede generar un riesgo cuando actúa de forma contraria a su rol dentro de la sociedad o cuando su organización interna facilita la afectación de derechos o bienes jurídicos; en otras palabras, el problema no siempre está en una conducta individual, sino también en la manera en que la organización estructura, supervisa o controla sus procesos internos.

Esta idea se ha explicado indicando que la empresa puede ser responsable cuando no organiza adecuadamente sus procesos para evitar daños o afectaciones a terceros, cuando su estructura dificulta identificar a un responsable concreto o cuando simplemente no adopta medidas de prevención que permitan evitar la ocurrencia de conductas incorrectas (Petro-González,

Mosquera & Torres, 2014); en escenarios de uso de inteligencia artificial, estas discusiones adquieren una relevancia especial, debido a que muchas decisiones automatizadas pueden producir consecuencias jurídicas importantes sin que resulte sencillo identificar de manera inmediata a una persona natural responsable.

En el caso colombiano, estas discusiones doctrinales no han tenido una influencia determinante en el desarrollo normativo, por cuanto el ordenamiento jurídico no ha adoptado un modelo de responsabilidad penal directa para las personas jurídicas; no obstante, sí han servido como fundamento para la implementación de mecanismos de control interno, como los programas de cumplimiento normativo (compliance), entendidos como herramientas orientadas al cumplimiento de normas legales y éticas dentro de una organización, con el propósito de prevenir infracciones y reducir riesgos derivados de su actividad (Alvear, 2024).

Este modelo se ha convertido en una de las principales herramientas para prevenir la comisión de conductas ilícitas dentro de las organizaciones, de manera especial en contextos donde las empresas utilizan tecnologías automatizadas o sistemas de inteligencia artificial para el desarrollo de sus actividades; en estos casos, los programas de cumplimiento adquieren relevancia porque permiten establecer mecanismos de supervisión, control y prevención frente a posibles riesgos derivados del uso de estas tecnologías.

Es así como la doctrina ha permitido ampliar la comprensión de la criminalidad empresarial y adoptar modelos que también pueden resultar aplicables frente al uso de tecnologías como la inteligencia artificial dentro de las organizaciones, de manera especial en escenarios donde estas herramientas intervienen en actuaciones con relevancia jurídica; no obstante, en Colombia la respuesta se ha orientado principalmente hacia mecanismos de prevención y control, como los programas de cumplimiento, cuya inobservancia genera principalmente

consecuencias administrativas y no una responsabilidad penal directa para las personas jurídicas.

El desarrollo reciente de la inteligencia artificial ha reactivado este debate doctrinal, debido a que la incorporación de sistemas automatizados dentro de las organizaciones plantea interrogantes adicionales sobre los criterios tradicionales de imputación; aunque estas tecnologías carecen de personalidad jurídica y no pueden ser consideradas sujetos de responsabilidad penal, sí participan de manera creciente en procesos empresariales que pueden producir consecuencias con relevancia jurídica; esta circunstancia obliga a analizar si los modelos dogmáticos tradicionales continúan siendo suficientes para responder a las nuevas formas de organización empresarial mediadas por herramientas tecnológicas (Del Rosal, 2023).

Partiendo de esta mirada, la doctrina contemporánea ha advertido que el verdadero problema no consiste en atribuir responsabilidad penal a los sistemas de inteligencia artificial, sino en determinar cómo debe evaluarse la actuación de las organizaciones que deciden incorporarlos dentro de sus procesos internos; en efecto, la implementación de estas tecnologías responde siempre a decisiones empresariales relacionadas con su adquisición, diseño, parametrización, entrenamiento, supervisión y utilización; en consecuencia, aun cuando determinadas decisiones sean ejecutadas mediante algoritmos, la existencia de una estructura organizacional responsable de su funcionamiento mantiene plena relevancia para el análisis jurídico (Januário, 2023).

Este planteamiento adquiere especial importancia porque muchos sistemas de inteligencia artificial operan mediante procesos de aprendizaje automático que dificultan reconstruir con precisión el itinerario seguido para producir una determinada decisión; tal situación genera

importantes desafíos probatorios, especialmente cuando la actuación automatizada ocasiona lesiones a bienes jurídicos protegidos o afecta derechos fundamentales de terceros; en estos supuestos, la dificultad para identificar una decisión humana inmediata no elimina la necesidad de examinar el grado de control que la organización ejercía sobre el funcionamiento del sistema ni el cumplimiento de los deberes de supervisión que le correspondían (Prieto, 2022).

De manera pues que la doctrina penal reciente expresa de manera vehemente que la incorporación de inteligencia artificial no transforma los principios estructurales del derecho penal, pero sí exige reinterpretar categorías tradicionales como el dominio del hecho, la posición de garante, la imputación objetiva y los deberes de organización; la automatización de determinados procesos empresariales incrementa la importancia de verificar si la organización diseñó mecanismos adecuados para identificar riesgos, controlar el funcionamiento de los sistemas tecnológicos y prevenir la producción de resultados lesivos; así, la atención doctrinal se desplaza progresivamente desde el análisis exclusivo de la conducta individual hacia la evaluación de la forma como la empresa administra los riesgos derivados de la utilización de estas herramientas tecnológicas (Del Rosal, 2023).

En paralelo, la expansión de modelos de cumplimiento normativo (compliance) ha adquirido una importancia creciente dentro de esta discusión; la doctrina ha expresado que los programas de cumplimiento ya no deben entenderse únicamente como instrumentos orientados a prevenir actos de corrupción o incumplimientos regulatorios, sino también como mecanismos destinados a gestionar los riesgos asociados a la implementación de tecnologías naciescentes; esto implica incorporar procedimientos internos de evaluación, protocolos de supervisión, auditorías periódicas y mecanismos de trazabilidad que permitan verificar el

funcionamiento de los sistemas de inteligencia artificial y corregir oportunamente eventuales fallas antes de que produzcan consecuencias jurídicamente relevantes (Gómez, 2016).

En el derecho comparado, particularmente en España, esta evolución doctrinal ha comenzado a orientar nuevas reflexiones sobre la manera en que deben responder las organizaciones frente a los riesgos derivados de la inteligencia artificial; pero ello no significa que exista consenso acerca de la necesidad de establecer una responsabilidad penal directa para las personas jurídicas en todos los supuestos; por el contrario, buena parte de la doctrina coincide en que cualquier transformación normativa debe preservar los principios de culpabilidad, legalidad y responsabilidad personal que caracterizan al derecho penal, evitando trasladar automáticamente a las organizaciones formas de responsabilidad objetiva incompatibles con un Estado social y democrático de derecho (Silva, 2008).

Como consecuencia de esto, discusión actual no puede reducirse a determinar si las personas jurídicas deben responder penalmente cuando interviene la inteligencia artificial; el verdadero desafío consiste en establecer cuáles son los criterios dogmáticos que permiten evaluar jurídicamente la actuación de las organizaciones frente a los nuevos riesgos tecnológicos, sin desconocer las garantías fundamentales que estructuran el sistema penal; precisamente Partiendo de esta mirada resulta pertinente analizar el caso colombiano, donde, pese a mantenerse la inexistencia de un régimen general de responsabilidad penal de las personas jurídicas, el ordenamiento jurídico ha venido fortaleciendo mecanismos administrativos, preventivos y de control orientados a exigir mayores niveles de diligencia, supervisión y organización frente al uso empresarial de sistemas de inteligencia artificial (Bacigalupo, 2016).

En la doctrina más reciente también se ha planteado que el desarrollo de sistemas de inteligencia

artificial obliga a revisar categorías tradicionales del derecho penal, debido a que estos sistemas comienzan a desempeñar funciones que anteriormente eran ejecutadas exclusivamente por personas naturales; Partiendo de esta mirada, la discusión ya no se limita a la responsabilidad de quien programa o utiliza la tecnología, sino que incorpora el análisis de la intervención de nuevos "actuales" tecnológicos dentro de los procesos de imputación penal, circunstancia que incrementa la importancia de los deberes de supervisión y control organizacional de las personas jurídicas (Navarro, 2025).

1.3 Marco Jurisprudencial de la responsabilidad de las personas jurídicas en Colombia en escenarios de uso de inteligencia artificial

La discusión en el ámbito jurisprudencial colombiano sobre la intervención de las personas jurídicas en conductas ilícitas ha partido por tradición de la idea de que el sistema penal se encuentra construido sobre la responsabilidad individual de las personas naturales; pero el desarrollo de estructuras empresariales cada vez más complejas y el uso creciente de tecnologías como la inteligencia artificial han llevado a que las altas cortes empiecen a pronunciarse sobre los límites del derecho penal y sobre las consecuencias jurídicas que pueden derivarse cuando las organizaciones intervienen en actuaciones con relevancia jurídica.

A través de la sentencia C-320 de 1998, la Corte Constitucional indicó que, aunque el ordenamiento jurídico colombiano ha sido reacio a reconocer responsabilidad penal directa de las personas jurídicas, no existe una prohibición absoluta para que el legislador lo haga en determinados casos; la Corte explica que, cuando una conducta ilícita se desarrolla en el marco de la actividad de una empresa y esta obtiene un beneficio o actúa en interés propio,

no resulta razonable limitar el análisis únicamente a las personas naturales que la reafirman. La Corte reconoce que las organizaciones cuentan con estructuras de dirección, control y funcionamiento a través de las cuales pueden intervenir en actuaciones con relevancia jurídica, razón por la cual, en determinados escenarios, podrían llegar a ser consideradas sujetos de imputación; no obstante, advierte que cualquier forma de atribución de responsabilidad debe respetar garantías fundamentales como el debido proceso y la prohibición de responsabilidad objetiva, lo que implica la existencia de elementos mínimos que permitan relacionar a la persona jurídica con la conducta investigada.

En esta decisión se deja claro que la eventual atribución de responsabilidad a las personas jurídicas no depende de una ficción, sino de la demostración de que la actividad desarrollada guarda relación con su funcionamiento, su organización y los beneficios obtenidos; esta postura adquiere relevancia en el contexto actual, donde muchas decisiones empresariales ya no dependen exclusivamente de personas naturales, sino también de sistemas tecnológicos y herramientas de inteligencia artificial; en estos escenarios, identificar de manera directa a un responsable individual puede resultar más complejo, lo que ha llevado a replantear los criterios tradicionales de atribución jurídica sin apartarse de las garantías propias del derecho penal.

En la sentencia SP16794-2014, la Sala de Casación Penal de la Corte Suprema de Justicia señaló que, aunque en otros sistemas jurídicos se ha avanzado hacia el reconocimiento de responsabilidad penal de las personas jurídicas, en Colombia esta posibilidad continúa siendo restringida; la Corte explica que esta dificultad responde a la forma en que está construido el derecho penal, el cual se fundamenta en la idea de que únicamente las personas naturales pueden actuar con conciencia y voluntad.

Por eso es que aunque es posible reconocer que muchas conductas ilícitas pueden desarrollarse dentro de estructuras empresariales complejas, el ordenamiento jurídico colombiano no ha dado el paso de atribuir responsabilidad penal directa a las empresas; además, el alto tribunal advierte que los intentos legislativos orientados hacia ese reconocimiento no han prosperado, no porque la idea resulte imposible, sino porque no se ha logrado construir una regulación clara que respete principios como el de legalidad.

Entonces, el modelo vigente mantiene la responsabilidad penal en cabeza de las personas naturales, siempre que se demuestre de manera concreta su participación en el hecho y su intención de cometerlo, mientras que las personas jurídicas continúan siendo objeto principalmente de consecuencias administrativas o civiles.

Esta postura de la Corte deja ver una tensión evidente entre la manera en que el derecho penal entiende la responsabilidad y la forma en que actualmente operan muchas estructuras empresariales, donde las decisiones no siempre dependen de una sola persona, sino de procesos organizacionales complejos e incluso de herramientas automatizadas; esto resulta especialmente relevante en escenarios de uso de inteligencia artificial, donde identificar de manera concreta a un autor individual puede ser aún más difícil; así, aunque la jurisprudencia colombiana ha mantenido una posición prudente frente a la responsabilidad penal de las personas jurídicas, sí permite advertir un reconocimiento indirecto de la intervención de las organizaciones en conductas ilícitas, lo que sirve como punto de partida para analizar las consecuencias jurídicas que podrían derivarse en estos nuevos contextos tecnológicos.

La Corte Constitucional, en la sentencia T-067 de 2025, abordó el tema de la transparencia en el uso de tecnologías como la inteligencia artificial dentro del sector público; en esta

decisión se discutió si la ciudadanía podía acceder al código fuente de una aplicación desarrollada por el Estado, frente a lo cual la Corte concluyó que, tratándose de herramientas financiadas con recursos públicos y utilizadas en procesos de toma de decisiones, debe garantizarse un nivel adecuado de acceso y control ciudadano.

La Corte resaltó que los algoritmos deben ser comprensibles y auditables, debido a que pueden incidir directamente en derechos fundamentales; también señaló que las limitaciones al acceso a este tipo de información deben encontrarse debidamente justificadas y no pueden sustentarse en argumentos generales.

Esta decisión evidencia que la inteligencia artificial no puede quedar por fuera del control jurídico y social, de manera especial en escenarios donde los sistemas automatizados intervienen en procesos capaces de afectar derechos fundamentales; la exigencia de transparencia y supervisión adquiere una importancia particular en el ámbito empresarial, donde muchas decisiones adoptadas mediante herramientas tecnológicas pueden generar consecuencias jurídicas relevantes sin que exista claridad inmediata sobre su funcionamiento o sobre los responsables de su implementación y control (Melo Rubiano, 2025).

2. CONCEPTO Y LOS USOS DE LA INTELIGENCIA ARTIFICIAL, SU IMPLEMENTACIÓN EN ENTORNOS EMPRESARIALES Y LOS POSIBLES ESCENARIOS EN LOS QUE PUEDE INTERVENIR EN ACTUACIONES CON RELEVANCIA JURÍDICA.

2.1 Concepto de inteligencia artificial

La inteligencia artificial se ha convertido en una herramienta cada vez más utilizada en distintos sectores, de manera especial en el ámbito empresarial, donde ha permitido optimizar procesos, mejorar la toma de decisiones y aumentar la eficiencia en diversas

actividades; pero no es un tema nuevo, aunque hoy tenga mucho auge; su origen data del siglo XX cuando Alan Turing, matemático, planteó la idea de que una máquina podría imitar el pensamiento humano, esto dio lugar al “test de Turing (1950), este test fue un razonamiento que permitía analizar si una máquina podía imitar la conversación de un humano sin que se lograra evidenciar una diferencia entre un humano y una máquina (IBM; s; f.); desde entonces ha venido dando pasos progresivos al punto de convertirse en un recurso clave desde un nivel científico, económico y social que va en crecimiento.

Hoy en día de manera general, la inteligencia artificial puede entenderse como *“un campo de la informática dedicado a resolver problemas cognitivos comúnmente asociados con la inteligencia humana o seres inteligentes, entendidos como aquellos que pueden adaptarse a situaciones cambiantes; su base es el desarrollo de sistemas informáticos, la disponibilidad de datos y los algoritmos.”* (Conpes 3975 de 2019).

En el contexto empresarial, la inteligencia artificial ha sido definida por la Organización para la Cooperación y el Desarrollo Económico, como *“un sistema basado en máquinas que, para objetivos explícitos o implícitos, infiere, a partir de la información que recibe (input), cómo generar resultados como predicciones, contenidos, recomendaciones o decisiones que pueden influir en entornos físicos o virtuales; los distintos sistemas de IA varían en sus niveles de autonomía y adaptabilidad tras su despliegue”* (OCDE Recomendaciones Sobre la Inteligencia Artificial) Este sistema se utiliza en múltiples áreas y ha venido en crecimiento durante la última década desde que Open Ai lanzó en 2020 GPT-3, y en el 2021 cerca de 300 aplicativos habían implementado GPT-3 en diversos sectores e industrias, desde el productivo y de educación hasta de recreación. OpenAI. (s; f.). *GPT-3 applications*.

Así, el uso de la inteligencia artificial se ha expandido en múltiples sectores, como el

financiero, educativo, comercial, de recursos humanos, de servicios y de la salud, generando transformaciones en la forma en que se desarrollan las actividades y se gestionan los procesos (Organización Mundial de la Salud, 2021).

Así muchas empresas han incorporado herramientas de inteligencia artificial para la toma de decisiones internas, lo que implica que determinadas acciones ya no dependen exclusivamente de una persona natural, sino de sistemas tecnológicos que operan con cierto grado de autonomía (European Parliament, 2020).

Este contexto es relevante desde un nivel jurídico por cuanto las tecnologías aplicadas y las decisiones adoptadas mediante inteligencia artificial pueden generar consecuencias que afecten bienes jurídicos, especialmente cuando no existen controles adecuados sobre su funcionamiento, son utilizadas de manera indebida o se encuentran provistas de errores y falta de control (Prieto, 2022).

Es por ello que organismos internacionales han advertido que el uso de la inteligencia artificial debe estar acompañado del respeto al Estado de derecho, los derechos humanos y los valores democráticos, incluidas la equidad y la privacidad; transparencia y explicabilidad, solidez, seguridad y protección y responsabilidad. (OCDE Recomendaciones Sobre la Inteligencia Artificial)

Así observamos que el uso de la inteligencia artificial en entornos empresariales, si bien representa una oportunidad en términos de transformación, eficiencia y aumento de la productividad, también plantea nuevos retos jurídicos, particularmente en lo relacionado con la determinación de responsabilidades cuando estas herramientas intervienen en la realización de actuaciones con relevancia jurídica.

Es por Lo mencionado anteriormente que resulta necesario analizar estos escenarios con el

fin de comprender cómo el uso de la inteligencia artificial puede incidir en la atribución de responsabilidad a las personas jurídicas dentro del marco jurídico colombiano.

2.2 Implementación y funcionamiento de la inteligencia artificial en entornos empresariales

A partir de lo mencionado anteriormente, es posible observar que la inteligencia artificial no solo constituye un desarrollo tecnológico relevante, sino que actualmente forma parte de las dinámicas cotidianas de múltiples organizaciones; su implementación en el ámbito empresarial ha permitido automatizar procesos, analizar grandes volúmenes de información y optimizar la ejecución de diversas actividades, transformando la manera en que las empresas operan y toman decisiones.

Uno de los sectores donde más se ha implementado la inteligencia artificial es el financiero. En este ámbito, las empresas utilizan sistemas automatizados para analizar grandes volúmenes de datos y comportamientos en tiempo real, lo que permite mejorar la evaluación del riesgo crediticio, detectar posibles fraudes y fortalecer los mecanismos de seguridad; estas herramientas también facilitan el cumplimiento de obligaciones normativas y amplían el acceso a financiación en determinados contextos, especialmente mediante modelos de análisis más ágiles y automatizados (Biallas & O'Neill, 2020).

En la industria manufacturera, la inteligencia artificial se ha incorporado a distintas etapas de la cadena de producción, desde el diseño hasta la distribución final de los productos; en las fases iniciales, estas herramientas permiten desarrollar simulaciones y procesos de modelación orientados a mejorar la innovación y la planificación; durante la fabricación, facilitan la automatización de tareas, la utilización de sistemas robóticos y el análisis de

información para optimizar la producción.

También se utilizan en el control de calidad para detectar fallas de manera más rápida y precisa, así como en actividades de almacenamiento y logística, donde contribuyen a organizar inventarios, prever la demanda y mejorar los procesos de distribución. Incluso en las etapas finales del ciclo productivo, la inteligencia artificial puede intervenir en actividades de clasificación y reciclaje, lo que evidencia el impacto que estas tecnologías tienen actualmente en el funcionamiento empresarial (Organización Internacional del Trabajo, 2026).

Otro escenario de implementación de inteligencia artificial se encuentra en el área de recursos humanos y en los procesos de contratación a través de plataformas digitales; según la Organización Internacional del Trabajo, estas plataformas utilizan algoritmos y sistemas automatizados para vincular trabajadores con clientes, analizando perfiles, necesidades del mercado y grandes volúmenes de información en tiempo real (OIT, 2021).

Así, la inteligencia artificial permite agilizar procesos de selección y asignación de personal, sustituyendo parcialmente funciones que antes eran desarrolladas exclusivamente por áreas humanas dentro de las organizaciones; esto pone en evidencia cómo muchas actividades empresariales que por tradición dependían de intervención humana hoy son ejecutadas mediante sistemas tecnológicos con capacidad de procesamiento automatizado.

En el sector salud, la inteligencia artificial también se ha incorporado progresivamente en actividades relacionadas con el análisis de imágenes médicas, el apoyo a diagnósticos clínicos y la administración de información de pacientes; mediante algoritmos especializados, estas herramientas permiten identificar patrones en datos clínicos, facilitando así la detección temprana de enfermedades y apoyando la toma de decisiones

médicas (Organización Mundial de la Salud, 2021).

Por otro lado en el ámbito comercial y de servicios, muchas empresas utilizan sistemas de inteligencia artificial para personalizar la oferta de productos, analizar hábitos de consumo y automatizar la atención al cliente mediante asistentes virtuales o chatbots; actualmente, en Colombia es frecuente el uso de agentes virtuales integrados a plataformas como WhatsApp, capaces de interactuar con usuarios, resolver inquietudes y promover productos o servicios sin que necesariamente exista interacción directa con una persona natural; estas herramientas han permitido una comunicación más rápida y una mayor adaptación a las necesidades de los consumidores.

La implementación de inteligencia artificial no se limita entonces únicamente al sector privado; en Colombia, algunas entidades estatales también han comenzado a incorporar estas tecnologías dentro de sus procesos de atención y gestión de información; en 2024, el Ministerio de Tecnologías de la Información y las Comunicaciones presentó “Alda”, una herramienta de inteligencia artificial diseñada para brindar orientación a los usuarios y procesar consultas en tiempo real sobre servicios relacionados con la entidad (Agencia Nacional Digital, 2024).

Los anteriores ejemplos permiten observar que la inteligencia artificial se ha integrado progresivamente en distintas áreas del funcionamiento empresarial y organizacional, incidiendo no solo en la ejecución de tareas operativas, sino también en la manera en que se gestionan procesos internos y se adoptan decisiones dentro de las organizaciones; esto ha generado nuevas dinámicas empresariales en las que múltiples actividades dependen cada vez más de herramientas tecnológicas capaces de operar con cierto grado de autonomía (Organización Internacional del Trabajo, 2026).

No obstante, la implementación de estas tecnologías también ha dado lugar a situaciones que trascienden el ámbito estrictamente operativo y pueden proyectarse hacia escenarios con implicaciones jurídicas relevantes; por esta razón, en el siguiente capítulo se abordarán algunos contextos en los que el uso de inteligencia artificial dentro de entornos empresariales puede intervenir en actuaciones con relevancia jurídica (European Parliament, 2020).

2.3 Escenarios prácticos de uso de la inteligencia artificial con relevancia jurídica en entornos empresariales.

En el contexto empresarial, la implementación de la inteligencia artificial no solo ha transformado la manera en que se desarrollan distintas actividades, sino que también ha generado nuevos escenarios en los que nacen actuaciones con una innegable relevancia jurídica; a medida que las organizaciones incorporan sistemas automatizados dentro de sus procesos principales, aumentan también los desafíos relacionados con la supervisión, el control y la clara identificación de responsabilidades frente a las consecuencias derivadas del uso de estas tecnologías (Del Rosal, 2023).

En Colombia, esta transición ha dejado de ser teórica para manifestarse en decisiones administrativas y judiciales que marcan la manera como el ordenamiento jurídico reacciona ante el comportamiento de los algoritmos. Uno de los escenarios más críticos se presenta en el sector financiero, particularmente ante fallas en sistemas de seguridad o mecanismos de autenticación; actualmente, herramientas de inteligencia artificial permiten desarrollar modalidades de fraude sofisticadas enfocadas en la clonación de voz o la creación de *deepfakes*, capaces de suplantar identidades para engañar tanto a

sistemas como a funcionarios; frente a esto, la Superintendencia Financiera ha fijado posturas determinantes, como ocurrió en el proceso contra Bancolombia S.A. Sentencia No. 2023-0130 (Proceso 2022-0442) ante transferencias electrónicas no reconocidas; en estos casos, se ha establecido que las entidades bancarias tienen un deber especial de custodia sobre los recursos; al no poder demostrar que existieron mecanismos suficientes de control, la responsabilidad recae sobre la institución, obligándola a la devolución de los fondos; este criterio se ve reforzado por la Circular Externa 001 de 2025, que exige a las *fintech* garantizar la transparencia y el derecho de los usuarios a recibir explicaciones claras sobre decisiones automatizadas que afecten su perfil crediticio o autenticación.

El manejo de datos personales constituye otro frente de alta sensibilidad jurídica; muchas empresas utilizan sistemas de inteligencia artificial que procesan volúmenes masivos de información sensible o biométrica, lo que ha derivado en intervenciones contundentes de la Superintendencia de Industria y Comercio. Un hito fundamental fue la Resolución 78798 de 2025, mediante la cual se sancionó a las sociedades World Foundation y Tools for Humanity Corporation; la investigación determinó que la recolección de datos biométricos mediante el escaneo del iris se realizaba sin cumplir con las exigencias del régimen de protección de datos, lo que resultó en el cierre definitivo de sus operaciones en Colombia; en la misma línea, la Resolución No. 13673 de 2025 sancionó a NANOCRED COLOMBIA S.A.S. (App PROFIN) con la suspensión de actividades por seis meses, tras verificar que la plataforma exigía acceso indebido a galerías de fotos y contactos de los usuarios sin justificación técnica ni legal; estos casos ponen en evidencia que, cuando las empresas priorizan la recolección masiva de información sin un esquema adecuado de prevención y consentimiento, el Estado responde con sanciones que limitan

directamente la capacidad operativa de la persona jurídica.

La inteligencia artificial también ha comenzado a intervenir en procesos de selección y contratación mediante algoritmos de filtrado de perfiles; si bien estas herramientas optimizan tiempos, su uso puede derivar en decisiones discriminatorias si reproducen sesgos de género o nacionalidad presentes en los datos de entrenamiento; en este ámbito, la jurisprudencia constitucional ha empezado a trazar límites claros; la Sentencia T-067 de 2025 exalta que los sistemas de decisión automatizada no pueden operar como "cajas negras" cuando inciden en derechos fundamentales, exigiendo niveles de explicabilidad que permitan el control humano; de esta misma manera la Sentencia T-323 de 2024 advirtió, a propósito del uso de ChatGPT en el sistema judicial, que la IA es una herramienta de apoyo que no puede sustituir la racionalidad y el juicio de valor humano, un principio perfectamente trasladable al ámbito corporativo para evitar la delegación absoluta de decisiones críticas en sistemas autónomos.

En el plano comercial y de mercado, estas tecnologías terminan influyendo en la fijación de precios y el análisis del consumidor, donde el uso inadecuado de sistemas automatizados podría facilitar prácticas que afecten la libre competencia; referentes globales como el AI Incident Database ya reportan incidentes recurrentes de manipulación y generación de contenido falso con impacto reputacional y organizacional; esto coincide con las advertencias de la OCDE (2019) sobre la necesidad de gestionar riesgos mediante la transparencia y la supervisión humana, aspectos que en Colombia ya se integran en leyes como la 2195 de 2022 y la 1581 de 2012 para exigir a las empresas una actuación diligente.

En definitiva, a pesar de los riesgos inherentes, la inteligencia artificial se ha consolidado

como un herramienta ampliamente utilizada dentro de distintos sectores económicos; por ello, el desafío actual no radica en excluir estas tecnologías, sino en fortalecer mecanismos de gobernanza y trazabilidad tecnológica que permitan reducir la falta de transparencia en el funcionamiento de los algoritmos; los escenarios y casos descritos confirman que, aunque la responsabilidad penal directa de la persona jurídica sea aún una asignatura pendiente en el código penal, el ordenamiento colombiano ya cuenta con herramientas administrativas y constitucionales capaces de reaccionar frente a fallas de control y supervisión dentro de las organizaciones, y proteger los derechos ciudadanos frente al poder de la automatización empresarial (Januário, 2023).

3. LÍMITES DEL DERECHO PENAL COLOMBIANO FRENTE A LAS PERSONAS JURÍDICAS EN ESCENARIOS DE USO DE INTELIGENCIA ARTIFICIAL Y CRITERIOS PARA SU VINCULACIÓN JURÍDICA.

3.1 Límites del derecho penal colombiano frente a la responsabilidad de las personas jurídicas.

En Colombia, el derecho penal continúa construido sobre la idea de que únicamente las personas naturales pueden ser sujetos de responsabilidad penal, postura por tradición explicada a partir del principio *societas delinquere non potest*, entonces, bajo esta concepción, la atribución de responsabilidad exige la existencia de voluntad y conciencia, elementos que históricamente han sido vinculados exclusivamente al comportamiento humano; pero el crecimiento de estructuras empresariales complejas y el uso cada vez más frecuente de sistemas de inteligencia artificial dentro de las organizaciones han generado escenarios en los que la clara identificación de un responsable individual resulta más difícil, especialmente cuando determinadas decisiones o actuaciones son ejecutadas mediante herramientas automatizadas.

El Código Penal colombiano se encuentra construido sobre la base de la culpabilidad individual, lo que implica que la imputación de una conducta punible exige la demostración de elementos como el dolo o la culpa, los cuales no pueden predicarse directamente de una persona jurídica; por esta razón, aun cuando una conducta ilícita se desarrolle en el marco de una organización empresarial, la responsabilidad penal continúa recayendo sobre las personas naturales que intervienen en su ejecución; este esquema ha permitido preservar las garantías propias del derecho penal, aunque también ha limitado la posibilidad de responder de manera integral frente a fenómenos de criminalidad desarrollados al interior de estructuras organizadas; esta dificultad se hace aún más visible en escenarios donde las decisiones empresariales se desarrollan mediante sistemas automatizados o herramientas de inteligencia artificial capaces de intervenir en procesos que antes dependían exclusivamente de actuación humana.

El mismo ordenamiento jurídico ha reconocido que las personas jurídicas pueden verse involucradas en la comisión de conductas ilícitas, lo cual es posible ver en figuras como las medidas contempladas en el artículo 91 de la Ley 906 de 2004, que permiten la suspensión o cancelación de la personería jurídica cuando esta ha sido utilizada para la realización de actividades delictivas; aunque estas medidas no constituyen sanciones penales en sentido estricto, sí reflejan que el ordenamiento jurídico reconoce la incidencia que pueden tener las organizaciones en la comisión de conductas ilícitas; en este punto resulta evidente que el sistema jurídico admite la relevancia de la persona jurídica dentro del hecho, pero evita atribuirle responsabilidad penal directa.

El uso de la inteligencia artificial introduce un nuevo nivel de complejidad, debido a que muchas decisiones pueden ser adoptadas mediante sistemas automatizados cuya intervención

no siempre resulta completamente visible o comprensible para quienes los utilizan; esto dificulta aún más la clara identificación de un responsable individual, de manera especial en escenarios donde las herramientas tecnológicas participan en procesos empresariales con consecuencias jurídicas relevantes; pero esta circunstancia no modifica la regla general del sistema penal colombiano, que continúa excluyendo la posibilidad de atribuir responsabilidad penal directa a las personas jurídicas.

De este modo, el marco jurídico colombiano enfrenta actualmente el reto de responder a dinámicas empresariales cada vez más complejas mediante estructuras normativas construidas, en gran parte, para modelos tradicionales de responsabilidad individual; esta tensión adquiere especial relevancia en escenarios donde las organizaciones utilizan sistemas de inteligencia artificial capaces de intervenir en decisiones con efectos jurídicos, sin que resulte siempre sencillo determinar hasta dónde llega el control humano o quién debe responder por las consecuencias derivadas de su funcionamiento.

Si bien el ordenamiento jurídico colombiano dispone actualmente de mecanismos administrativos, civiles y procesales para enfrentar actuaciones ilícitas desarrolladas por personas jurídicas, dichas herramientas no resuelven plenamente los riesgos derivados de la utilización de inteligencia artificial; las medidas administrativas cumplen principalmente una función correctiva y sancionatoria frente al incumplimiento de obligaciones legales; los mecanismos civiles se orientan a la reparación de los daños ocasionados; y las medidas procesales, como las previstas en el artículo 91 de la Ley 906 de 2004, buscan impedir que las organizaciones continúen siendo utilizadas para la comisión de actividades ilícitas; pero ninguna de estas respuestas fue diseñada específicamente para abordar problemas asociados con la opacidad algorítmica, la autonomía funcional de determinados sistemas, la

trazabilidad de las decisiones automatizadas o la distribución de responsabilidades dentro de organizaciones altamente tecnificadas; en consecuencia, más que evidenciar un vacío absoluto de protección jurídica, este escenario pone en evidencia la necesidad de fortalecer los mecanismos existentes mediante mayores exigencias de supervisión, gobernanza tecnológica, programas de cumplimiento y control organizacional, sin que ello implique, por ahora, la adopción de un régimen general de responsabilidad penal para las personas jurídicas (Prieto, 2022).

Esta postura también encuentra sustento en el principio de intervención mínima, conforme al cual el derecho penal únicamente debe intervenir cuando los demás mecanismos de protección jurídica resulten insuficientes para garantizar la tutela efectiva de los bienes jurídicos; de manera pues que la expansión de la inteligencia artificial dentro de las organizaciones no constituye, por sí sola, una razón suficiente para ampliar el ámbito de aplicación del derecho penal, pues previamente deben fortalecerse y evaluarse los instrumentos administrativos, regulatorios, civiles y procesales ya existentes, verificando su capacidad para responder a los nuevos riesgos tecnológicos.

De una forma complementaria, el principio de ultima ratio impone que la intervención penal opere como el último recurso del ordenamiento jurídico y no como la primera respuesta frente a toda problemática social o tecnológica; por ello, la posición asumida en esta investigación consiste en considerar que el contexto colombiano aún permite desarrollar respuestas eficaces mediante el fortalecimiento de los programas de cumplimiento, los deberes de organización, la supervisión tecnológica y las herramientas regulatorias actualmente vigentes; solo si dichos mecanismos demostraran objetivamente su insuficiencia podría justificarse la apertura de un debate legislativo orientado a modificar el

régimen de responsabilidad penal de las personas jurídicas, preservando siempre las garantías propias del Estado social de derecho (Silva, 2008).

Lo mencionado anteriormente es coherente con el principio de ultima ratio, conforme al cual la intervención del derecho penal únicamente se justifica cuando los mecanismos administrativos, civiles, regulatorios y procesales existentes resultan insuficientes para proteger eficazmente los bienes jurídicos comprometidos; en consecuencia, antes de plantear la ampliación de la responsabilidad penal de las personas jurídicas, corresponde valorar la capacidad de dichos instrumentos para responder a los riesgos derivados del uso de inteligencia artificial y determinar si realmente existe una necesidad de intervención penal adicional (Silva, 2008).

Aunque el ordenamiento jurídico colombiano dispone actualmente de diversos mecanismos para reaccionar frente a actuaciones ilícitas desarrolladas por personas jurídicas, tales como sanciones administrativas, medidas de prevención, programas de transparencia, obligaciones de cumplimiento y las consecuencias previstas en el artículo 91 de la Ley 906 de 2004, dichas herramientas exponen importantes limitaciones cuando los riesgos provienen de la utilización de sistemas de inteligencia artificial; en efecto, la mayoría de estas medidas fueron concebidas para enfrentar conductas desarrolladas mediante actuaciones humanas identificables y no para responder a procesos empresariales caracterizados por decisiones automatizadas, algoritmos complejos o sistemas de aprendizaje automático (Ley 2195 de 2022).

Una de las principales limitaciones consiste en que el régimen vigente continúa centrando gran parte del análisis jurídico en la clara identificación de la persona natural responsable; pero en escenarios donde la inteligencia artificial participa en procesos de decisión

empresarial, la determinación de la intervención individual resulta considerablemente más compleja debido a la distribución de funciones, la utilización de herramientas tecnológicas y la existencia de múltiples niveles de supervisión dentro de la organización; esta situación dificulta establecer con claridad el grado de participación de cada uno de los actores involucrados y, en consecuencia, limita la eficacia de las respuestas jurídicas tradicionales (Prieto, 2022).

De igual manera, las consecuencias jurídicas actualmente existentes privilegian una reacción posterior a la materialización del daño, mientras que los riesgos asociados al uso de inteligencia artificial exigen mecanismos preventivos permanentes orientados a la identificación temprana de riesgos, la supervisión tecnológica y el fortalecimiento de los sistemas internos de control; la sola imposición de sanciones administrativas o la adopción de medidas procesales resulta insuficiente cuando las organizaciones no cuentan previamente con protocolos de gobernanza tecnológica, auditoría algorítmica, trazabilidad de decisiones automatizadas y programas eficaces de cumplimiento que permitan prevenir la producción de resultados lesivos (Del Rosal, 2023).

La rápida evolución tecnológica supera con frecuencia la capacidad de adaptación del marco normativo vigente; mientras los sistemas de inteligencia artificial incorporan nuevas funcionalidades y niveles crecientes de autonomía operativa, las consecuencias jurídicas actualmente previstas continúan respondiendo a esquemas regulatorios diseñados para modelos tradicionales de organización empresarial; esta brecha regulatoria genera incertidumbre respecto de los criterios de imputación, de los deberes concretos de supervisión y de las obligaciones que deben asumir las personas jurídicas frente a la utilización responsable de estas tecnologías (CONPES 4144, 2025).

En consecuencia, la principal insuficiencia del modelo vigente no radica en la ausencia absoluta de consecuencias jurídicas para las personas jurídicas, sino en la necesidad de adaptar dichas herramientas a los riesgos específicos derivados de la inteligencia artificial; por ello, la investigación considera que el fortalecimiento de los mecanismos de prevención, cumplimiento, supervisión tecnológica y gobernanza empresarial constituye actualmente una respuesta más adecuada que la simple ampliación del catálogo de sanciones penales, manteniendo la coherencia con los principios que orientan el derecho penal colombiano (Silva, 2008).

A juicio de esta investigación, las transformaciones tecnológicas asociadas al uso de inteligencia artificial no justifican, por sí mismas, la adopción inmediata de un régimen de responsabilidad penal para las personas jurídicas en Colombia; si bien resulta evidente que las organizaciones desempeñan un papel determinante en la generación, administración y aprovechamiento de los sistemas automatizados, ello no supone que deban abandonarse los principios estructurales sobre los cuales se encuentra construido el derecho penal colombiano; la evolución tecnológica exige respuestas jurídicas más eficaces, pero dichas respuestas deben mantenerse dentro de los límites impuestos por la legalidad, la culpabilidad y la responsabilidad personal (Silva, 2008).

De manera pues que la investigación considera que las principales dificultades actuales no provienen de la inexistencia de un régimen de responsabilidad penal empresarial, sino de las limitaciones existentes para identificar y controlar los riesgos derivados del funcionamiento interno de las organizaciones; como ha expresado la doctrina, el verdadero desafío consiste en fortalecer los mecanismos de organización, supervisión y control empresarial, de manera que las empresas asuman un papel activo en la prevención de los

riesgos generados por la utilización de tecnologías nacientes, especialmente aquellas enfocadas en inteligencia artificial (Gómez, 2016).

Esta postura encuentra respaldo en el desarrollo reciente del derecho comparado, donde el fortalecimiento de los programas de cumplimiento (compliance) y de los deberes de organización ha adquirido una importancia creciente frente a la simple ampliación del catálogo de sanciones penales; en escenarios caracterizados por decisiones automatizadas, algoritmos complejos y aprendizaje automático, resulta jurídicamente más razonable exigir mayores estándares de diligencia, supervisión y trazabilidad tecnológica que extender automáticamente la intervención del derecho penal hacia las personas jurídicas (Del Rosal, 2023).

Por ello, esta investigación considera que la respuesta más compatible con el modelo constitucional colombiano consiste en fortalecer las herramientas preventivas, administrativas y regulatorias ya existentes, complementándolas con mayores exigencias de control organizacional y gobernanza tecnológica; solo en la medida en que dichas herramientas resulten insuficientes podría abrirse una discusión legislativa sobre eventuales modificaciones al régimen vigente, siempre respetando el carácter de ultima ratio que distingue al derecho penal dentro del Estado social de derecho (Prieto, 2022).

Las distintas propuestas doctrinales desarrolladas durante las últimas décadas ponen en evidencia que no existe una posición uniforme acerca de la conveniencia de reconocer responsabilidad penal directa a las personas jurídicas; mientras algunos ordenamientos, especialmente europeos, han optado por incorporar modelos de responsabilidad empresarial fundamentados en defectos de organización y en el incumplimiento de deberes de supervisión, otros sistemas jurídicos continúan privilegiando la responsabilidad individual

como eje estructural del derecho penal (Gómez, 2016).

En Colombia también han existido iniciativas orientadas a ampliar los mecanismos de control sobre las personas jurídicas, principalmente mediante normas dirigidas al fortalecimiento de la transparencia, la prevención de la corrupción, la protección de datos personales y el cumplimiento empresarial; no obstante, el legislador ha optado por desarrollar estas respuestas desde el ámbito administrativo, preventivo y regulatorio, manteniendo inalterada la estructura del derecho penal basada en la responsabilidad personal de las personas naturales. Incluso las recientes iniciativas relacionadas con la regulación de la inteligencia artificial, como el Proyecto de Ley 043-2025S, se orientan hacia principios de gobernanza, supervisión, transparencia y uso responsable de estas tecnologías, sin proponer un régimen general de responsabilidad penal para las personas jurídicas (Cámara de Reafirmantes de Colombia, 2024).

A partir del análisis realizado en esta investigación, se considera que dicha orientación resulta actualmente más compatible con el modelo constitucional colombiano; la simple incorporación de un régimen de responsabilidad penal empresarial no solucionaría, por sí misma, las dificultades que hoy plantea el uso de inteligencia artificial dentro de las organizaciones; el problema principal no radica en la ausencia de una sanción penal para la persona jurídica, sino en las dificultades para identificar oportunamente los riesgos derivados de la utilización de estas tecnologías, fortalecer los mecanismos internos de control y garantizar una supervisión efectiva sobre los procesos automatizados (Del Rosal, 2023).

Esta investigación expresa de manera vehemente que la respuesta jurídica más adecuada para el contexto colombiano consiste en consolidar los instrumentos preventivos ya

existentes, fortalecer los programas de cumplimiento, incrementar los deberes de organización y supervisión tecnológica y mejorar los mecanismos administrativos y regulatorios aplicables a las personas jurídicas; solo una vez agotadas estas herramientas podría plantearse un debate legislativo sobre la necesidad de introducir modificaciones al régimen penal vigente; anticipar dicha discusión sin demostrar previamente la insuficiencia del modelo actual implicaría desconocer el carácter subsidiario y de ultima ratio que debe conservar el derecho penal dentro del Estado social de derecho (Silva, 2008).

Esta tendencia también puede observarse en la doctrina europea más reciente, la cual expresa de manera vehemente que el uso de inteligencia artificial exige fortalecer los mecanismos de prevención empresarial, los programas de cumplimiento y la gobernanza tecnológica antes que ampliar indiscriminadamente la intervención penal; en consecuencia, las respuestas jurídicas más eficaces continúan orientándose hacia modelos integrales de prevención y gestión del riesgo, reservando la intervención penal para aquellos supuestos en los que exista una verdadera justificación conforme a los principios que estructuran el derecho penal contemporáneo (Mongillo, 2024).

La doctrina española reciente también ofrece elementos relevantes para la evolución del derecho colombiano; los aportes de Prieto (2022) y Del Rosal (2023) muestran que el principal desafío jurídico no consiste únicamente en determinar si las personas jurídicas deben responder penalmente cuando interviene la inteligencia artificial, sino en fortalecer los mecanismos de organización, supervisión y cumplimiento que permitan prevenir la materialización de riesgos tecnológicos; aunque estas propuestas fueron desarrolladas en un contexto normativo distinto al colombiano, resultan útiles para interpretar el alcance de los deberes empresariales de control, diligencia y gobernanza tecnológica previstos en la

legislación nacional; en consecuencia, esta investigación considera que la experiencia española constituye un referente doctrinal valioso para orientar futuras reformas y para fortalecer la aplicación de los mecanismos preventivos actualmente existentes en Colombia, sin que ello implique trasladar de manera automática los modelos de responsabilidad penal empresarial desarrollados en ese ordenamiento.

3.2 Criterios jurídicos para vincular a las personas jurídicas en escenarios de uso de inteligencia artificial

A pesar de que el ordenamiento jurídico colombiano no reconoce la responsabilidad penal directa de las personas jurídicas, el análisis del marco normativo, jurisprudencial y doctrinal permite identificar ciertos criterios que hacen posible examinar su intervención en actuaciones con relevancia jurídica; no se trata de crear una forma de imputación distinta a la prevista en el sistema penal, sino de entender cómo, en la práctica, el funcionamiento interno de la empresa puede influir en el resultado, de manera especial en escenarios en los que interviene la inteligencia artificial; estos criterios permiten aproximarse de una manera más cercana a la realidad empresarial actual.

Uno de los primeros elementos a considerar es el criterio del beneficio o interés de la persona jurídica; a partir de este es fundamental establecer si la actuación se desarrolla en función de la actividad empresarial o si genera algún tipo de provecho para la organización; este criterio encuentra respaldo en el ámbito normativo, particularmente en regímenes como el previsto en la Ley 1778 de 2016, y permite identificar un vínculo entre el resultado y la empresa, incluso cuando no es posible determinar con claridad quién tomó la decisión concreta; en la práctica, este suele ser uno de los puntos de partida del análisis, en tanto que

el beneficio obtenido permite evidenciar con mayor facilidad la conexión entre la conducta y la organización; en escenarios de uso de inteligencia artificial, este aspecto mantiene plena relevancia, pues el hecho de que la herramienta tecnológica haga parte de los procesos internos de la empresa evidencia que el resultado se encuentra integrado a su actividad.

Desde el punto de vista jurídico, la corroboración de este criterio permite activar consecuencias relevantes para la persona jurídica, principalmente en el ámbito administrativo, donde pueden imponerse sanciones como multas, inhabilidades para contratar con el Estado o restricciones en el ejercicio de la actividad económica, conforme a lo previsto en normas como la Ley 1778 de 2016 y la Ley 1474 de 2011 (estatuto anticorrupción); de esta misma manera en el ámbito procesal penal, este elemento puede justificar la adopción de medidas como la suspensión o cancelación de la personería jurídica, en los términos del artículo 91 de la Ley 906 de 2004, cuando es posible ver que la organización ha sido utilizada como instrumento para la comisión de conductas ilícitas; así, el beneficio obtenido no solo permite establecer un vínculo con la conducta, sino que también incide directamente en la posibilidad de imponer consecuencias jurídicas a la entidad.

Es el caso de aquellas empresas que utilizan sistemas de inteligencia artificial para la segmentación de clientes y la personalización de ofertas comerciales, realizando análisis masivos de datos personales para diseñar estrategias orientadas a incrementar las ventas; si durante estos procesos se desarrolla un tratamiento indebido de la información, por ejemplo, sin consentimiento válido de los titulares o excediendo la finalidad autorizada, la organización puede obtener un beneficio económico directo derivado del uso de la

tecnología; en este escenario, la situación no puede analizarse únicamente desde la actuación individual de un empleado o desde el funcionamiento técnico del sistema, sino también desde la actividad empresarial y el provecho obtenido por la organización.

Un segundo elemento corresponde al criterio del control organizacional, relacionado con la capacidad de la empresa para dirigir, supervisar y regular las actividades desarrolladas en su interior; este aspecto adquiere especial relevancia frente al uso de herramientas tecnológicas, en la medida en que su implementación no constituye un hecho ajeno a la organización, sino una decisión adoptada dentro de su actividad empresarial; De manera pues que no resulta suficiente alegar desconocimiento sobre el comportamiento de los sistemas de inteligencia artificial, pues el deber de control implica asumir las consecuencias derivadas de su utilización; en la práctica es frecuente encontrar organizaciones que intentan desvincularse de ciertos resultados alegando una aparente autonomía del sistema; pero este argumento pierde fuerza si se tiene en cuenta que el diseño, implementación y supervisión de estas herramientas forman parte de las decisiones adoptadas por la propia empresa.

Es el caso particular de aquellas empresas que implementan sistemas de inteligencia artificial para la atención automatizada de clientes mediante chatbots, los cuales interactúan directamente con los usuarios y ofrecen información sobre productos o condiciones contractuales; si estos sistemas suministran información inexacta o inducen a error al consumidor, por ejemplo, respecto de precios, condiciones o alcances del servicio, la empresa no puede excusarse en la autonomía del sistema, debido a que fue ella quien decidió su implementación y definió los parámetros bajo los cuales operaría. Bajo este criterio, la ausencia de supervisión, actualización o control sobre el funcionamiento de la herramienta evidencia fallas organizacionales jurídicamente relevantes.

Este deber de control encuentra sustento en distintas disposiciones del ordenamiento jurídico colombiano, principalmente en el régimen de protección de datos personales previsto en la Ley 1581 de 2012, que impone a los responsables y encargados del tratamiento la obligación de garantizar la seguridad, confidencialidad y adecuado manejo de la información, así como en las directrices emitidas por la Superintendencia de Industria y Comercio frente al uso de tecnologías nacientes; de igual manera, normas relacionadas con la transparencia y la lucha contra la corrupción, como la Ley 1474 de 2011 y la Ley 2195 de 2022, evidencian la necesidad de que las organizaciones implementen mecanismos de control interno y supervisión real sobre sus procesos.

En tercer lugar, se encuentra el criterio del deber de prevención, vinculado con la adopción de mecanismos de cumplimiento normativo o compliance; las normas vigentes en lo que se refiere a lucha contra la corrupción y control empresarial han resaltado la necesidad de implementar medidas orientadas a evitar la comisión de conductas ilícitas; así, el análisis no se limita únicamente a lo ocurrido, sino también a la forma en que la organización gestionó los riesgos asociados a su actividad; esto adquiere especial importancia en entornos tecnológicos, donde muchos riesgos no resultan evidentes desde el inicio; en la práctica, algunas organizaciones solo adoptan medidas de cumplimiento después de que ocurre un incidente, lo que evidencia modelos empresariales reactivos frente al riesgo y permite cuestionar si realmente existía un sistema preventivo efectivo.

Es el caso de aquellas empresas que utilizan sistemas de inteligencia artificial en procesos de selección de personal, donde los candidatos son filtrados automáticamente a partir de determinados criterios definidos por el sistema; si la organización no evalúa previamente los riesgos asociados al funcionamiento de la herramienta, por ejemplo, la posible reproducción

de sesgos relacionados con género, edad o nacionalidad, puede terminar excluyendo injustificadamente a determinados aspirantes; en estos escenarios, la afectación ya se ha producido, lo que evidencia que la organización no contaba con mecanismos preventivos realmente efectivos frente al funcionamiento de la herramienta tecnológica utilizada.

El criterio del deber de prevención encuentra sustento en diversas disposiciones del ordenamiento jurídico colombiano que imponen la necesidad de adoptar medidas orientadas a evitar la comisión de irregularidades dentro del ámbito empresarial; en particular, la Ley 1778 de 2016 establece la obligación de implementar programas de ética empresarial en lo que se refiere a soborno transnacional, reflejando una perspectiva preventiva frente a la actuación de las organizaciones; de igual manera, la Ley 1474 de 2011 y la Ley 2195 de 2022 han fortalecido mecanismos de transparencia, control y prevención de la corrupción, promoviendo la adopción de prácticas internas dirigidas a la gestión de riesgos.

Estas disposiciones, aunque no consagran un deber general de compliance en sentido estricto, sí evidencian una tendencia normativa orientada a exigir a las personas jurídicas una actuación diligente frente a la prevención de irregularidades; así, el análisis del comportamiento empresarial no se limita únicamente a la ocurrencia del hecho, sino también a la evaluación de las medidas adoptadas para evitarlo, aspecto especialmente relevante en escenarios donde intervienen tecnologías como la inteligencia artificial.

Para dar cierre, el criterio de trazabilidad tecnológica permite examinar si es posible reconstruir el funcionamiento de los sistemas de inteligencia artificial utilizados por la organización; este aspecto resulta fundamental, en tanto que en muchos casos la dificultad no radica únicamente en determinar quién actuó, sino también en comprender cómo se produjo el resultado dentro del sistema; la opacidad de ciertos modelos tecnológicos puede

dificultar este ejercicio; pero ello no puede asumirse como una circunstancia neutra, pues la ausencia de trazabilidad evidencia deficiencias en la implementación y supervisión de estas herramientas; esta falta de claridad se convierte en uno de los principales obstáculos para el análisis jurídico y refuerza la necesidad de exigir mayores niveles de transparencia y explicabilidad.

El criterio de trazabilidad tecnológica encuentra respaldo en el ordenamiento jurídico colombiano a partir de los deberes de transparencia y control en el uso de información y tecnologías; en particular, la Ley 1581 de 2012 exige a los responsables del tratamiento garantizar el adecuado manejo de los datos personales y la posibilidad de conocer la información que se recolecta y utiliza, lo que implica la necesidad de comprender los procesos mediante los cuales se adoptan decisiones que afectan a los titulares; en la misma línea, la Corte Constitucional ha expresado que las decisiones automatizadas no pueden operar como “cajas negras” cuando inciden en derechos fundamentales, destacando la importancia de su explicabilidad y control, como se expuso en la Sentencia T-067 de 2025; así, la posibilidad de reconstruir el funcionamiento de los sistemas utilizados se convierte en un elemento relevante para evaluar la actuación de la organización y el nivel de supervisión ejercido sobre estas herramientas.

En conjunto, estos criterios no operan de manera aislada, sino que suelen concurrir dentro del análisis de un mismo caso; su importancia no radica en sustituir las categorías tradicionales del derecho penal, sino en permitir una aproximación más completa frente a realidades que desbordan los esquemas clásicos de imputación y que hoy hacen parte de las dinámicas empresariales asociadas al uso de inteligencia artificial.

3.3; aplicación de criterios jurídicos frente a la intervención de personas jurídicas en

escenarios de inteligencia artificial en Colombia.

A partir de los criterios desarrollados, es posible analizar de una manera más concreta cómo responde actualmente el ordenamiento jurídico colombiano frente a escenarios en los que las personas jurídicas intervienen en actuaciones con relevancia jurídica mediante el uso de herramientas de inteligencia artificial; aunque en Colombia no existe un régimen de responsabilidad penal directa para las personas jurídicas, ello no significa que la actuación de las organizaciones quede completamente por fuera del alcance del derecho, especialmente cuando la actividad empresarial participa de manera determinante en la producción del resultado.

En un escenario real, cuando las autoridades encuentran que la organización obtuvo un beneficio derivado de la conducta, existieron fallas de supervisión, no se implementaron medidas de prevención adecuadas o resulta imposible reconstruir el funcionamiento de los sistemas utilizados, la empresa deja de ser vista únicamente como el escenario donde ocurrieron los hechos y pasa a ocupar un lugar relevante dentro del análisis jurídico; esto adquiere especial importancia en contextos empresariales donde las decisiones se desarrollan mediante sistemas automatizados capaces de intervenir en procesos de selección, atención al cliente, análisis de datos, corroboración de identidad o segmentación de usuarios.

Esta intervención en el ámbito de la administración puede traducirse en consecuencias relevantes para la persona jurídica, tales como multas, suspensión de actividades, restricciones al ejercicio de determinadas operaciones o incluso el cierre definitivo de actividades empresariales; casos como las sanciones impuestas por la Superintendencia de Industria y Comercio a sociedades como World Foundation, Tools for Humanity

Corporation o NANOCRED COLOMBIA S.A.S; permiten observar que el ordenamiento jurídico colombiano ya cuenta con mecanismos orientados a reaccionar frente a prácticas empresariales desarrolladas mediante herramientas tecnológicas cuando estas afectan derechos de los ciudadanos o desconocen obligaciones legales relacionadas con protección de datos, transparencia o deberes de control.

Pero estas respuestas continúan desarrollándose principalmente desde ámbitos administrativos y regulatorios; en materia penal, la responsabilidad sigue recayendo sobre personas naturales concretas, aun en escenarios donde la estructura organizacional o las herramientas tecnológicas utilizadas por la empresa hayan facilitado la realización de la conducta; en estos casos, la intervención de la persona jurídica suele manifestarse a través de medidas excepcionales como la suspensión o cancelación de la personería jurídica, previstas en el artículo 91 de la Ley 906 de 2004, cuando se depone en evidencia que la organización fue utilizada para la realización de actividades ilícitas.

Otro aspecto relevante se relaciona con la prueba y reconstrucción de los hechos; en escenarios de uso de inteligencia artificial, comprender cómo funcionaban los sistemas utilizados, cuáles eran los mecanismos de supervisión existentes y qué nivel de control ejercía realmente la organización sobre dichas herramientas se convierte en un elemento fundamental para el análisis jurídico; sin ese ejercicio, el estudio del caso termina concentrándose únicamente en actuaciones individuales, dejando por fuera aspectos relacionados con el funcionamiento interno de la empresa y con las decisiones organizacionales que hicieron posible el resultado (Januário, 2023).

Esto resulta especialmente importante en sistemas de inteligencia artificial cuya operación no siempre es completamente visible o comprensible para quienes los implementan; en

muchos casos no existe una decisión individual claramente identificable, sino procesos automatizados que participan en la producción del resultado a partir de parámetros definidos previamente por la organización; por esta razón, criterios como el control organizacional, el deber de prevención y la trazabilidad tecnológica permiten aproximarse de manera más adecuada a este tipo de realidades empresariales (Prieto, 2022).

Puede afirmarse entonces que el ordenamiento jurídico colombiano sí cuenta actualmente con herramientas que permiten reaccionar frente a actuaciones empresariales desarrolladas mediante inteligencia artificial; pero estas respuestas todavía resultan limitadas frente al impacto que pueden generar determinadas tecnologías y frente a la complejidad de las dinámicas empresariales actuales; en algunos casos, las consecuencias jurídicas existentes pueden resultar insuficientes frente al daño ocasionado o frente a los beneficios obtenidos por la organización a partir del uso de estas herramientas tecnológicas.

Lo mencionado anteriormente permite advertir la necesidad de avanzar hacia interpretaciones jurídicas que respondan de manera más adecuada a estos nuevos escenarios, sin que ello implique desconocer las garantías propias del derecho penal colombiano; más que trasladar automáticamente modelos de responsabilidad penal empresarial, el desafío consiste en fortalecer mecanismos de supervisión, prevención y control dentro de las organizaciones, especialmente cuando utilizan sistemas de inteligencia artificial capaces de intervenir en decisiones con consecuencias jurídicas relevantes; así, el análisis de la actuación empresarial deja de centrarse exclusivamente en la conducta individual y permite examinar también el funcionamiento real de la organización y el papel que cumplen las herramientas tecnológicas dentro de su actividad (Silva, 2008).

CONCLUSIONES

Solución al problema de investigación

El problema de investigación se centró en determinar cómo puede analizarse la intervención de las personas jurídicas en escenarios donde el uso de inteligencia artificial incide en la realización de actuaciones con relevancia jurídica, dentro de un sistema como el colombiano que no admite la responsabilidad penal directa de las organizaciones.

A partir del desarrollo de la investigación, es posible dar cierre con la idea de que el ordenamiento jurídico colombiano mantiene una estructura basada en la responsabilidad penal individual; pero el análisis del marco normativo, jurisprudencial y doctrinal evidencia la existencia de herramientas que permiten examinar la actuación de las personas jurídicas desde una perspectiva más amplia, de manera especial en contextos empresariales donde intervienen sistemas automatizados y herramientas de inteligencia artificial.

De manera pues que criterios como el beneficio obtenido por la organización, el control organizacional, el deber de prevención y la trazabilidad tecnológica facilitan una comprensión en torno al hecho de de una manera más adecuada cómo las empresas pueden incidir en la producción de resultados con relevancia jurídica, aun cuando no sea posible atribuirles responsabilidad penal directa en sentido estricto; estos criterios no sustituyen las categorías tradicionales del derecho penal colombiano, pero sí permiten aproximarse de mejor manera a dinámicas empresariales que actualmente desbordan los esquemas clásicos de imputación individual.

La investigación permitió evidenciar que, en Colombia, las respuestas jurídicas frente a este tipo de escenarios se han desarrollado principalmente desde ámbitos administrativos,

regulatorios y preventivos; casos como las actuaciones adelantadas por la Superintendencia de Industria y Comercio frente al tratamiento de datos biométricos, el uso de tecnologías automatizadas o las fallas en mecanismos de control empresarial pone en evidencian que el ordenamiento jurídico sí cuenta con mecanismos para reaccionar frente a conductas desarrolladas mediante herramientas tecnológicas; no obstante, dichas respuestas continúan siendo limitadas frente a la complejidad de las nuevas dinámicas empresariales y frente al impacto que puede generar el uso de inteligencia artificial en la afectación de bienes jurídicos.

Así, la solución al problema planteado no radica en la creación inmediata de un régimen de responsabilidad penal para las personas jurídicas, sino en la utilización e interpretación de herramientas jurídicas que ya encuentran sustento dentro del ordenamiento colombiano y que permiten analizar de una manera más adecuada la intervención de las organizaciones en escenarios de uso de inteligencia artificial; esto implica fortalecer mecanismos de supervisión, control y prevención dentro de las empresas, especialmente cuando implementan sistemas automatizados capaces de intervenir en decisiones con consecuencias jurídicas relevantes.

En consecuencia, el principal desafío para el ordenamiento jurídico colombiano no consiste únicamente en discutir si las personas jurídicas pueden ser penalmente responsables, sino en desarrollar respuestas jurídicas capaces de adaptarse a contextos empresariales donde las decisiones y actuaciones ya no dependen exclusivamente de personas naturales, sino también de herramientas tecnológicas cuyo funcionamiento puede incidir directamente en la producción de resultados con relevancia jurídica.

Corroboración de la hipótesis

La hipótesis planteada en esta investigación partía de la idea de que, aunque en el ordenamiento jurídico colombiano no existe un régimen de responsabilidad penal directa para las personas jurídicas, sí es posible identificar consecuencias jurídicas aplicables a las organizaciones en escenarios donde interviene el uso de inteligencia artificial, a partir de la interpretación del marco normativo vigente y de los mecanismos de control ya existentes dentro del sistema jurídico.

A partir del desarrollo de la investigación, dicha hipótesis se corrobora en los términos propuestos, en la medida en que se puso en evidencia que el sistema jurídico colombiano, aun manteniendo el principio tradicional de culpabilidad individual, no resulta ajeno a la intervención de las personas jurídicas en actuaciones con relevancia jurídica desarrolladas mediante herramientas tecnológicas y sistemas automatizados; por el contrario, el análisis normativo, jurisprudencial y doctrinal permitió identificar distintas formas de reacción jurídica frente a conductas empresariales relacionadas con el uso de inteligencia artificial, especialmente desde ámbitos administrativos, regulatorios y preventivos.

La investigación también permitió establecer que, aunque el derecho penal colombiano continúa limitando la atribución de responsabilidad penal directa a las personas jurídicas, ello no impide que las organizaciones puedan verse sometidas a consecuencias jurídicas cuando su actividad empresarial interviene de manera relevante en la producción del resultado; casos relacionados con tratamiento indebido de datos biométricos, fallas en mecanismos de control tecnológico, uso de sistemas automatizados o deficiencias en procesos de supervisión empresarial ponen en evidencia que actualmente existen mecanismos de sanción y control aplicables frente a este tipo de escenarios.

Los criterios de beneficio o interés de la organización, control organizacional, deber de

prevención y trazabilidad tecnológica permitieron estructurar un marco de análisis orientado a examinar la forma en que las personas jurídicas pueden incidir en resultados con relevancia jurídica, de manera especial en contextos donde intervienen sistemas de inteligencia artificial; estos criterios no buscan reemplazar las categorías tradicionales del derecho penal colombiano, sino ofrecer herramientas que permitan comprender de manera más adecuada dinámicas empresariales que actualmente superan los modelos clásicos de imputación individual.

Así, la hipótesis no solo se confirma desde el plano teórico, sino también desde una perspectiva práctica, al evidenciar que el ordenamiento jurídico colombiano ya cuenta con mecanismos que permiten reaccionar frente a nuevas dinámicas empresariales mediadas por tecnologías automatizadas, aun cuando dichas respuestas todavía resulten limitadas frente a la complejidad y alcance de los escenarios asociados al uso de inteligencia artificial.

Cumplimiento de los objetivos

Con relación a los objetivos planteados en la investigación, Es posible dar cierre con la idea de que estos fueron desarrollados y cumplidos de manera satisfactoria a lo largo del trabajo. Primero se logró analizar el marco normativo, jurisprudencial y doctrinal existente en Colombia frente a la responsabilidad de las personas jurídicas y las consecuencias jurídicas aplicables a su actuación; a partir de este análisis Fue posible evidenciar también que, aunque el ordenamiento jurídico colombiano no reconoce un régimen de responsabilidad penal directa para las organizaciones, sí existen mecanismos administrativos, procesales y regulatorios que permiten reaccionar frente a conductas desarrolladas en el ámbito empresarial, especialmente cuando estas afectan bienes jurídicos relevantes.

También se examinó el concepto de inteligencia artificial, sus principales usos dentro de entornos empresariales y algunos escenarios en los que estas tecnologías pueden intervenir en actuaciones con relevancia jurídica; el desarrollo de este objetivo permitió identificar cómo herramientas automatizadas participan actualmente en procesos relacionados con análisis de datos, atención al cliente, corroboración de identidad, selección de personal, servicios financieros y toma de decisiones empresariales, así como los riesgos que pueden derivarse de su utilización cuando no existen mecanismos adecuados de supervisión y control.

Tercero, también fueron analizados los límites del derecho penal colombiano frente a la intervención de personas jurídicas en escenarios de uso de inteligencia artificial, identificando las dificultades que presenta un modelo construido sobre la culpabilidad individual frente a dinámicas empresariales complejas mediadas por tecnologías automatizadas; a partir de ello, se desarrollaron criterios jurídicos como el beneficio o interés de la organización, el control organizacional, el deber de prevención y la trazabilidad tecnológica, los cuales permiten examinar de una manera más adecuada la intervención de las personas jurídicas dentro de este tipo de escenarios.

Para dar cierre el desarrollo de la investigación permitió aplicar dichos criterios al contexto del ordenamiento jurídico colombiano, demostrando que es posible identificar consecuencias jurídicas frente a la actuación de las personas jurídicas sin necesidad de modificar las bases estructurales del sistema penal vigente; De manera pues que la investigación evidenció que el análisis de la actividad empresarial no puede limitarse exclusivamente a la actuación individual de una persona natural, de manera especial en contextos donde intervienen herramientas tecnológicas capaces de influir directamente en la

producción del resultado.

Se evidenció que el derecho penal colombiano, construido históricamente sobre la base de la responsabilidad individual, enfrenta desafíos importantes frente a realidades empresariales cada vez más complejas, donde la intervención de herramientas tecnológicas y sistemas automatizados modifica la forma en que se desarrollan determinadas actividades; sin que ello implique desconocer las garantías y principios estructurales del derecho penal, se hace necesario avanzar hacia interpretaciones jurídicas que permitan comprender de manera más adecuada fenómenos en los que la producción del resultado no depende exclusivamente de una decisión humana individual, sino también de dinámicas organizacionales mediadas por tecnologías de creciente impacto dentro de la actividad empresarial.

BIBLIOGRAFÍA

Referentes normativos

- Cámara de Representantes de Colombia. (2024). *Proyecto de Ley 043-2025S sobre inteligencia artificial en Colombia*.
- Congreso de la República de Colombia. (2004). *Ley 906 de 2004*.
- Congreso de la República de Colombia. (2011). *Ley 1474 de 2011*.
- Congreso de la República de Colombia. (2012). *Ley 1581 de 2012*.
- Congreso de la República de Colombia. (2016). *Ley 1778 de 2016*.
- Congreso de la República de Colombia. (2022). *Ley 2195 de 2022*.

- Departamento Nacional de Planeación. (2019). *CONPES 3975 de 2019. Política Nacional para la Transformación Digital e Inteligencia Artificial.*
- Departamento Nacional de Planeación. (2025). *CONPES 4144 de 2025 sobre inteligencia artificial.*
- Superintendencia de Industria y Comercio. (2024). *Circular Externa No. 002 del 21 de agosto de 2024.*
- Superintendencia de Industria y Comercio. (2025). *Circular Externa 01 de 2025 sobre tratamiento de datos personales en servicios financieros digitales.*
-

Referentes jurisprudenciales

- Corte Constitucional. (2016). *Sentencia C-320 de 2016.*
- Corte Constitucional. (2024). *Sentencia T-323 de 2024.*
- Corte Constitucional. (2025). *Sentencia T-067 de 2025.*
- Corte Suprema de Justicia. (2014). *Sentencia SP16794-2014.*
- Corte Suprema de Justicia. (2017). *Sentencia SP-2339-2017 (Rad. 49274).*
- Superintendencia de Industria y Comercio. (2025). *Resolución 78798 de 2025.*

Referentes doctrinales

- Agencia Nacional Digital. (2024). *Presentación de “Alda”, herramienta de inteligencia artificial del MinTIC.*

- Biallas, M., & O'Neill, F. (2020). *Artificial intelligence innovation in financial services*. International Finance Corporation (IFC).
- European Parliament. (2020). *The ethics of artificial intelligence*.
- FATF. (2021). *Opportunities and Challenges of New Technologies for AML/CFT*.
- Gómez, C. (2016). *Responsabilidad penal de las personas jurídicas*.
- IBM. (s. f.). *What is the Turing Test?*
- Melo Rubiano, M. (2025). *La transparencia algorítmica como derecho fundamental: análisis de la Sentencia T-067 de 2025 de la Corte Constitucional de Colombia*. Universidad Externado de Colombia.
- OECD. (2017). *Algorithms and collusion*.
- OECD. (2019). *OECD Principles on Artificial Intelligence*.
- OpenAI. (s. f.). *GPT-3 Applications*.
- Organización Internacional del Trabajo. (2021). *Perspectivas sociales y del empleo en el mundo: el papel de las plataformas digitales laborales*.
- Organización Internacional del Trabajo. (2026). *La inteligencia artificial en la industria manufacturera: desafíos y oportunidades para la promoción del trabajo decente, la productividad y una transición justa*.
- Organización Mundial de la Salud. (2021). *Ethics and governance of artificial intelligence for health: WHO guidance*.
- Petro-González, I., Mosquera-Rentería, J., & Torres-Molina, L. (2014). *La*

responsabilidad penal de las personas jurídicas como omisión legislativa en Colombia. Revista Criminalidad.

- Tolosa, D. (2015). *Sobre la responsabilidad penal de las personas jurídicas y su incidencia en Colombia.*
- Silva, J.-M. (2008). La evolución ideológica de la discusión sobre la “responsabilidad penal” de las personas jurídicas. SSRN (versión del artículo).
https://papers.ssrn.com/sol3/Delivery.cfm/SSRN_ID1501202_code1327823.pdf?abstractid=1501202&mirid=1
- Del Rosal, B. (2023). ¿El modelo de la responsabilidad penal de las personas jurídicas para los daños punibles derivados del uso de la inteligencia artificial? REDEPEC: Revista Electrónica de Responsabilidad Penal de Personas Jurídicas y Compliance, (2). <https://dialnet.unirioja.es/servlet/articulo?codigo=9148639>
- Januário, T. F. X. (2023). Inteligencia artificial y responsabilidad penal de personas jurídicas: un análisis de sus aspectos materiales y procesales. Estudios Penales y Criminológicos, 43. <https://revistas.usc.gal/index.php/epc/article/view/8902/13236>
- Prieto, J. V. (2022). Sobre la responsabilidad penal por la utilización de sistemas de inteligencia artificial. Revista Electrónica de Ciencia Penal y Criminología, 24-27. <http://criminnet.ugr.es/recpc/24/recpc24-27.pdf>
- Gómez, C. (2016). Fundamentos de la responsabilidad penal de las personas jurídicas. En M. Bajo Fernández, B. Feijoo Sánchez y C. Gómez (Coords.), Tratado de responsabilidad penal de las personas jurídicas (2.^a ed.). Aranzadi.
https://www.researchgate.net/publication/375548728_Inteligencia_artificial_y

_responsabilidad_penal_de_personas_juridicas_un_analisis_de_sus_aspectos_materiales_y_procesales

- Navarro-Dolmestch, R. (2025). Inteligencia artificial como «actuante» en el derecho penal. Una primera aproximación. IDP. Revista de Internet, Derecho y Política, (43). <https://raco.cat/index.php/IDP/article/view/432787>
- Mongillo, V. (2024). Responsabilidad penal y extrapenal de las personas jurídicas por delitos relacionados con la inteligencia artificial: vías de intervención legal y principales obstáculos. REDEPEC. <https://www.redepec.com/wp-content/uploads/pdf/responsabilidad-penal-y-extrapenal-de-las-personas-juridicas-por-delitos-relacionados-con-la-inteligencia-artificial-v-as-de-intervencion-legal-y-principales-obstaculos-4782.pdf>