



DERECHO PENAL EN LA ERA DE LA INTELIGENCIA ARTIFICIAL

AB. DIANA ELIZABETH CORREA MANZANO. MG.

AB. JOSÉ FABIÁN MOLINA MORA. MG.

AB. CÉSAR ELÍAS PAUCAR PAUCAR. MG.

AB. CINTHIA MARIELA CAJAS PÁRRAGA. MG.

Editado y distribuido por

CASA EDITORA DEL POLO

Manta, Manabí, Ecuador 2025

Correo electrónico: revistapolodelco@gmail.com

Hecho el Depósito de Ley.

Depósito Legal:

ISBN: 978-9942-684-56-1

Serie: Derecho Penal

DERECHO PENAL EN LA ERA DE LA INTELIGENCIA ARTIFICIAL**Autores:**

Ab. Diana Elizabeth Correa Manzano. Mg.*

correaabogada15@gmail.com

ORCID ID:0009-0007-5492-6262

Ab. José Fabián Molina Mora. Mg.

docentep43@uniandes.edu.ec

ORCID ID: 0000-0002-2523-2721

Ab. César Elías Paucar Paucar. Mg.

uq.cesarpaucar@uniandes.edu.ec

ORCID ID:0000-0003-2624-0427

Ab. Cinthia Mariela Cajas Párraga. Mg.

uq.cinthiacajas@uniandes.edu.ec

ORCID ID: 0000-0003-2644-0074

Todas las obras publicadas por la Casa Editora del Polo se someten previamente a un riguroso proceso de evaluación académica llevado a cabo por pares expertos debidamente acreditados. Esta obra está destinada exclusivamente al uso personal y colectivo en actividades de carácter académico, investigativo, formativo y de divulgación científica.

Esta obra está bajo una licencia internacional

Revisión, Ortografía y Redacción

Lcda. Thalía Cifuentes Rojas MSc.

Diseño de portada

Lcda. Rosa Chicaiza Chicaiza MSc.

Diagramación:

Ing. Gabriela Almache Granda MSc.

CONSTANCIA DE ARBITRAJE ACADÉMICO PARA PUBLICACIÓN EN FORMATO DIGITAL

La Casa Editora del Polo certifica que el manuscrito presentado para su publicación en formato digital ha sido sometido a un proceso de arbitraje académico exhaustivo, conforme a los estándares internacionales de evaluación por pares.

El proceso fue desarrollado por evaluadores externos con formación doctoral, seleccionados por su solvencia académica, producción científica y experticia disciplinar. La evaluación se llevó a cabo bajo la modalidad de arbitraje doble ciego, asegurando la independencia, transparencia e imparcialidad de los dictámenes.

Los especialistas designados analizaron de manera sistemática los siguientes criterios:

- Solidez metodológica y coherencia epistemológica,
- Pertinencia, vigencia y profundidad del marco teórico,
- Originalidad, aporte científico y relevancia para el campo de estudio,
- Consistencia argumentativa, claridad expositiva y estructura lógica del texto,
- Cumplimiento de estándares editoriales, éticos y de calidad académica,
- Adecuación del contenido a los requisitos técnicos para su difusión digital.

Tras concluir el proceso de evaluación, el manuscrito obtuvo un dictamen favorable, condicionado a la incorporación de las recomendaciones formuladas por los árbitros, las cuales fueron atendidas satisfactoriamente por los autores.

Comité Editorial

**RESOLUCIÓN DEL RECTORADO DE LA
UNIVERSIDAD REGIONAL AUTÓNOMA DE LOS ANDES (UNIANDES)**

Considerando

Que, la Ab. Diana Elizabeth Correa Manzano, Mg.; el Ab. José Fabián Molina Mora, Mg.; el Ab. César Elías Paucar Paucar Mg.; y la Ab. Cinthia Mariela Cajas Párraga Mg., han desempeñado importantes funciones como profesores en la Universidad Regional Autónoma de Los Andes (UNIANDES).

Que, en el desempeño de sus funciones han demostrado capacidad profesional, eficiencia, y lealtad institucional, constituyéndose en docentes e investigadores que han propiciado el desarrollo y fortalecimiento de la UNIANDES.

Que, en el período de sus ejercicios docentes han demostrado un alto nivel de conocimientos, excelentes métodos pedagógicos y el nexos hacia sus estudiantes, por lo que han sido y son estimados y respetados en el campo académico de nuestra universidad.

Que, la Ley Orgánica de Educación Superior (LOES) prevé que las Instituciones de Educación Superior deben incentivar a sus docentes y docentes investigadores en la generación de obras de carácter científico relevante para el desempeño de sus actividades, y por ende este Rectorado apoya a los distintos docentes y profesionales administrativos para que desarrollen y publiquen obras en el contexto de su gestión.

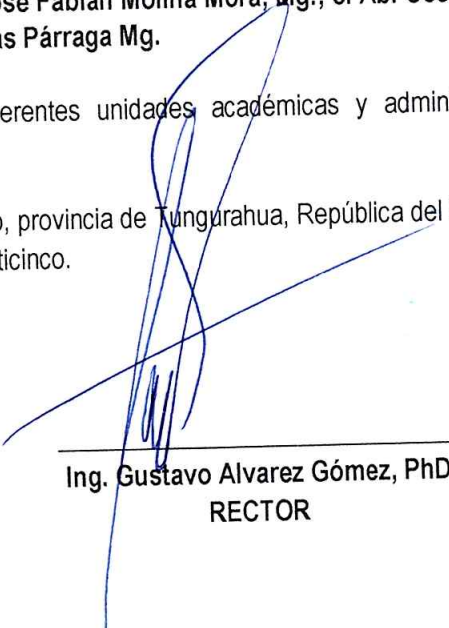
Que, la UNIANDES ha presentado los informes técnicos favorables (avales de pares) para que se impulse el desarrollo investigativo, la elaboración del contenido y la publicación de la obra **"Derecho Penal en la Era de la Inteligencia Artificial"**, la cual puede convertirse en un aporte para la comunidad científica universitaria.

Por tanto, el Rectorado de conformidad al art. 48 de la Ley Orgánica de Educación Superior y en concordancia con el art. 34 del Estatuto de la Universidad Regional Autónoma de Los Andes (UNIANDES):

RESUELVE:

- 1) Auspiciar y conceder el aval académico de la Universidad Regional Autónoma de Los Andes (UNIANDES) en favor de la investigación, desarrollo y publicación de la obra **"Derecho Penal en la Era de la Inteligencia Artificial"**, cuya autoría le corresponde a: la Ab. Diana Elizabeth Correa Manzano, Mg.; el Ab. José Fabián Molina Mora, Mg.; el Ab. César Elías Paucar Paucar Mg.; y la Ab. Cinthia Mariela Cajas Párraga Mg.
- 2) Comuníquese a las diferentes unidades académicas y administrativas para los fines legales pertinentes.

Dado en la ciudad de Ambato, provincia de Tungurahua, República del Ecuador, a los veinte días del mes de diciembre del dos mil veinticinco.


Ing. Gustavo Alvarez Gómez, PhD
RECTOR



UNIVERSIDAD REGIONAL AUTÓNOMA DE LOS ANDES UNIANDES
DIRECCIÓN DE INVESTIGACIÓN
INFORME DEL EVALUADOR DE LIBROS

Nombre y apellidos del evaluador: Ab. Iván Alfonso Carrera Gutiérrez. MSc.

Grado académico: Doctor

Institución donde labora: Universidad de Los Hemisferios

Cargo o función que desempeña: Docente

Título del libro: Derecho Penal en la Era de la Inteligencia Artificial.

Criterio	Mal	Regular	Bien	Excelente
1. El tema tratado es de actualidad e importancia para la ciencia específica.				X
2. La extensión del libro es adecuada				X
3. El análisis teórico es actualizado (más del 50% de las referencias son de los últimos cinco años)				X
4. El libro denota un aporte a la disciplina que aborda				X
5. Está bien fundamentada la teoría incluida en el libro				X
6. Se evidencia objetividad en los temas tratados				X
7. Aborda las corrientes principales de la ciencia específica				X
8. Los datos abordados en el libro se encuentran validados por métodos que lo fundamentan.				X
9. La redacción y ortografía son buenas.				X
10. Existe relación entre el título y los aspectos abordados en el libro.				X
11. Los cuadros, tablas y figuras tienen buena calidad.				X

Aspectos a comentar.

Comente en una o varias hojas los siguientes elementos relacionados con el libro.

- Actualidad e importancia del libro.
- Aporte al estudio de la ciencia específica que trata.
- Objetividad de la información presentada
- Actualidad de las citas y referencias bibliográficas.
- Validez de los datos incluidos en el libro.

Finalmente marque con una X su criterio general sobre la obra analizada

Publicar de manera directa	X
Publicar con adecuaciones menores (hasta 30 días para solucionar)	
Publicar con adecuaciones mayores (hasta 90 días para solucionar)	
No publicar	

IVAN ALFONSO CARRERA GUTIERREZ
Firma: 
Ab. Iván Carrera Gutierrez. Dr.

Firmado digitalmente por
IVAN ALFONSO CARRERA GUTIERREZ
Fecha: 2026.04.09 10:44:56 -05'00'

Fecha: 16 de abril 2026.



UNIVERSIDAD REGIONAL AUTÓNOMA DE LOS ANDES UNIANDES
DIRECCIÓN DE INVESTIGACIÓN
INFORME DEL EVALUADOR DE LIBROS

Nombre y apellidos del evaluador: Ab. Rina Rosalinda Castañeda Junco

Grado académico: Master

Institución donde labora: Universidad Técnica de Babahoyo

Cargo o función que desempeña: Docente

Título del libro: Derecho Penal en la Era de la Inteligencia Artificial

Criterio	Mal	Regular	Bien	Excelente
12. El tema tratado es de actualidad e importancia para la ciencia específica.				X
13. La extensión del libro es adecuada				X
14. El análisis teórico es actualizado (más del 50% de las referencias son de los últimos cinco años)				X
15. El libro denota un aporte a la disciplina que aborda				X
16. Está bien fundamentada la teoría incluida en el libro				X
17. Se evidencia objetividad en los temas tratados				X
18. Aborda las corrientes principales de la ciencia específica				X
19. Los datos abordados en el libro se encuentran validados por métodos que lo fundamentan.				X
20. La redacción y ortografía son buenas.				X
21. Existe relación entre el título y los aspectos abordados en el libro.				X
22. Los cuadros, tablas y figuras tienen buena calidad.				X

Aspectos a comentar.

Comente en una o varias hojas los siguientes elementos relacionados con el libro.

- f) Actualidad e importancia del libro.
 - g) Aporte al estudio de la ciencia específica que trata.
 - h) Objetividad de la información presentada
 - i) Actualidad de las citas y referencias bibliográficas.
 - j) Validez de los datos incluidos en el libro.
- Finalmente marque con una X su criterio general sobre la obra analizada

Publicar de manera directa	X
Publicar con adecuaciones menores (hasta 30 días para solucionar)	
Publicar con adecuaciones mayores (hasta 90 días para solucionar)	
No publicar	



Firmado electrónicamente por:
**RINA ROSALINDA
CASTANEDA JUNCO**

Validar únicamente con FirmaSC

Firma:

Ab. Rina Castañeda Junco MSc.

Fecha: 30 de marzo 2026.

CONTENIDO

01. Prólogo

02. Introducción

03. Capítulo 1

Introducción a la Intersección entre Derecho Penal y Tecnología

- Impacto de la inteligencia artificial en el derecho penal
- Desafíos y oportunidades
- Inteligencia artificial al servicio de los derechos de acceso

04. Capítulo 2

Fundamentos Legales y Éticos de la Inteligencia Artificial en el Derecho Penal

- Principios legales aplicables
- Aspectos legales de la IA en el derecho penal
- Principios legales aplicables
- Ética de la inteligencia artificial en el ámbito penal
- Marco regulatorio internacional y nacional
- Definición de denuncias falsas
- B. Desafíos legales y normativos
- A. Innovaciones tecnológicas y su impacto
- A. Definición y objetivos
- A. Introducción a la inteligencia artificial
- A. Principios éticos en el uso de IA
- B. Implicaciones éticas en la emisión de sentencias
- Marco regulatorio internacional y nacional

05. Capítulo 3

Riesgos y Desafíos de la Inteligencia Artificial en la Justicia Penal

- Sesgos algorítmicos y discriminación

06. Capítulo 4

Juicio y proceso penal en la era de la inteligencia artificial.

- 4.1 Automatización de procedimientos judiciales
- Utilización de algoritmos en la toma de decisiones judiciales
- Desafíos de la implementación de la IA en los tribunales
- Desarrollos jurisprudenciales y legislación sobre inteligencia artificial en el derecho penal

07. Referencias



PRÓLOGO

Este libro, Derecho penal en la Era de la IA, trata uno de los problemas más profundos y esenciales de nuestro tiempo: la convergencia de los sistemas inteligentes con la estructura del derecho penal que regula la conducta humana. Ante la incesante aceleración tecnológica y el desarrollo ininterrumpido de herramientas autónomas, es inevitable abordar la problemática de la forma en la que estas innovaciones activan el modo de legislativa, interpretativa y práctica del derecho penal. La IA se ha convertido, particularmente, en un nuevo actor cuyas potencias transforman no sólo la forma del proceso, sino, además, el modo de considerar los conceptos de responsabilidad, prueba y garantías procesales. En el primer capítulo, el lector es introducido a la compleja interacción de los avances tecnológicos y la esencia de los principios del derecho penal, presentadas de la forma más clara posible, de la que se obtiene un armamento conceptual que permite entender los nuevos problemas contemporáneos que presenta la IA. Desde este punto inicial, el libro profundiza en las bases éticas y jurídicas que son necesarias para su adecuado desenvolvimiento, subrayando la necesidad de la garantía de sistemas que sean claros, auditables y carentes de sesgos discriminatorios. De esta manera, se hace un examen de las tensiones que surgen a la hora de considerar la cuestión de la responsabilidad penal a la hora de intervenir sistemas autónomos dotados de capacidad de conocer, decidir y actuar sin supervisión, con las interrogantes hasta ahora inexploradas para la teoría del delito. El desarrollo del libro aborda también los riesgos, límites y problemas que tiene el uso de tecnologías avanzadas en la investigación y enjuiciamiento penal, que desde la manipulación de pruebas digitales a los efectos de los algoritmos en la toma de decisiones judiciales. Del mismo modo, se estudia la forma en que la inteligencia artificial puede cooperar en el fortalecimiento de la administración de justicia, ya sea por la mejora en la imposición de cargas procesales o por lo más actual que es, el análisis predictivo en materias delictivas, pero siempre bajo el resguardo estricto de los derechos y garantías constitucionales. Este equilibrio entre amenazas y oportunidades, constituye una de las reflexiones fundamentales de la obra. Sus últimos capítulos se preguntan también, como los operadores jurídicos, las instituciones del Estado, y la misma sociedad, deberán prepararse para enfrentar esta nueva forma tecnológica. La integración de la inteligencia artificial al proceso penal exige un sistema normativo robusto, formación permanente y una cultura jurídica que propugne la dignidad del hombre frente a la automatización. En este sentido se revisan doctrinas contemporáneas, marcos regulatorios emergentes, y propuestas orientadas a lograr que la administración de justicia penal progrese sin perder su esencia garantista. Esta obra fruto de un desarrollo riguroso y una reflexión crítica, debe ser consultada por juristas, docentes, alumnos y abogados en actividad, para que puedan comprender y anticiparse a los desafíos que implica la introducción en este ámbito de la inteligencia artificial. En realidad, este libro no es un estudio descriptivo, sino que propone caminos para que el derecho penal avance en paralelo a los avances tecnológicos, sin renunciar a los valores que sustentan la convivencia democrática y el respeto irrestricto de los derechos humanos. Así invita al lector a integrar un sistema penal, cuyo diseño institucional estará preparado para afrontar la era digital al servicio de la justicia en todos los órdenes.

INTRODUCCIÓN

Es necesario señalar que la llegada de la inteligencia artificial (IA) al Derecho Penal en Ecuador, es el principio de una nueva época en el que se entrelazan grandes oportunidades con grandes desafíos. Por un lado, esta IA, promete un aumento de la eficiencia y eficacia del sistema judicial, como ya está manifestado en procesos como la investigación predictiva o la automatización judicial, produciendo una bajada espectacular en los tiempos de asignación de casos. Pero esta transformación tecnológica no escapa a una serie de riesgos críticos que requieren una cuidadosa regulación y un profundo rigor ético. En este sentido, la institucionalización progresiva de sistemas inteligentes precisa de una profunda reflexión sobre las repercusiones de esta transformación tecnológica en la estructura de administración de justicia.

Este libro hace un análisis profundo de qué es la inteligencia artificial, sus características, su tipología, sus aplicaciones concretas en la justicia penal para, posteriormente, dar paso a sus posibles evoluciones futuras. Se requiere la necesidad de que el marco legal ecuatoriano pueda adaptarse para que pueda integrar controles rigurosos que aseguren un uso justo y equitativo de la IA, así como el respeto de los principios constitucionales de dignidad humana y debido proceso. Entre las dificultades, se señala la replicación de sesgos algorítmicos que pueden producir la perpetuación de desigualdades históricas entre los grupos sociales, como podría ser la sobre imputación a grupos indígenas, y las lagunas normativas en lo que respecta a la validez probatoria de las decisiones que están asistidas por IA. Igualmente se mencionan las dificultades que emergen respecto a la responsabilidad penal a que está sujeta el uso de sistemas automatizados, materia esta que ha sido poco estudiada en la doctrina nacional.

También es de vital importancia que se establezcan estándares de calidad, auditorías independientes y la utilización de equipos multidisciplinarios que aseguren una mayor transparencia y equidad. La justicia penal no debe ser sometida a la tecnología, sino que esta debe ser aplicada y diseñada para que la IA sea un instrumento que propicie el mejoramiento del sistema penal, sin que por ello se vean vulnerados los derechos humanos, ni la igualdad ante la ley. En definitiva, la idea es dar una visión crítica y fundada para que el país pueda aprovechar las ventajas de la inteligencia artificial, sin que por ello se dejen de lado las desventajas que esta inadecuada utilización podría producir.

De esta forma, se propicia un diálogo técnico entre juristas, ingenieros, criminólogos y responsables de políticas públicas, que procure una mejor gobernanza responsable de la IA. Igualmente se estima que debe promoverse una cultura institucional de evaluación permanente que permita corregir las desviaciones en el uso de estos sistemas y conseguir su mejora continua.



INTRODUCCIÓN A LA INTERSECCIÓN ENTRE DERECHO PENAL Y TECNOLOGÍA

Origen y Evolución Histórica de la Inteligencia Artificial en el Contexto del Derecho Penal

Previo a abordar este fascinante primer tema de inteligencia artificial, es necesario explorar brevemente sus orígenes, trazar su historia y entender el camino que ha recorrido. Esta herramienta creada por el ser humano se ha vuelto indispensable en nuestra vida cotidiana y juega un papel crítico en el estudio del Derecho Penal que va a tener importancia en la redacción de sentencias por parte de los Jueces. Por lo tanto, al entender los orígenes de esta transformación digital, tendremos la oportunidad de imaginar el futuro de la ia en el derecho penal y en su Código Orgánico Integral Penal. ¹La llegada de la inteligencia artificial (IA) ha revolucionado múltiples campos, y el Derecho Penal no es una excepción.

A medida que la IA se integra cada vez más en diversos aspectos de la vida cotidiana, también plantea desafíos y oportunidades significativas para el sistema de justicia penal. Esta era de transformación tecnológica requiere una revisión crítica de cómo las leyes penales se aplican y se adaptan a las nuevas realidades tecnológicas. El nacimiento de la inteligencia artificial (IA) se remonta al siglo XX, abarcando específicamente el período de 1936 a 1956. Durante estos años, emergió una figura clave en este campo: Alan Turing, originario de Londres, Reino Unido. Turing, un visionario matemático cuyas ideas parecían extraídas de películas futuristas, realizó una serie de publicaciones influyentes que sentaron las bases para el desarrollo posterior de la IA.

Además, comprender esta evolución histórica no solo permite visualizar el origen matemático y computacional de la IA, sino también reconocer cómo estos avances impactan directamente en la estructura del Derecho Penal contemporáneo. La progresiva automatización de procesos, el análisis predictivo de patrones delictivos, los sistemas de apoyo a la decisión judicial y el tratamiento masivo

¹ **Código Orgánico Integral Penal (COIP):** cuerpo normativo ecuatoriano que unifica y regula las disposiciones penales, procesales penales y penitenciarias, estableciendo los delitos, las sanciones, los procedimientos y el sistema de rehabilitación social vigente en el Ecuador.

de datos forenses demuestran que la IA ha dejado de ser una mera herramienta tecnológica para convertirse en un componente transversal que influye en la investigación, acusación y juzgamiento penal. Esta interacción creciente exige marcos normativos sólidos y una reflexión profunda sobre los límites éticos y jurídicos que deben guiar su aplicación dentro del sistema penal ecuatoriano.

Tabla 1.

Línea de tiempo de hitos fundamentales de la IA (1936–1956)

Año	Autor / Evento	Aporte Principal
1936	Alan Turing	Publica <i>Números Calculables</i> y conceptualiza la “Máquina Universal de Turing”.
1950	Alan Turing	Propone el <i>Test de Turing</i> basado en el juego de imitación.
1956	Marvin Minsky, John McCarthy, Shannon, Simon, Nevell	Conferencia de Dartmouth: se acuña formalmente el término “Inteligencia Artificial”.

Nota: Esta línea de tiempo presenta los principales hitos que marcaron el desarrollo inicial de la Inteligencia Artificial y la computación moderna entre 1936 y 1956.

En abril de 1936, Turing publicó un destacado artículo titulado números calculables en 1937. En este artículo presentó dos conceptos trascendentales. Primero, definió computador como la idea de una máquina que realiza el mismo trabajo que un humano. Segundo y más relevante, introdujo la máquina universal de Turing, Se trata de un dispositivo programable capaz de emular cualquier algoritmo informático, sin que su nivel de complejidad represente un límite insalvable. Ya finalizada la Segunda Guerra Mundial, en 1950 Turing formuló otro aporte decisivo para el plano teórico: la prueba —o test— que llevaría su nombre. Este test, basado en el juego de la imitación, busca evaluar si una máquina puede exhibir comportamientos inteligentes que sean indistinguibles de los de un ser humano. Los trabajos de Turing han tenido un impacto profundo en el avance de las ciencias computacionales, la informática moderna y, en particular, en la inteligencia artificial (IA). A pesar de la importancia de sus contribuciones, no fue hasta 1956 que la IA se estableció formalmente como un campo de investigación científica. Ese año marcó la transición de la IA de la teoría a un área concreta de estudio. El término «inteligencia artificial» fue oficialmente instaurado en la conferencia de Dartmouth College celebrada el 31 de agosto de 1956.

En dicho encuentro convergieron figuras señeras de la disciplina: Marvin Minsky, Claude Shannon, Herbert Simon y Allen Newell. Fue John McCarthy, artífice del término, quien consignó una definición llamada a marcar el rumbo del campo, entendida como «la ciencia e ingenio de hacer máquinas inteligentes, especialmente programas de cómputo inteligentes». Este grupo de científicos tenía la ambición de construir máquinas inteligentes antes del final del siglo. (Gogolin, 2021). La primera fase de gran optimismo y altas expectativas, conocida como los años dorados de la IA, tuvo lugar entre las décadas de 1950 y 1970. Sin embargo, esto fue seguido por un declive en

los años 70 y 80, debido a la disminución de financiación y el interés general por la IA, así como a promesas incumplidas y limitaciones técnicas. Desde 1994, la inteligencia artificial experimentó un repunte considerable, impulsado por los avances de la tecnología informática que permitieron sortear buena parte de los obstáculos que antes frenaban su desarrollo. Ese impulso no se ha detenido. Continúa ampliando las fronteras de lo que esta disciplina es capaz de alcanzar. En la actualidad, la IA se inscribe dentro de la cuarta revolución industrial, denominada Revolución 4.0, equiparable a las transformaciones que en su momento generaron la mecánica, la energía eléctrica y la informática sobre la sociedad y las economías, la IA está forjando un nuevo paradigma.

En marzo de 2023 se hizo visible una expansión vertiginosa de la inteligencia artificial, sostenida en capacidades como el aprendizaje automático y la toma de decisiones basada en datos, fenómenos que están reconfigurando organizaciones empresariales, estructuras estatales y las dinámicas cotidianas de las personas. Toda revolución tecnológica exige algo más que la simple participación pasiva de quienes la atraviesan. Demanda, además, una capacidad de adaptación constante frente a un ritmo de innovación que no da tregua. Erik J. Larson, especialista en la materia, sostiene que en torno a la inteligencia artificial circula un mito persistente. No se trata de negar la viabilidad futura de una IA genuina, cuestión que continúa siendo un enigma sin resolver para la ciencia. El mito señalado por Larson reside más bien en la creencia de que su advenimiento resulta ineludible y depende únicamente del transcurso del tiempo, como si ya se hubiese emprendido irreversiblemente la ruta hacia una inteligencia de nivel humano y, más allá, hacia una eventual superinteligencia.

Tabla 2.
Evolución de la IA y revoluciones tecnológicas

Periodo	Características	Estado de la IA
1950–1970	Optimismo, investigación acelerada	“Años dorados”
1970–1990	Falta de financiamiento, limitaciones técnicas	“Invierno de la IA”
2000–Actualidad	Machine learning, Big Data	Renacimiento y Revolución 4.0

Nota: La tabla resume las principales etapas históricas de la Inteligencia Artificial y su relación con los cambios tecnológicos que marcaron su desarrollo y consolidación.

Basándonos en las investigaciones científicas y la doctrina actual, podemos definir la inteligencia artificial (IA) como un software que, mediante algoritmos y una alimentación de datos, establece un objetivo y produce un resultado. Según Miguel Ángel Presno, en su libro *Derechos fundamentales e Inteligencia Artificial* de 2022, «la IA busca sintetizar o reproducir procesos cognitivos humanos, como la percepción, la creatividad, la comprensión, el lenguaje y el aprendizaje». En Europa, que está a la vanguardia de la regulación de la IA, su borrador de Ley de

Inteligencia Artificial ²define la IA como el software desarrollado usando técnicas y estrategias específicas que, para objetivos determinados por seres humanos, puede generar información como contenidos, predicciones, recomendaciones o decisiones que afectan a los entornos con los que interactúa. Es importante destacar que la IA utilizada entre los años 50 y 90 era simbólica, mientras que, a partir del año 2000, se ha basado en datos y aprendizaje automático (machine learning). La IA tiene como objetivo desarrollar sistemas capaces de realizar tareas que normalmente requieren «inteligencia humana», como el reconocimiento de voz, el aprendizaje, la planificación y el reconocimiento de patrones. Sin embargo, los humanos juegan un papel crucial en esta transformación digital. No solo ingresan datos en los sistemas de IA, sino que también establecen los algoritmos, que son las instrucciones que dirigen el funcionamiento de estos sistemas.

La eficacia de un algoritmo de IA depende no solo de su diseño técnico, sino también de cómo los humanos configuran los objetivos y estrategias. Por lo tanto, la calidad de los resultados depende de la precisión, veracidad y relevancia de los datos ingresados, así como de los objetivos y parámetros establecidos. Si se introducen datos incorrectos, los resultados no serán los deseados. En conclusión, aunque la IA se basa en máquinas, son las habilidades, experiencias y juicios humanos los que realmente impulsan y determinan su éxito. El traductor de Google y Watson son solo dos ejemplos entre muchos otros que ilustran la ola de inteligencia artificial en expansión en diversos campos.

Tabla 3.
Definiciones de Inteligencia Artificial

Fuente	Definición	Enfoque
Miguel Ángel Presno (2022)	Reproducción o síntesis de procesos cognitivos humanos.	Cognitivo-humano
Reglamento IA de la UE (borrador)	Software capaz de generar contenidos, predicciones o decisiones que afecten su entorno.	Regulatorio
Paradigma 1950–90	IA simbólica.	Lógica
Paradigma 2000–actual	IA basada en datos (ML).	Estadístico-algorítmico

Nota: Las definiciones recopiladas reflejan la diversidad de enfoques desde los cuales se ha conceptualizado la inteligencia artificial, abarcando perspectivas cognitivas, regulatorias, lógicas y algorítmicas.

² **Ley de Inteligencia Artificial:** marco jurídico que regula el desarrollo, uso, implementación y supervisión de sistemas de inteligencia artificial, estableciendo principios de transparencia, seguridad, ética, responsabilidad y protección de derechos fundamentales frente a los riesgos asociados a estas tecnologías.

Estos sistemas están involucrados en la creación de música, la pintura de cuadros, el reconocimiento de rostros y objetos, la predicción de empresas exitosas en la bolsa, la detección de enfermedades y la protección del medio ambiente, entre muchas otras aplicaciones. Estamos presenciando una verdadera carrera por desarrollar IA para simplificar y optimizar múltiples actividades humanas. En este contexto, surgen tres grandes desafíos en el ámbito jurídico: primero, cómo protegernos de los algoritmos inteligentes que pueden reemplazarnos y superar nuestras capacidades en diversas tareas; segundo, cómo asegurar que esta nueva tecnología contribuya al desarrollo sostenible e inclusivo de la humanidad; y tercero, cómo se protegerán y transformarán los derechos humanos en una transición que parece avanzar hacia una integración entre lo biológico, lo digital y lo artificial.

Tabla 4.
Desafíos del ámbito jurídico

Desafío	Explicación
Riesgo de sustitución humana	Algoritmos que superan capacidades humanas.
Desarrollo sostenible e inclusivo	Evitar brechas digitales.
Protección de derechos humanos	Afectaciones en privacidad, igualdad, justicia.

Nota: Los desafíos identificados reflejan la necesidad de regular el uso de la IA para garantizar que su implementación respete los derechos fundamentales y promueva la equidad en el ámbito jurídico.

Para encarar estos desafíos podemos partir de dos grandes líneas. La primera hace referencia a lo que podríamos llamar el “lado amable de la inteligencia artificial”. En este caso, la técnica tiene un valor disruptivo en la medida que logra hacer efectivos ciertos derechos y se produce un avance notable en la gestión de organizaciones y sus entornos con los ciudadanos. ((2020)) La segunda línea se relaciona con lo que denominamos el “lado oscuro de la IA”. Desde esta óptica es muy importante darle preponderancia a posibles riesgos, como la pérdida de control que se produce en el ser humano respecto de los sistemas de inteligencia artificial que se desarrollan, pero este problema será proyectado a mediano y largo plazo. A corto plazo es importante considerar los problemas que genera en los derechos fundamentales de los seres humanos el desarrollo y uso de sistemas de IA. Seguidamente, se harán algunas propuestas breves en relación a las dos líneas. Suele hablarse de un desarrollo asimétrico, que suele ser la característica de países menos aventajados. En el desarrollo tecnológico está la presencia de este fenómeno, donde da cuenta de asimetrías varias en el desarrollo. Por ejemplo, en la CABA hay una Administración Pública totalmente digital (además se ha dictado más de 58 normas que regulan el proceso de digitalización de la administración pública), por el contrario, en algunas provincias no ha comenzado el proceso. Esto se da también a un nivel mucho más abarcativo. En la actualidad el 17% de la población mundial, 1300 millones de personas, no tiene acceso a los beneficios de la segunda revolución industrial

(electrificación). Y más de la mitad de la población mundial, 4000 millones de personas, no tiene aún acceso a internet. Las asimetrías en el desarrollo van acompañadas con la necesidad de protección y efectivización de derechos asimétricos también usufrutuados. Es decir, se va a tener que afrontar el problema de derechos de “primera necesidad” (acceso al agua, acceso a servicios elementales, etc.), pero también hay que avanzar en la protección contra otras violaciones masivas de derechos en el plano digital. En ocasiones, aunque suele ser lo más habitual, se tiende a pensar que como es difícil resolver ciertos problemas implícitos de una urgencia mayor, sería ilógico afrontar otros. Sin embargo, es importante razonar y actuar en sentido inverso. Si bien es cierto que hay que expedirse en cuestiones básicas, es indispensable ya iniciar una actividad tendiente a abordar los nuevos desafíos de llegar a un estado de cosas que de esta manera parta de un espectro más amplio de violaciones de derechos. Por ejemplo, existen en el ámbito del derecho penal numerosos desafíos que son complejos de resolver (tráfico de drogas, comercialización ilegal de todo tipo, robo a mano armada, etc.). Pero a la vez, estamos frente a nuevas circunstancias que ofrece el uso del mundo digital y se presentan nuevos derechos que hay que tutelar. Nos referimos a todas las cuestiones vinculadas al cibercrimen (cyberbullying, pornografía infantil, grooming, estafas, etc.). ((Mendoza) Al mismo tiempo también hay que tutelar a los ciudadanos de estos derechos violadores. En síntesis, el desarrollo asimétrico, es un factor adicional que complejiza y acrecienta la esfuerzo para hacer efectivos los derechos de los ciudadanos.

En toda Latinoamérica y en particular en la Argentina existen diferencias y disparidades que involucran a los ciudadanos, a sus distritos, a sus lugares de mayor vulnerabilidad. Por un lado, hay que considerar la brecha digital que existe entre los ciudadanos que tienen posibilidades de estar conectados a internet y los que no. Por el otro existe una organización y un desarrollo de los poderes públicos asimétricos en cuanto a la infraestructura y su desarrollo. Pero esto no quita que el Estado no esté en condiciones de avanzar y realizarlo sobre varios frentes a la vez, a la par que realiza una aceleración de la transición hacia el nuevo espacio y tiempo al que hay que adecuarse. De lo contrario, en la medida que se espera será el ciudadano el que “pierde”. Por ejemplo, los múltiples problemas de Internet y de las redes (todas cuestiones vinculadas al cibercrimen y a la privacidad) hacen tiempo que afectan a muchas personas que están conectadas sin importar si viven en provincial argentinas distintas (Formosa, Tierra del Fuego, etc.), Brasil, Francia o Italia.

En un sentido progresivo este enfoque está vinculado a un nuevo paradigma tecnológico que se denomina la inteligencia en la interfaz. Desde esta óptica la interfaz tiene conocimiento acerca del usuario, lo comprende en el contexto, existe un carácter protagónico y se va perfeccionando con la experiencia. Para que se comprenda mejor veamos cómo se llevan a cabo las interrelaciones en el mundo digital. Por un lado, existe un sistema en donde el usuario tiene la posibilidad de elegir el

orden del trayecto y la tecnología une los puntos, tal como ocurre con los hipervínculos. Por el otro, existe lo que se denomina “portal” donde el usuario elige el canal por donde se comunica la tecnología con la cual recibe el contenido. Y en tercer lugar existe una de las más empleadas que tiene que ver con los motores de búsqueda (el más célebre de ellos, es Google). Aquí el usuario establece un ¿cuál es el objetivo que desea indagar? Y la tecnología busca la información buena y pertinente para remitirla.

Impacto de la inteligencia artificial en el derecho penal

La IA y su relación con el Derecho y la Justicia penal los nuevos paradigmas del aprendizaje profundo y otros modelos matemáticos abren la posibilidad de un futuro en el que los sistemas informáticos puedan aprender de manera autónoma, lo que constituiría una inteligencia artificial (IA) verdaderamente autónoma. Esto explica por qué ya se están planteando los retos legales que tales sistemas de IA podrían implicar.

Se está considerando la necesidad de regular o incluso prohibir el diseño de IA letales para fines militares; se está proponiendo la creación de un derecho específico para robots, como en el proyecto RoboLaw³; y se busca controlar los sistemas de IA que puedan mejorar o reproducirse a sí mismos, como se establece en la Convención de Asilomar⁴ celebrada en 2017 en Pacific Grove⁵, California, Estas propuestas, en mayor o menor medida, abordan el reconocimiento de identidad para las IA autónomas. Esto podría influir en su responsabilidad legal, ya que podrían actuar como sujetos libres, e incluso como sujetos morales, lo que plantearía la cuestión de su responsabilidad penal. Además, surge la necesidad de proteger a estas IA como bienes de especial tutela o como sujetos con derechos más o menos equivalentes a los de las personas. (celebrada, 2017). Sin embargo, no solo estamos lejos de alcanzar una verdadera inteligencia artificial (IA) autónoma, sino que la IA existente ya plantea retos significativos para el Derecho penal que no deben ser ignorados. La IA actual, que se basa en algoritmos de predicción para realizar acciones o recomendaciones a partir de datos existentes, y cuya operativa depende completamente de la información y algoritmos proporcionados por los humanos, no requiere por ahora cambios en el sistema de atribución de responsabilidad diseñado para seres humanos. Este sistema podría necesitar ajustes en el futuro si desarrollamos IA con rasgos de autonomía.

³ **RoboLaw** fue un proyecto europeo (2012–2014) que analizó los desafíos éticos y legales de la robótica y la IA, proponiendo lineamientos regulatorios.

⁴ Conjunto de 23 principios éticos establecidos en 2017 durante la conferencia Beneficial AI en Asilomar, California, orientados a guiar el desarrollo seguro, transparente y beneficioso de la inteligencia artificial a nivel global.

⁵ **Pacific Grove**: Localidad del estado de California, Estados Unidos, reconocida por ser la sede de la conferencia donde se formularon los Principios de Asilomar sobre Inteligencia Artificial en 2017

El impacto de la inteligencia artificial (IA) en el derecho penal también se manifiesta en el aumento del uso de herramientas algorítmicas en la investigación delictiva, como los sistemas de reconocimiento facial, análisis predictivos y minería de datos, lo cual, entre sus principales resultados, promete facilitar la detección de delitos, la anticipación de patrones de criminalidad y la mejor distribución de recursos policiales. Ahora, la incorporación de dichas tecnologías, que podrían parecer en sí mismas inmejorables, plantea riesgos considerables, sobre todo cuando los algoritmos reproducen sesgos raciales, étnicos o socioeconómicos resultantes de los datos con que han sido entrenados. Todo lo cual, lleva a la necesidad de un debate serio sobre la validez de estas herramientas como pruebas, así como de la necesidad de evaluaciones técnicas independientes, que aseguren que se alcancen niveles de precisión y equidad. El uso de la IA en el proceso penal plantea desafíos severos a las garantías constitucionales. La automatización de decisiones judiciales como la fijación de medidas cautelares o valoración del riesgo de reincidencia puede afectar principios esenciales como el debido proceso, motivación de las resoluciones o la presunción de inocencia. La opacidad de los modelos de “caja negra” combinada a la imposibilidad de comprender del todo en qué consisten los algoritmos y la manera en que ponderan ciertos factores, puede arrojar resultados en que las decisiones que tengan que ver con los procesados sean tomadas de manera automatizada y sin posibilidad real de cuestionarlas. Por tal motivo se refuerza la importancia de que la supervisión humana de estas actividades siga siendo el eje central y fundamental de la actividad jurisdiccional. Finalmente, el avance acelerado de la IA exige que el derecho penal tenga una actitud proactiva, que le permita adelantarse a los eventuales, nuevos escenarios que puedan ir apareciendo, antes de que la tecnología supere el nivel de respuesta normativo. Esto implica evaluar también la posible creación de nuevos tipos penales relativos a la manipulación algorítmica, ciberataques avanzados o daños por sistemas inteligentes en circunstancias excepcionales, así como necesariamente fomentar la formación de los operadores de justicia en alfabetización digital y tecnológica. Así, es importante que jueces, fiscales y defensores cuenten con herramientas suficientes para entender la naturaleza técnica de dichos avances. Solo así podrá haber un equilibrio entre innovación y protección de garantías que permita construir un sistema penal preparado para los desafíos de la era algorítmica. No obstante, la aplicación de algoritmos en el sistema de justicia penal y la posibilidad de que las máquinas, sean materiales o inmateriales, causen daños a intereses protegidos por la ley como son la vida o el orden económico, ha hecho necesario presentar además un asomo a la ética relacionada con la construcción de estos instrumentos. Esto nos obliga a pensar también en su implicación en el orden penal. La doctrina penal ha mostrado interés particular en este aspecto, por lo que han ocurrido accidentes y daños económicos en relación con los robots, tanto en el ámbito del trabajo como en el tráfico, en el cual la conducción autónoma está

empezando a dar sus primeros pasos. Pero, además, los sistemas de IA basados en modelos de aprendizaje complejo hacen difícil poder hablar de la definición del curso causal de las decisiones que tomen las máquinas. Esto ha conducido a plantear por la doctrina si el modelo de responsabilidad fundado en la teoría del delito resulta suficiente y a plantear soluciones interpretativas para el caso de que se presente la ocasión de siniestros causados por máquinas. La conclusión general parece ser que mientras no se dé una autonomía a las personas que tienen en su poder la IA, los sistemas de la teoría del delito resultan válidos para abordar problemas de causalidad y responsabilidad, aunque se cuentan en idea general como imprudencia. Es preciso no obstante vigilar cual será la evolución por el lado de atribución de responsabilidad de la IA, para que no ocurra un día un problema en donde el aprendizaje de las máquinas no permita identificar responsables de decisiones imprudentes con resultado de daños. Muchos de los dilemas éticos importantes que hay en la actualidad, en especial en el caso de la conducción autónoma, y en aquellos otros que entrañan riesgos, pero también en relación con las "máquinas inteligentes" están relacionados íntimamente con la responsabilidad penal.

Los dilemas de estado de necesidad en la conducción autónoma, analizados brillantemente por Coca Vila, J. (2023). Responsabilidad penal y ética en la inteligencia artificial. pp. 45-46. demuestran que el sistema de la teoría del delito, influido por el consecuencialismo y el de ontologismo⁶, puede ser un aliado para tomar mejores decisiones éticas en el desarrollo de IA. Sin embargo, puede ser que los penalistas todavía estemos demasiado enfocados en el ámbito físico, particularmente en el contexto del delito de homicidio, y por ello solo nos preocupemos por la IA en relación con estos tipos de resultados lesivos. Además, el tradicional olvido que quienes nos dedicamos al Derecho sustantivo solemos tener respecto al Derecho penitenciario y, aún más, al Derecho procesal penal, ha llevado a que prestemos menos atención a los problemas que la utilización actual de la IA plantea para aspectos fundamentales como la privacidad y el funcionamiento del sistema penal. (Coca Vila, 2023).

Hoy en día, la IA es una realidad en la actuación policial para la prevención e investigación de delitos, y está comenzando a tener un papel en la determinación judicial y el tratamiento penitenciario. Por ello, es crucial que su uso en el sistema de justicia penal se base en los principios fundamentales de esta área del Derecho. Es necesario que nosotros, como especialistas, asumamos la responsabilidad de abordar estos temas. Como se ha mencionado, la destacada capacidad de la

⁶ **Ontologismo:** corriente filosófica que sostiene que el conocimiento humano tiene un origen directo en la intuición del ser o de la realidad absoluta, priorizando la ontología como fundamento del pensamiento y del conocimiento.

inteligencia artificial (IA) para gestionar y procesar diversos tipos de datos con gran precisión ha suscitado interrogantes sobre su utilidad en la justicia penal.

Es innegable que las aplicaciones potenciales de la IA en este ámbito son amplias y están en constante expansión, con desarrollos que probablemente abarcarán un alcance mucho mayor en el futuro. Para simplificar, y con el objetivo de distinguir entre los dos principales ámbitos de aplicación de la IA en EE.UU., donde se ha desarrollado tanto el uso como la discusión académica, podemos clasificar los usos actuales y futuros de la IA en el sistema de justicia penal en dos grandes categorías: (1) IA para la prevención e investigación policial del crimen, a la que llamaremos Inteligencia Artificial Policial ⁷(IAP), y (2) IA aplicada al proceso de determinación judicial de la responsabilidad por delitos, que denominaremos Inteligencia Artificial Judicial (IAJ).

Tabla 5.
Diferencias entre IAP e IAJ

Aspecto	IAP (Policial)	IAJ (Judicial)
Finalidad	Prevención e investigación	Apoyo en sentencias
Datos usados	Georreferenciales, patrones de crimen	Datos personales, variables de riesgo
Riesgos	Privacidad, vigilancia excesiva	Sesgos, transparencia algorítmica
Ejemplos	PredPol, análisis de metadatos	COMPAS, PEIRCE-IGTT

Nota: La distinción entre IAP e IAJ permite identificar las diferencias en objetivos, tipos de datos y riesgos asociados, aspectos clave para su adecuada regulación en el sistema penal.

Aunque el interés académico y jurídico en España y en el resto del mundo ha estado más enfocado en la IAJ debido a las implicaciones potenciales para los derechos fundamentales que surgen de su mal uso, es crucial también considerar la IAP. Esto no solo se debe a que su uso práctico es considerablemente mayor y está en camino de generalizarse en el ámbito policial, sino también porque sus implicaciones éticas y jurídicas, especialmente en relación con la privacidad, son igualmente importantes. La IA en la Prevención del Crimen en lo que respecta a la Inteligencia Artificial Policial, su creciente adopción en países como EE.UU. y el Reino Unido sugiere que es probable que estos sistemas se integren ampliamente en los diversos niveles de la actuación policial en un futuro cercano. Desde una perspectiva optimista sobre el impacto de la tecnología en la prevención del crimen, la IAP representa una evolución natural de las técnicas tradicionales de análisis del delito.

⁷ **Inteligencia Artificial Policial:** conjunto de sistemas y algoritmos utilizados por instituciones de seguridad para analizar datos, predecir patrones delictivos, optimizar la gestión operativa y apoyar la toma de decisiones en tareas de prevención, investigación y vigilancia policial.

A pesar del extenso conocimiento que los oficiales de policía tienen sobre las dinámicas del crimen, no siempre tienen la información necesaria para identificar con precisión dónde y cuándo ocurrirán los delitos, ni para saber qué tipos de delitos investigan mejor. Detectar patrones específicos de crimen y comportamientos criminales sigue siendo una tarea compleja que requiere almacenamiento masivo de datos y un análisis adecuado para extraer inteligencia útil. El Papel de la IA en la Ciberdelincuencia, Además de la prevención e investigación de crímenes tradicionales en entornos físicos, los avances en Tecnologías de la Información y Comunicación han dado lugar a nuevas formas de delito en el ciberespacio.

Estos desarrollos ofrecen oportunidades para que los delincuentes cometan una variedad de delitos. Las agencias de seguridad, enfrentadas a estas nuevas amenazas, están cada vez más enfocadas en la necesidad de soluciones para predecir y prevenir la ciberdelincuencia. Históricamente, el enfoque principal ha estado en identificar vulnerabilidades en las infraestructuras digitales susceptibles de ser atacadas. Sin embargo, en la última década se han desarrollado sistemas de Inteligencia Artificial Policial (IAP) cada vez más avanzados, capaces de detectar y prevenir una amplia gama de amenazas en tiempo real. (Díaz, 2020)

Estos sistemas están diseñados para ser flexibles y adaptables, y toman decisiones informadas para enfrentar diversos riesgos. Además del interés en la prevención técnica de la ciberdelincuencia, hay un creciente enfoque en el llamado Factor Humano en la ciberseguridad. Este enfoque examina la motivación de los delincuentes cibernéticos, las redes criminales organizadas, las actividades en línea de posibles víctimas y estrategias para abordar la criminalidad cibernética desde una perspectiva más social. También se está prestando atención a cómo las redes sociales contribuyen a la radicalización y la difusión de contenido delictivo. Como resultado, hay una necesidad emergente de herramientas que puedan analizar automáticamente grandes volúmenes de datos de estas plataformas digitales, facilitando la investigación y prevención de estos tipos de crimen. En ambos contextos, las IAP modernas integran datos específicos del entorno digital, como metadatos. Estos datos incluyen información sobre el medio de creación, el propósito, la hora y fecha de creación, el autor, la ubicación en la red, las normas aplicadas, el tamaño del archivo, la calidad de los datos, la fuente y otros detalles. La inclusión de estos metadatos ha demostrado ser fundamental para la predicción efectiva de delitos cibernéticos.

La inteligencia artificial en el ámbito de la justicia penal la integración de tecnologías de Inteligencia Artificial (IA) en el sistema de justicia penal está generando un creciente interés académico y social, debido a las importantes implicaciones que puede tener para mejorar el sistema de justicia, así como

a los posibles riesgos que plantea para los derechos y garantías fundamentales. Aunque el uso de algoritmos de "policía predictiva" ha ganado popularidad, la Inteligencia Artificial Judicial (IAJ) aún no se ha generalizado por completo.

Tabla 6.
Herramientas judiciales basadas en IA

Herramienta	Función	País / Contexto
STEVIE	Estructura de sentencias	Europa
EMBRACE	Evaluación probatoria	UE
ECHO	Razonamiento judicial	UE
PEIRCE-IGTT	Análisis de pruebas	Sistemas pilotos
COMPAS	Valoración de riesgo	EE.UU.

Nota: Las herramientas listadas representan algunos de los sistemas más utilizados o experimentales en la administración de justicia, destacando su diversidad funcional y los distintos contextos regulatorios donde operan.

Sin embargo, su uso en diferentes etapas del proceso judicial penal por diversos operadores legales está empezando a ser más común, y se prevé que se vuelva aún más frecuente en el futuro, la IA tiene numerosas aplicaciones potenciales en el ámbito de la justicia penal. Estas incluyen la sistematización y análisis de la gran cantidad de documentación presente en los procesos judiciales para mejorar la eficiencia, especialmente en términos de tiempo, así como el uso de herramientas que asisten a los jueces en la valoración de pruebas y en la estructuración de su razonamiento, como STEVIE, EMBRACE, ECHO, y PEIRCE-IGTT, entre otras. (Abreu, 2013).

A pesar de la utilidad potencial de estas herramientas para mejorar la justicia, el mayor interés se centra en aquellas que apoyan a los tribunales en la toma de decisiones en casos penales. En particular, las herramientas diseñadas para evaluar automáticamente los factores de riesgo que podrían prever la conducta delictiva futura están ganando relevancia. Estas herramientas, conocidas como Sistemas de Inteligencia Artificial Judicial de Valoración del Riesgo (IAJVR), se basan en la automatización de las evaluaciones de riesgo y pueden aplicarse en diversas decisiones judiciales, como la determinación del régimen penitenciario, la concesión de libertad provisional y condicional, y la reubicación de reclusos.

El funcionamiento de estos sistemas se basa en el análisis de conjuntos de datos para identificar patrones y relaciones entre variables que permitan predecir el comportamiento futuro. Estas herramientas van más allá del juicio psicológico clínico tradicional, utilizando estudios analíticos sistematizados que se han aplicado durante décadas a ciertos delitos graves y están comenzando a

extenderse a otros tipos de delitos. Es importante no confundir las herramientas actuariales tradicionales con las herramientas IAJVR ⁸ actuales y futuras. Aunque las primeras incluyen elementos automatizados, para que una herramienta sea considerada IA, la intervención de la máquina debe ser fundamental. Es pertinente indicar que la Inteligencia Artificial (IA) puede definirse como el uso de sistemas computacionales diseñados para imitar procesos cognitivos humanos.

Estos sistemas combinan conceptos de estadísticas, computación y otros campos relacionados, con el objetivo de desarrollar estructuras automatizadas capaces de realizar tareas que habitualmente requieren de inteligencia humana. En el ámbito del derecho penal, la aplicación de la Inteligencia Artificial está en pleno crecimiento. Este campo emergente presenta tanto oportunidades innovadoras como desafíos significativos. La IA tiene el potencial de transformar varios aspectos del sistema de justicia penal, aunque también plantea cuestiones importantes que deben ser abordadas con cuidado. A continuación, se destacan algunas de las principales características de esta tecnología en el contexto legal:

1. *Análisis Predictivo Basado en Datos:* La IA puede procesar grandes volúmenes de datos legales para identificar patrones, proyecciones y tendencias que podrían ser relevantes para la toma de decisiones en casos penales. Esto permite a jueces y fiscales estar mejor informados y preparados para emitir juicios y recomendaciones, fundamentadas en datos históricos y especificaciones particulares de cada caso. Los abogados también se benefician al contar con información más detallada para preparar sus argumentos.
2. *Optimización de Tareas Legales:* La digitalización de datos mediante IA puede acelerar y simplificar diversas tareas legales, como la revisión de documentos, la verificación de información y el análisis de antecedentes. Esto libera a los abogados y otros profesionales del derecho de tareas repetitivas y les permite concentrarse en aspectos más estratégicos y complejos de sus casos.
3. *Predicción de Resultados Judiciales:* Algunos sistemas de IA tienen la capacidad de simular posibles escenarios de juicios, proporcionando análisis detallados de los resultados que podrían surgir. Esta capacidad predictiva es útil tanto para los operadores de justicia como para los abogados y otras partes involucradas en un litigio.
4. *Detección y Prevención de Conductas Reincidentes:* La IA puede analizar patrones de comportamiento delictivo para prever la posibilidad de reincidencia. Identificar estas

⁸ **IAJVR:** conjunto de tecnologías de *Inteligencia Artificial para la Justicia, la Vigilancia y la Revisión*, orientadas a apoyar tareas judiciales, monitoreo institucional y análisis automatizado de información para mejorar la eficiencia y precisión en procesos legales y de control.

tendencias de manera temprana puede ser crucial para desarrollar estrategias de prevención del delito y gestionar de manera más efectiva a los individuos que han cometido delitos.

La integración de la Inteligencia Artificial en el derecho penal requiere un enfoque meticuloso respecto a varios temas cruciales, como la transparencia, la equidad, la protección de la privacidad y la correcta interpretación de los resultados. Es fundamental encontrar un equilibrio entre el uso de la tecnología y la toma de decisiones humanas, que debe basarse en el juicio y la experiencia profesional. Para asegurar el respeto a los derechos fundamentales y mantener la integridad del sistema de justicia, la incorporación de la Inteligencia Artificial en el derecho penal debe ser un proceso cuidadosamente regulado y supervisado.

La implementación de estas tecnologías debe considerar tanto los beneficios como las implicaciones éticas y legales, garantizando que se respeten los principios de justicia y equidad. El uso de la Inteligencia Artificial (IA) ha ido en aumento conforme las tecnologías han evolucionado. Sin embargo, ha sido la Emergencia Sanitaria reciente la que ha impulsado a la administración de justicia a adoptar de manera más abrupta el uso de la IA para seguir prestando sus servicios. ((Mendoza). A continuación, se presentan ejemplos que ilustran cómo la IA está siendo utilizada en el ámbito jurídico, tanto en el ámbito judicial como fuera de él. La integración de la IA en la administración de justicia comenzó de manera gradual con el uso de herramientas tecnológicas simples, como los motores de búsqueda de jurisprudencia, y ha evolucionado hasta incluir asistentes artificiales para estandarizar condenas y algoritmos para tomar decisiones. En China, por ejemplo, existe Xiao Fa, un asistente artificial cuyo nombre se traduce como “pequeño derecho”.

Este sistema fue probado por primera vez en 2004 en Shandong para casos penales, con el objetivo de estandarizar condenas y generar borradores de sentencias automáticamente. Esto llevó a la creación del primer tribunal virtual en Hangzhou en agosto de 2017, seguido por la apertura de tribunales similares en Pekín y Guangzhou. Estos tribunales en línea se encargan de asuntos relacionados con operaciones en red, comercio electrónico y propiedad intelectual (The Technolawgist, 2020). La participación de la IA no se limita a la recopilación de información; hoy en día, hay sistemas que ayudan a los jueces a dictar sentencias o a resolver conflictos en contextos extrajudiciales.

En Estonia, se han realizado pruebas piloto con jueces robot para casos con un valor que no supera los 7000 euros, con el objetivo de simplificar los servicios judiciales. Un desafío significativo es obtener la aceptación de los usuarios, que temen que la calidad del servicio se vea afectada por la IA. En estos ensayos, las partes presentan sus documentos en una plataforma, y la IA decide sobre

el caso, aunque las decisiones están sujetas a revisión por un juez humano, asegurando así un grado de supervisión humana. En Colombia, actualmente no se cuenta con herramientas que sustituyan al juez en la toma de decisiones, que sigue siendo una función principalmente humana.

Sin embargo, la influencia de la IA puede ser crucial al momento de dictar sentencia. La IA tiene una presunción de legitimidad basada en la confianza en métodos científicos y resultados racionales. Aunque las pruebas científicas suelen ser más confiables para establecer hechos y reducir errores, la implementación de IA promete optimizar el sistema judicial al reducir riesgos de error y mejorar la eficiencia procesal. En este sentido, el proceso penal está experimentando un impacto significativo debido a la incorporación de la tecnología.

Desafíos y Oportunidades

En la actualidad, la Inteligencia Artificial (IA) se valora en gran medida por su potencial para lograr avances significativos, como la posibilidad de colonizar Marte o extender indefinidamente la vida humana. El interés por la inteligencia artificial es creciente, pues ofrece soluciones a diversas necesidades, incluso en lo jurídico. Sin embargo, el mismo, muchas veces es omiso en los peligros que acarrearán sus consecuencias. Tradicionalmente, el derecho ha sido una práctica intrínsecamente humana siendo el juez un actor fundamental en la procuración de justicia. La ciencia jurídica ha estudiado y tratado de definir cómo debe pensar un juez para que sus decisiones aparejen el derecho de manera correcta. Sin embargo, la incorporación de la inteligencia artificial podría propiciar un cambio radical en el funcionamiento de los tribunales públicos. La inteligencia artificial trae consigo inmensos peligros y retos ante los derechos fundamentales de los individuos. Su uso indiscriminado podría traer como resultado sentencias arbitrarias o ilegítimas y, en el peor de los casos, un estancamiento del derecho. Pese a que sería una calamidad de enorme perjuicio, una imprudente decisión que se tomase al efecto de rechazar la inteligencia artificial, por el arraigo fenómeno social que representa en más de un área del desempeño humano y en el proceso penal, importa valorar con razón dicho fin. Este artículo tratará de cómo la aplicación masiva y sistemática de algoritmos que se han desarrollado, como es el caso del algoritmo que ha creado la IBM Watson, incide en el proceso penal. La aplicación aiosa de la tecnología referida podría ser justificada por la premura que se busca en la rapidez en la administración de justicia y la eficiencia del proceso, sin embargo, la velocidad en la emisión de las sentencias podría comprometer la calidad y certeza en la dictada. (Zaptest). Por Inteligencia Artificial se entiende toda una gama de sistemas informáticos que realizan actividades que normalmente requieren la inteligencia humana, tales como aprender, pensar, razonar, decidir y resolver. En el campo del derecho Penal, la inteligencia artificial se utiliza en dos áreas fundamentales: Inteligencia Artificial policiaca IAP: Aquí se incluye una serie de

herramientas dedicadas a la prevención e investigación de crímenes. Como ejemplo de las mismas podemos señalar los sistemas de análisis predictivo, que detectan los patrones de los delitos y son capaces de prever delitos futuros. Inteligencia Artificial Judicial IA-J: Estas herramientas operan en el área de la fase judicial con el objeto de determinar la valoración de los riesgos (predictiva), de analizar las pruebas y ayudar a la toma de decisiones. En este caso se tienen herramientas para valorar al efecto el riesgo, así como para realizar análisis de volumetrías más allá de las pruebas (grandes volúmenes de información procesal). En el campo de la inteligencia artificial puede valorarse su uso en estas diversas funciones: Policía predictiva: que utiliza algoritmos para el análisis de datos y prevé los delitos antes de que ocurran. Análisis de pruebas: herramientas que atacan el objeto de las pruebas para ser utilizadas por los Jueces en el sentido de valorar grandiosos volúmenes de las mismas y poder emitir decisiones judiciales. Valoración de riesgos: sistemas que, evaluando las probabilidades de reincidencia, ayudan a la determinación de la libertad condicional y otras disposiciones.

Uno de los desafíos principales es garantizar que el uso de la IA en el sistema penal no transgreda los derechos fundamentales de los usuarios. Esto incluye; Privacidad. Los sistemas de IA recogen y analizan volúmenes significativos de datos. Y esto puede significar perder la privacidad de las personas. (Chamorro, 2020) La opacidad de los algoritmos de la IA puede dificultar el entender cómo se toman las decisiones. Esto afecta el derecho a tener un juicio justo. Discriminación. Los algoritmos pueden ahondar en la discriminación que ya existe en los datos; y pueden tomar decisiones discriminatorias, basadas en la raza, el género o el estado socioeconómico. El uso de la IA en el derecho penal presenta la pregunta de la responsabilidad y de la rendición de cuentas: Responsabilidad Penal. ¿Quién es responsable?, si un sistema de IA comete un error y conduce a una condena injusta? La imputación de la responsabilidad penal es un área que se tiene que desarrollar. Errores de IA. Los sistemas de IA pueden tener errores o confusiones que afectan a la justicia. Determinar la responsabilidad en estos casos es complicado. La inserción de la IA en el sistema penal exige que haya una correcta regulación para garantizar su uso ético y eficaz: Normativas. Es muy importante la creación de marcos jurídicos y normativas, que den una guía sobre el uso de la IA en el derecho penal; garantizando el respeto a los derechos humanos y la igualdad. Control y supervisión. Es necesaria una supervisión y control fidedignos, para prevenir abusos y que los sistemas de IA son justos y transparentes. La IA tiene la posibilidad de mejorarse la eficacia del sistema penal. Procesamiento de datos. Los sistemas de IA pueden tratar y analizar, de forma inmediata, grandes volúmenes de datos; mejorando así la celeridad en la tramitación judicial. Reducción de la carga del trabajo. Otorgar la posibilidad de automatizar tareas rutinarias y ayudar a los jueces y abogados en la revisión de la prueba puede reducir el número de trabajo. La

IA puede mejorar la precisión de los resultados en la judicatura. Evaluación de riesgos. Existen herramientas de IA que pueden aportar evaluaciones más certeras de los riesgos de reincidencia, contribuyendo así a hacer una decisión más informada de las medidas cautelares y de la libertad provisional. Análisis predictivo. También podría la IA determinar patrones o tendencias en el delito, ayudando a prevenir el delito antes de que se produzca.

La IA puede facilitar las investigaciones penales: *Reconocimiento de Imágenes*: Sistemas de IA pueden analizar imágenes y videos para identificar sospechosos y evidencias. *Análisis de Redes Sociales*: Herramientas de IA pueden analizar datos de redes sociales para detectar actividades delictivas y redes criminales. El uso de IA en el sistema penal plantea varias cuestiones éticas: *Autonomía de la Máquina*: La capacidad de IA para tomar decisiones plantea preguntas sobre la autonomía de las máquinas y la influencia humana en la justicia. *Equidad y Justicia*: Asegurar que los sistemas de IA no perpetúen sesgos y mantengan la equidad es crucial.

El desarrollo de un marco legal para el uso de IA en el Derecho Penal es esencial: *Legislación Específica*: Se deben crear leyes específicas para regular el uso de IA en el sistema penal, abordando temas como la protección de datos y la responsabilidad. *Desarrollo Continuo*: El marco legal debe adaptarse continuamente para enfrentar los avances tecnológicos y los nuevos desafíos que surgen. Examinar casos de estudio internacionales puede proporcionar una visión valiosa sobre el uso de IA en el *Derecho Penal*: *Estados Unidos*: El uso de IA en la policía predictiva y la evaluación de riesgos en la libertad condicional. Reino Unido: La aplicación de IA en la revisión de pruebas y en la gestión de casos judiciales. En América Latina, las iniciativas sobre IA en el sistema penal son aún incipientes, pero se están desarrollando proyectos que buscan integrar tecnologías avanzadas para mejorar la justicia penal. (Coca Vila, 2023)

La inteligencia artificial presenta tanto desafíos como oportunidades para el Derecho Penal. Si bien ofrece el potencial para mejorar la eficiencia y precisión del sistema judicial, también plantea riesgos significativos para los derechos fundamentales y la justicia. Es esencial que el sistema penal desarrolle marcos legales adecuados y establezca controles rigurosos para garantizar que la IA se utilice de manera ética y efectiva. A medida que la tecnología avanza, el Derecho Penal debe adaptarse para enfrentar estos nuevos desafíos y aprovechar las oportunidades que la IA ofrece para mejorar la justicia. (Figuerola, 2022). Aunque quizás no lo notemos plenamente, estamos viviendo una etapa sin precedentes en la historia de la humanidad.

Esto se debe, entre otras razones, a la eliminación progresiva de las barreras lingüísticas de manera casi instantánea, gracias al desarrollo acelerado de sistemas de inteligencia artificial como el

traductor de Google. Este conocido traductor es uno de los muchos sistemas de inteligencia artificial dedicados al procesamiento del lenguaje natural. Básicamente, emplea un enfoque de aprendizaje basado en enormes cantidades de datos, en lugar de aprender o aplicar reglas gramaticales específicas de cada idioma.

En términos sencillos, se generan vastas bases de datos de traducciones comunes, respaldadas por extensos documentos traducidos entre idiomas, incluidos aquellos proporcionados por la Organización de las Naciones Unidas (ONU). Para finales de 2016, el traductor de Google casi igualó el trabajo de 500 traductores humanos expertos. Ahora, analicemos con más detalle cómo funciona este sistema de inteligencia artificial. La evaluación del traductor de Google se realizó utilizando una escala del 0 al 6 para medir la fluidez de las traducciones de 500 frases tomadas de Wikipedia o noticias. En el caso de las traducciones del inglés al español, el nuevo sistema de Google obtuvo una puntuación promedio de 5,43, muy cercana al 5,55 que lograron los 500 traductores humanos. Si hace tiempo que no has probado el traductor, es probable que recuerdes que solía cometer muchos errores. En las pruebas realizadas, los humanos evaluaron el nuevo sistema entre un 64% y un 87% mejor que su versión anterior.

En lugar de aprender conceptos o gramática, los algoritmos crean sus propias maneras de descomponer el texto en fragmentos más pequeños, que a menudo parecen sin sentido y no corresponden a los fonemas hablados. Además, el sistema de inteligencia artificial trabaja a una velocidad impresionante. Como señala uno de sus desarrolladores: “Puede ser sorprendente, pero lo hemos probado en numerosos contextos y simplemente funciona”. Para entender este fenómeno, es necesario considerar brevemente el concepto de inteligencia humana con el que trabajan los especialistas en ciencias cognitivas.

Entre las diversas definiciones de inteligencia, lo que las une es la capacidad de procesar información para resolver problemas y alcanzar objetivos. La idea de inteligencia está estrechamente vinculada al procesamiento de información. Es crucial entender que nos referimos a la información en un sentido amplio, tal como lo abordan las ciencias cognitivas, que examinan cómo la información del entorno se codifica, organiza, selecciona, almacena y recupera a través de los sistemas sensoriales y perceptivos.

La inteligencia humana se asocia con varias capacidades cognitivas relativamente independientes, que a menudo se agrupan en “perfiles de inteligencia” o “inteligencias múltiples”, como la inteligencia social, lingüística (o musical), lógico-matemática, interpersonal, intrapersonal o emocional, e inteligencia fluida, entre otras. En esencia, el cerebro regula nuestra capacidad para

procesar la información que proviene del entorno y de nuestro propio cuerpo, información que utilizamos para evaluar y decidir nuestras futuras acciones. (Coca Vila, 2023).

En este contexto, el proceso de toma de decisiones y evaluación implica seleccionar, filtrar y organizar la información disponible. A partir de la inteligencia humana, se han generado diversas innovaciones tecnológicas. En particular, aquí nos enfocamos en el procesamiento de información para resolver problemas y tomar decisiones mediante máquinas que utilizan algoritmos inteligentes. La inteligencia artificial (IA) se basa en estos algoritmos avanzados o en algoritmos de aprendizaje que sirven para identificar tendencias económicas, predecir delitos, diagnosticar enfermedades, anticipar comportamientos digitales, entre otros. Un algoritmo puede definirse como un conjunto específico de instrucciones o reglas, o como una secuencia metódica de pasos para realizar cálculos, resolver problemas y tomar decisiones.

Es la fórmula utilizada para realizar un cálculo. En las últimas décadas, se han empleado diversos métodos para desarrollar algoritmos mediante el análisis de grandes volúmenes de datos e información, tales como redes neuronales, algoritmos genéticos y aprendizaje por refuerzo, entre otros. El objetivo de aplicar IA es permitir que las tecnologías hagan que los sistemas computacionales sean: autónomos, adaptables, capaces de negociar de manera inteligente, cooperativos, y capaces de operar con mínima intervención humana, entre otras características.

Esto implica el uso de técnicas basadas en el reconocimiento de patrones para resolver problemas, alcanzar objetivos y optimizar el procesamiento de información. A continuación, exploraremos otro ejemplo para comprender mejor cómo funcionan los sistemas más exitosos de IA. En el año 2011, la inteligencia artificial que desarrolló IBM llamada “Watson” compitió contra los expertos humanos en un célebre juego llamado *Jeopardy*. Este concurso de televisión de Estados Unidos basado en responder preguntas sobre numerosos temas como historia, idiomas, literatura, entre otros, reside en que cada uno de los tres concursantes elige uno de los paneles del tablero de juego que, al ser descubierto, revela una pista en forma de respuesta. Los concursantes tienen que dar sus respuestas en forma de una pregunta.

El interés por la inteligencia artificial es creciente, pues ofrece soluciones a diversas necesidades, incluso en lo jurídico. Sin embargo, el mismo, muchas veces es omiso en los peligros que acarrearán sus consecuencias. Tradicionalmente, el derecho ha sido una práctica intrínsecamente humana siendo el juez un actor fundamental en la procuración de justicia. La ciencia jurídica ha estudiado y tratado de definir cómo debe pensar un juez para que sus decisiones aparejen el derecho de manera correcta. Sin embargo, la incorporación de la inteligencia artificial podría propiciar un cambio radical en el funcionamiento de los tribunales públicos. La inteligencia artificial trae consigo

inmensos peligros y retos ante los derechos fundamentales de los individuos. Su uso indiscriminado podría traer como resultado sentencias arbitrarias o ilegítimas y, en el peor de los casos, un estancamiento del derecho. Pese a que sería una calamidad de enorme perjuicio, una imprudente decisión que se tomase al efecto de rechazar la inteligencia artificial, por el arraigo fenómeno social que representa en más de un área del desempeño humano y en el proceso penal, importa valorar con razón dicho fin.

Inteligencia Artificial al Servicio de los Derechos de Acceso.

Este artículo tratará de cómo la aplicación masiva y sistemática de algoritmos que se han desarrollado, como es el caso del algoritmo que ha creado la IBM Watson, incide en el proceso penal. La aplicación aiosa de la tecnología referida podría ser justificada por la premura que se busca en la rapidez en la administración de justicia y la eficiencia del proceso, sin embargo, la velocidad en la emisión de las sentencias podría comprometer la calidad y certeza en la dictada. (Zaptest). Por Inteligencia Artificial se entiende toda una gama de sistemas informáticos que realizan actividades que normalmente requieren la inteligencia humana, tales como aprender, pensar, razonar, decidir y resolver. En el campo del derecho Penal, la inteligencia artificial se utiliza en dos áreas fundamentales: Inteligencia Artificial policíaca IAP: Aquí se incluye una serie de herramientas dedicadas a la prevención e investigación de crímenes. Como ejemplo de las mismas podemos señalar los sistemas de análisis predictivo, que detectan los patrones de los delitos y son capaces de prever delitos futuros. Inteligencia Artificial Judicial IA-J: Estas herramientas operan en el área de la fase judicial con el objeto de determinar la valoración de los riesgos (predictiva), de analizar las pruebas y ayudar a la toma de decisiones. En este caso se tienen herramientas para valorar al efecto el riesgo, así como para realizar análisis de volumetrías más allá de las pruebas (grandes volúmenes de información procesal). En el campo de la inteligencia artificial puede valorarse su uso en estas diversas funciones: Policía predictiva: que utiliza algoritmos para el análisis de datos y prevé los delitos antes de que ocurran. Análisis de pruebas: herramientas que atacan el objeto de las pruebas para ser utilizadas por los Jueces en el sentido de valorar grandiosos volúmenes de las mismas y poder emitir decisiones judiciales. Valoración de riesgos: sistemas que, evaluando las probabilidades de reincidencia, ayudan a la determinación de la libertad condicional y otras disposiciones.

Uno de los desafíos principales es garantizar que el uso de la IA en el sistema penal no transgreda los derechos fundamentales de los usuarios. Esto incluye; Privacidad. Los sistemas de IA recogen y analizan volúmenes significativos de datos. Y esto puede significar perder la privacidad de las personas. (Chamorro, 2020) La opacidad de los algoritmos de la IA puede dificultar el entender

cómo se toman las decisiones. Esto afecta el derecho a tener un juicio justo. Discriminación. Los algoritmos pueden ahondar en la discriminación que ya existe en los datos; y pueden tomar decisiones discriminatorias, basadas en la raza, el género o el estado socioeconómico. El uso de la IA en el derecho penal presenta la pregunta de la responsabilidad y de la rendición de cuentas: Responsabilidad Penal. ¿Quién es responsable?, si un sistema de IA comete un error y conduce a una condena injusta? La imputación de la responsabilidad penal es un área que se tiene que desarrollar. Errores de IA. Los sistemas de IA pueden tener errores o confusiones que afectan a la justicia. Determinar la responsabilidad en estos casos es complicado. La inserción de la IA en el sistema penal exige que haya una correcta regulación para garantizar su uso ético y eficaz: Normativas. Es muy importante la creación de marcos jurídicos y normativas, que den una guía sobre el uso de la IA en el derecho penal; garantizando el respeto a los derechos humanos y la igualdad. Control y supervisión. Es necesaria una supervisión y control fidedignos, para prevenir abusos y que los sistemas de IA son justos y transparentes. La IA tiene la posibilidad de mejorarse la eficacia del sistema penal. Procesamiento de datos. Los sistemas de IA pueden tratar y analizar, de forma inmediata, grandes volúmenes de datos; mejorando así la celeridad en la tramitación judicial. Reducción de la carga del trabajo. Otorgar la posibilidad de automatizar tareas rutinarias y ayudar a los jueces y abogados en la revisión de la prueba puede reducir el número de trabajo. La IA puede mejorar la precisión de los resultados en la judicatura. Evaluación de riesgos. Existen herramientas de IA que pueden aportar evaluaciones más certeras de los riesgos de reincidencia, contribuyendo así a hacer una decisión más informada de las medidas cautelares y de la libertad provisional. Análisis predictivo. También podría la IA determinar patrones o tendencias en el delito, ayudando a prevenir el delito antes de que se produzca.

Tabla 7.
Riesgos críticos de la IA en justicia penal

Riesgo	Ejemplo	Impacto
Cajas negras	Redes neuronales profundas	Falta de explicabilidad
Sesgo algorítmico	Caso COMPAS	Violación de igualdad
Vigilancia excesiva	IAP basada en metadatos	Afecta privacidad
Autonomía machine	Decisiones sin control humano	Riesgo sistémico
Manipulación comercial	Secreto industrial	Falta de control público

Nota: Los riesgos señalados evidencian los desafíos técnicos, éticos y jurídicos que deben abordarse para garantizar un uso responsable y transparente de la IA en el sistema de justicia penal.

A comienzos de este año, más de dos mil quinientos expertos (entre los que se encuentra el Dr. Stephen Hawking) establecieron el siguiente principio: “Los riesgos que presentan los sistemas de IA, los riesgos catastróficos y existenciales sobre todo, deberían estar sujetos a los esfuerzos de

planificación y mitigación que correspondan, considerando la magnitud del impacto que se espera. Y más allá, deberían estar sometidos a estrictas medidas de seguridad y control”. Hoy por hoy, hay varios problemas para asegurar la compatibilidad en el desarrollo de la inteligencia artificial con el derecho interno de los Estados y con el derecho internacional vigente. Se utilizan algoritmos inteligentes para captar todos nuestros datos, para recomendar qué buscar, a dónde ir, que hacer, cómo llegar antes a algún punto, para realizar diagnósticos médicos, para la prevención de las enfermedades, etcétera. Cada uno de estos aspectos exige que se preste atención a algunos detalles.

En primer lugar, es fundamental conocer la estructura de esta nueva tecnología. No se puede pensar en la adecuada regulación, desconociendo la dinámica del objeto que se quiere regular. Algo análogo sucede con respecto a los sistemas de leyes que regulan los alimentos, los medicamentos, etcétera. Aquí, como los sistemas de la IA son de crecimiento exponencial, es imprescindible estar en constante evolución respecto de los nuevos métodos que se están utilizando. ((Farfán Intriago)

En segundo lugar, lo esencial a examinar, es el hecho de analizar ciertos sectores y derechos en forma particularizada. Es otro el supuesto en que los sistemas de la IA se refieren a la recomendación de música etcétera, y se encargan de la administración de los gustos musicales de nuestra cuenta en Spotify, (o cuáles son los videos que pueden interesarnos en YouTube) , a que el supuesto se refiere a la ciencia en que ciertos algoritmos inteligentes se encargan de predecir si voy a sufrir de una enfermedad, o si corresponde otorgar la libertad condicional a una persona detenida. En tercer lugar, cuando se trata de derechos fundamentales, es esencial considerar un aspecto trascendente de todos los sistemas de IA más sofisticados que hoy se utilizan (Watson de IBM, Alexa, Quid, Siri, entre muchos otros).

Se trata de cajas negras auténticas. Esto es, se trata de que los algoritmos no pueden ofrecer una explicación precisa respecto de cómo llegan a un determinado resultado. O sea, no puede establecerse cómo el sistema de la IA pondera los datos, y la información que procesa. Por lo que sucede que se usa el término “cajas negras”. Se llama a una herramienta computacional sistema de caja negra, en donde uno entiende el significado de los datos que introduce y de los resultado que obtiene, pero nada comprende del procedimiento subyacente de procesamiento. Aquí el código es ininteligible porque el programa “evoluciona” y el ser humano no puede entender el proceso que siguió para resolver un programa determinado. – (Cordero, 2023) Cuarta razón, y a tenor de lo anterior, es absolutamente necesario el afianzarnos en los principios de igualdad y de no discriminación cuando de predicciones de las inteligentes artificiales se trate frente a derechos fundamentales. Por ejemplo, ciertas IA predictivas que se utilizan en USA 24, se basan en un código fuente y tienen en cuenta distinciones en la raza, género, etc. etc., y se producen así casos

inadmisibles de discriminación estructural algorítmica. Por ejemplo. En el caso “State vs. Loomis” el apelante sostuvo que el algoritmo inteligente hacía un uso incorrecto de las valoraciones de género. Veamos el asunto con detenimiento. La agencia de noticias independiente Pro Publica hizo una investigación sobre la fiabilidad o no del pronóstico de la reincidencia a través de algoritmos inteligentes en el campo delictivo. Básicamente se determinó el funcionamiento de COMPAS. Se examinaron las puntuaciones de riesgo dadas a más de 7.000 personas detenidas en el Condado de Broward en Florida, entre los años de 2013 y 2014, y se observó cuántas de ellas fueron acusadas después nuevamente de delincuencia durante los próximos dos años. La puntuación resultó ser enormemente poco fiable para la predicción de los delitos violentos, ya que sólo el 20 % de las personas predichas que habían de cometer delitos violentos lo hicieron. En cambio, en cuanto se consideraban todos los delitos, incluyendo los delitos menores -tales como conducir permisos de circulación caducados, la predicción resultó más fiable. En este caso, el porcentaje de acierto en quienes efectivamente reincidían fue del 61 %. Pero además se notaba que había mayor grado de predicción de reincidencia en los delincuentes afroamericanos y mayor cantidad de falsos positivos (es decir, de equivocada predicción de reincidencia) en estos delincuentes. A comienzos de este año, más de dos mil quinientos expertos (entre los que se encuentra el Dr. Stephen Hawking) establecieron el siguiente principio: “Los riesgos que presentan los sistemas de IA, los riesgos catastróficos y existenciales sobre todo, deberían estar sujetos a los esfuerzos de planificación y mitigación que correspondan, considerando la magnitud del impacto que se espera. Y más allá, deberían estar sometidos a estrictas medidas de seguridad y control”. Hoy por hoy, hay varios problemas para asegurar la compatibilidad en el desarrollo de la inteligencia artificial con el derecho interno de los Estados y con el derecho internacional vigente. Se utilizan algoritmos inteligentes para captar todos nuestros datos, para recomendar qué buscar, a dónde ir, que hacer, cómo llegar antes a algún punto, para realizar diagnósticos médicos, para la prevención de las enfermedades, etcétera. Cada uno de estos aspectos exige que se preste atención a algunos detalles.

En primer lugar, es fundamental conocer la estructura de esta nueva tecnología. No se puede pensar en la adecuada regulación, desconociendo la dinámica del objeto que se quiere regular. Algo análogo sucede con respecto a los sistemas de leyes que regulan los alimentos, los medicamentos, etcétera. Aquí, como los sistemas de la IA son de crecimiento exponencial, es imprescindible estar en constante evolución respecto de los nuevos métodos que se están utilizando. ((Farfán Intriago)

En segundo lugar, lo esencial a examinar, es el hecho de analizar ciertos sectores y derechos en forma particularizada. Es otro el supuesto en que los sistemas de la IA se refieren a la recomendación de música etcétera, y se encargan de la administración de los gustos musicales de nuestra cuenta en Spotify, (o cuáles son los videos que pueden interesarnos en YouTube) , a que el

supuesto se refiere a la ciencia en que ciertos algoritmos inteligentes se encargan de predecir si voy a sufrir de una enfermedad, o si corresponde otorgar la libertad condicional a una persona detenida. En tercer lugar, cuando se trata de derechos fundamentales, es esencial considerar un aspecto trascendente de todos los sistemas de IA más sofisticados que hoy se utilizan (Watson de IBM, Alexa, Quid, Siri, entre muchos otros).

Se trata de auténticas cajas negras. Es decir, en el sentido de que los algoritmos, no pueden dar una explicación exacta de cómo llegan a un resultado determinado. O sea, no puede saberse cómo el sistema de la IA pondera los datos, y la información que es procesada. Y es así que se emplea el término de “cajas negras”. Cuando se da a la herramienta computacional el nombre de sistema de caja negra, en donde se comprende el sentido de los datos que se le dan, y el sentido de los resultados que se obtienen, pero nunca se entiende el sentido del procedimiento de procesamiento subyacente. En este caso el código es ininteligible, porque el programa “evoluciona” y el ser humano nunca comprende, por lo tanto, el procedimiento seguido para la solución de un programa determinado. – (Cordero, 2023) Cuarta razón, y a tenor de lo anterior, es absolutamente necesario el afianzarnos en los principios de igualdad y de no discriminación, cuando se trata de predicciones de las inteligentes artificiales frente a derechos fundamentales. Por ejemplo, ciertas IA predictivas que se usan en USA 24, que se basan en un código fuente y consideran distinciones en la raza, género, etcétera, etcétera, se producen así casos inadmisibles de discriminación estructural algorítmica. Por ejemplo. En el caso del “State vs. Loomis” el apelante sostuvo que el algoritmo inteligente hacía un uso incorrecto de las valoraciones de género. Disentimos del asunto con seriedad. La agencia de noticias independiente Pro Publica hizo una investigación sobre si el pronóstico de la reincidencia a través del uso de algoritmos inteligentes en el campo delictivo era o no fiable. Básicamente se examinó el funcionamiento del COMPAS. Se examinaron las puntuaciones de riesgo que tuvieron más de 7.000 personas detenidas en el Condado de Broward en Florida, entre los años 2013 y 2014 y se vio cuáles de ellas después fueron nuevamente acusadas de delincuencia, durante los próximos dos años. La puntuación resultó ser enormemente poco fiable para la predicción de los delitos violentos, ya que mediando solo el 20 % de las personas predichas que debían cometer delitos violentos, lo hicieron. En cambio, sí se considera todos los delitos, incluyendo los hasta delictivos menores – tales como conducir permisos de circulación caducados, resultó más fiable la predicción. En este caso el porcentaje de efectivamente reincidentes, fue del 61 % - Pero se notaba también, que había mayor grado de predicción de reincidencia en los delincuentes afroamericanos y mayor tasa de falsos positivos (Es decir, equivocada predicción de reincidencia) de dichos delincuentes. Incluso, en el mejor estilo del oráculo grego Calcante se llegó a la conclusión de que sus desarrolladores de COMPAS (empresa

Northpointe) no hacen públicos cuáles son los cálculos en virtud de los cuales se llegan a los puntajes de riesgo de los inculpados, por lo que no es posible que los inculpados ni el público en general adviertan qué puede estar provocando la disparidad. (Díaz, 2020). Hasta estos “oráculos artificiales” parecen ser incapaces de ofrecer una explicación inteligible, en un lenguaje humano, sobre cómo es que se ponderan o pesan los factores que llegan a los porcentajes. Figúrese el lector que está discutiendo con alguien si le adeuda o no la suma de veinte mil pesos (\$ 20.000), por lo que ante el problema mediando una discusión acude a la justicia. Supóngase que el juez decide que no se le adeuda nada, pues examinó diversos factores. Pero no le dice cómo los examino. Sin duda, existiríamos ante un típico caso de sentencia arbitraria. Por eso es que, si se emplean algoritmos inteligentes como medios para decidir en la justicia penal acerca de la libertad condicional de los inculpados, nuestro sistema convencional y constitucional prohíbe ya emplear un sistema de este carácter. En efecto, no sólo se trata de que el sistema no se funde en distinciones de raza, sexo etc., sino que además resulta necesario que la IA debe ser capaz de explicar en un lenguaje inteligible para los hombres, cuáles son los factores que se basan y cómo pondera los elementos que las soportan. Por ello, hoy es algo imposible de aplicar en estos campos la inteligencia artificial. Y de allí la importancia suprema del movimiento que se denomina “Inteligencia Artificial Explicable”. De otro modo, será difícil que ante sistemas tan opacos se admita el desarrollo masivo de vehículos autónomos, “oráculos artificiales” que, en materia de salud, seguridad y en todo lo que respecta a armas de guerra pueden predecir los estados. En quinto lugar, quienes se dedican al desarrollo de IA suelen estar amparándose en el secreto comercial y en los derechos patentados. Y si bien esto viene a ser en principio razonable, al menos lo es en la medida de que se trata de sistemas de IA que tienen que ver con factores comerciales (ventas online, publicidad, marketing, etc.), no pueden ser opuestos en el caso de que se trate de cuestiones que tienen que ver con la dignidad del hombre. En tal aspecto, cobra especial relieve lo que dice el Art. 13.2 inc.) de la Convención Americana de los Derechos del Hombre, cuando dice que el derecho a la libertad de expresión no puede ser sujeto a censura previa, sino a responsabilidades ulteriores, las que deben estar expresamente fijadas por la ley y ser necesarias para asegurar: a. el respeto a los derechos o a la reputación de los demás.

Como no podemos continuar siempre desmenuzando las cuestiones que implica el desarrollo de la IA, estas breves muestras evidencian la complejidad y dificultad para abordar esta cuestión innovativa. Por ello, es fundamental ponerla en la agenda, pensar en una cooperación internacional y, a la vez, crear espacios normativos apropiados. Esto implica, también, consagrar principios rectores que se le apliquen a los sistemas de inteligencia artificial que sean compatibles con nuestro modelo de derechos humanos, es decir, que se dé una posibilidad de desarrollo de la IA compatible con el Estado constitucional y con el Derecho internacional de derechos humanos. (Ávila Zea). El

“modelo de derechos humanos” se concreta en un paradigma protector que surge de los pactos internacionales, y que tiene como base en la dignidad humana: así el centro del sistema se ubica en la igualdad y en lo no alienable o indisponible. Existe una conexión directa entre estos derechos, la dignidad humana, la paz, la protección de las minorías, de los más débiles o poderosos. Se trata de un esquema por el que se obliga a los Estados y a la comunidad internacional a garantizar la eficacia de derechos, principios y reglas que están consagrados en las constituciones, en los pactos internacionales y en las leyes internas. Pero un enfoque de derecho humanos vinculado a las nuevas tecnologías implica haber aceptado un punto prima: la innovación inclusiva para desarrollo sostenible. Sobre esta plataforma para que el desarrollo de la IA sea compatible con “modelo de derechos humanos” es necesario impulsar una regulación que incorpore toda una serie de principios que están muy relacionados a tres categorías incipientes que, por una cuestión de espacio, se ampliará en las publicaciones futuras, dignidad algorítmica, La identidad algorítmica y la vulnerabilidad algorítmica. Todas ellas son un derivado de la dignidad digital (que a su vez está compuesta por la identidad digital) de las personas humanas en el mundo digital. Se trata, por cierto, de robustecer el sistema de protección, siendo ello posible a través de la inclusión en el bloque de la juridicidad de una serie de principios generales que dejan una regulación de la misma, veamos. Prevención/Precaución.

Estos principios representan dos funciones distintas ateniéndose a un solo denominador que parece ser la necesidad de prevención frente a la producción de un daño. En una síntesis radical, actúan sobre distintos tipos de daño que puede producirse. Al riesgo potencial, la precaución. Al riesgo ya verificado corresponde la prevención. (Wilson, 2018). El principio precautorio que hay en la AI (de un modo análogo a lo que sucede en el derecho ambiental), está ligado a la ausencia de certeza o certeza absoluta o total, acerca de la ausencia de riesgos que genera.

Cuando se pretenda utilizar inteligencia artificial y que los derechos fundamentales de las personas (salud, libertad, igualdad y no discriminación, seguridad) estén afectados no podrá utilizarse inteligencia artificial de ninguna manera y en caso que se presenten las siguientes situaciones: i) código fuente cerrado o existencia de un sistema en el que uno conoce la información que se introduce o los resultados, pero ignorando el procedimiento subyacente o sea el “caja negra”; II) ausencia de trazabilidad algorítmica; III) no se permite garantizar la posibilidad de un “botón de apagado” o un “mecanismo seguro de contención” que se conoce de la inteligencia artificial; IV) cuando se advierte en cualquiera de las fases (diseño, desarrollo o utilización) que estas se basan en diferenciaciones que violan el principio de igualdad y no discriminación. Ahí esto operaría como una especie de “categoría sospechosa algorítmica”. (Echeverría, 2021).

Autodeterminación algorítmica

La autodeterminación es un derecho fundamental, nacido a partir de la dignidad de la persona. Consiste en poder garantizar el “libre desarrollo de la personalidad”, fundamentalmente también el poder mente de la autodeterminación informativa, que se orienta a garantizar el derecho de elección, esto sienta las bases respecto de la libertad de información, el “derecho a saber”, al “conocimiento”, a la “auto regulación” de la información. Sobre esta base y por supuesto en los Estados y a nivel internacional, responsablemente deben invertirse, montarse y hacerse los máximos esfuerzos de toda índole, para que se pueda dar la autodeterminación humana en relación a lo que hace al uso de los algoritmos inteligentes. Si bien la IA va mediando la relación entre los datos/información y la decisión de la persona, es indispensable y está en juego la tutela de tales derechos, por lo que además debe promoverse el respeto a principios como los de necesidad, finalidad, proporcionalidad y pertenencia respecto de los datos personales. Transparencia algorítmica, e imparcialidad del validador. Cuando se pretende hacer uso de sistemas de IA en temas de salud, libertad, seguridad, u otras materias que tienen que ver con derechos fundamentales, el diseño, desarrollo y uso de la inteligencia artificial debe garantizar que no habrá allí “cajas negras”, o fallas de arquitectura, respecto los perjuicios que pueda acarrear. Por lo tanto, la inteligencia artificial debe ser transparente en sus decisiones, lo que resulta que en ella se podrá inferir o deducir una “explicación entendible” respecto de los criterios que hubiese seguido para llegar a determinada conclusión, recomendación o resultado. Esta problemática tiene por un lado dos grandes caras. Por un lado, resulta pertinente abocarse a lo que se llama los secretos comerciales, que protegen a la información confidencial comercial, que otorga ventajas competitivas a las empresas. Ello abarca a los secretos industriales o de producción y a los secretos comerciales. La utilización no autorizada de dicha información por personas distintas del titular, se considera competencia desleal y vulneración del secreto comercial. En virtud del sistema jurídico y del país, la protección de los secretos comerciales forma parte de la idea general de la protección frente a competencia desleal o tiene base en ciertas prescripciones o en veredictos de tribunales respecto de la protección de la información confidencial. Por otro lado, y a pesar de que el desarrollador tenga voluntad en “dar a conocer” el sistema (el código fuente) en los sistemas de IA más avanzados no se da forma técnica de conocer la forma en que los algoritmos progresivamente (la trazabilidad) llegan al resultado, decisión o predicción. Esto se da generalmente en uno de los métodos de los más utilizados, como son las redes neuronales artificiales. Ahora bien, si bien hay que tener en cuenta, en el hecho de las cajas negras, que los sistemas de IA están contruidos para maximizar resultados, así como para la optimización del procesamiento de la información y de los datos. Pero cuando hay en los derechos fundamentales de la persona (la salud, la vida, la libertad, la privacidad, la libertad de expresión,

etc.) es fundamental que los resultados intermedios del sistema tengan que ser verificados. (el, 2022). Lo que significa que el razonamiento o las estructuras de razonamientos que hay que dar hasta el llegar a las decisiones o a la predicción, tienen que ser sometidos a un proceso de tres grandes fases: 1) verificación, 2) validación y 3) evaluación Y aquí es donde entra la importancia en la garantía de la calidad y de la transparencia de los procesos algorítmicos. La idea básica es conseguir que los sistemas de procesamiento de la información y de datos que llevan a cabo los sistemas de IA, cumplan con unos procesos de calidad, para que los resultados, sean los esperados y se obtengan y no a costa de lo que sea. La primera fase de la que antes hablábamos, está relacionada con la arquitectura de la AI (verificación). Consistir en garantizar unos mínimos, unos estándares o unos principios que como son la consistencia, la completitud, la corrección y no ser redundante. Entre otros. Uno de los métodos, es conseguir que sean expertos humanos y debidamente cualificados los que puedan simular el proceso, en cuanto a lo posible, para la detección de las discrepancias. Pero aquí aparece un factor trascendental, en el caso de algunos sistemas de IA que afectan a los derechos, que deberán tener importancia en cuanto a la producción en los derechos fundamentales de la persona. Aquellos que diseñan, enseñan o desarrollan los algoritmos inteligentes, no pueden intervenir en el proceso de validación. A esto fenómeno le llamaremos principio de imparcialidad del validador. Incluso es necesario que en el proceso se intervenga en su caso por parte de las autoridades públicas y se le obligue legalmente a ello. Lo que no significa que todos los sistemas de IA tengan que ser objeto de este proceso de verificación y validez. Máximo acceso. Derecho de acceso a la información algorítmica. La autodeterminación es un derecho fundamental que deriva de la dignidad de la persona. Consiste en garantizar el “libre desarrollo de la personalidad” y con ello reconocer la autodeterminación informativa, que se orienta a garantizar el derecho de elección -en relación a la libertad de información-, el “derecho a saber”, al “conocimiento”, a la “auto regulación” de la información. Sobre esta base los Estados y la comunidad internacional, responsablemente, deben invertir, contemplar y poner los máximos esfuerzos de toda índole, para que pueda darse la autodeterminación humana frente al uso de algoritmos inteligentes.

Si bien la IA va mediando en la relación entre los datos/información y la decisión de la persona, es indispensable tutelar sus derechos a partir de promover el respeto a los principios de necesidad, finalidad, proporcionalidad y pertenencia de los datos personales. Transparencia algorítmica y principio de imparcialidad del validador. Cuando se pretende utilizar sistemas de IA en el área de salud, libertad, seguridad, u otros derechos fundamentales, el diseño, desarrollo y utilización de la inteligencia artificial debe garantizar que no se configurará “cajas negras”, o que verifique fallas de arquitectura, frente a los perjuicios que pueda causar. Por lo tanto, la inteligencia artificial tiene que

ser transparente en sus decisiones, lo que implica que se puede inferir o deducir una “explicación entendible” acerca de los criterios que tiene para llegar a determinada conclusión, recomendación o resultado.

Esta cuestión tiene dos grandes caras. En primer lugar, es relevante considerar el llamado secreto comercial, que ampara a la información comercial confidencial que les da a las empresas ventajas competitivas. Esto comprende a los secretos industriales o de fabricación y a los secretos comerciales. La utilización no autorizada de dicha información por personas distintas al titular, se considera competencia desleal y vulneración del secreto comercial. En virtud del sistema jurídico y del país, la protección de los secretos comerciales forma parte de la idea general de la protección frente a competencia desleal o se fundamenta en determinadas prescripciones o en veredictos de los tribunales en cuanto a la protección de la información confidencial.

En segundo lugar, aun cuando el desarrollador tenga la intención de “dar a conocer” el sistema (el código fuente), los sistemas más avanzados de la IA no tienen forma técnica de saber la forma progresiva (la trazabilidad) en que los algoritmos llegan hasta el resultado, decisión o predicción. Esto ocurre en uno de los sistemas más utilizados que son las redes neuronales artificiales. Pero en el tema de las back boxes, es importante insistir en el tema que es que los sistemas de IA están constituidos para maximizar resultados y para optimizar el tratamiento de la información y de los datos. Pero cuando hay en juego derechos fundamentales de la persona (la salud, la vida, la libertad, la intimidad, la libertad de expresión, etc.) se hace imprescindible, que los resultados intermedios del sistema, sean validados. (el, 2022). Esto significa que el razonamiento o las estructuras de razonamientos que hay que dar hasta llegar a las decisiones o a la predicción, deberán ser sometidas a un proceso de tres fases grandes, 1) verificación 2) validación 3) evaluación. Y aquí es donde entra la importancia de la garantía de la calidad y de las transparencias de los procesos algorítmicos. La idea básica es que los sistemas de proceso de información y de datos que hacen los sistemas de IA se sometan a ciertos tratamientos de calidad para que los resultados sean los que se esperaban y sean y se consigan no a costa de lo que sea. La primera fase, de la que antes nos referíamos, está referida a la arquitectura de la IA (verificación). Se trata de asegurar ciertos estándares o principios que son los de consistencia, de completud, de corrección, de no redundancia. Entre otros. Un sistema es conseguir que sean los expertos humanos, debidamente cualificados, los que puedan simular el proceso, en la medida de lo posible, y la detección, si la hubiera, de las discrepancias que pudieran darse. Pero aquí se da un factor trascendental, en el caso de que ciertos sistemas de IA afecten a los derechos, que habrán de tener importante producción en los derechos fundamentales de la persona. Quienes constituya diseñan, enseñan, o desarrollan los algoritmos inteligentes, no podrán intervenir en el proceso de validación. A este fenómeno es al que lo llamaremos principio

de imparcialidad del validador. Pero incluso, es necesario que en el proceso participen las autoridades públicas en él y que por Ley se les obligue a ello. Esto no significa que tuviese que pasar por el proceso de verificación y de validación todos los sistemas de IA. Máximo acceso. Derecho de acceso a la información algorítmica.

Derecho a la explicación y a la impugnación de decisiones automatizadas

La autodeterminación algorítmica no se agota en la transparencia del modelo o en el acceso formal a la información sobre su funcionamiento, sino que precisa también de garantías procedimentales efectivas para la persona que se ve afectada por una decisión automatizada o asistida significativamente por IA. Por ello el derecho a la explicación se encuentra especialmente reforzado en la medida que lo entendemos como la efectiva posibilidad de obtener una explicación comprensible, suficiente y comprobable por las razones que fundamentan una recomendación, calificación, perfilamiento o resultado sobre los que incide en derechos o intereses legítimos. Por ello la misma tendrá que ser proporcional a la influencia de la decisión algorítmica: a mayor interferencia de la decisión sobre derechos fundamentales (salud, libertad, seguridad, acceso a prestaciones, trabajo, justicia), mayor será el estándar de claridad, detalle y trazabilidad exigibles. Complementario a lo anterior la autodeterminación algorítmica lleva consigo el reconocimiento de derechos de impugnación a las decisiones automatizadas, garantizando (i) la posibilidad de una significativa revisión humana por parte de un funcionario o evaluador independiente competente capaz de corregir el resultado, (ii) existencia de canales de reclamo ágiles y debidamente motivados y (iii) posibilidad de prueba y rectificación de datos y revisión del modelo o exclusión de variables sensibles o indefendibles.

Estas garantías se encuentran directamente vinculadas al debido proceso, al derecho de defensa y a la tutela efectiva, evitando que la persona se vea aprisionada por una decisión técnica inaccesible por su complejidad o el argumento de secreto comercial. En escenarios estatales, especialmente en ámbitos como la justicia digital, la seguridad o la atención de los servicios públicos, este subtema adquiere un carácter estructural: no basta con presentar un argumento sobre la publicidad o la eficiencia de la tecnología utilizada, sino que es imprescindible asegurar que toda decisión algorítmica relevante es auditada, motivada y accesible de forma recursiva, existiendo responsabilidades definidas respecto a la entidad que utiliza la tecnología, incluso en ámbitos de prestación por parte de terceros.



FUNDAMENTOS LEGALES Y ETICOS DE LA INTELIGENCIA ARTIFICIAL EN EL DERECHO PENAL

Principios legales aplicables

La inteligencia artificial (IA) ha aflorado como un factor transformador en un gran número de campos del conocimiento y de la actividad humana. Lo ha hecho en una manera especialmente significativa en el ámbito del derecho penal. La IA en el derecho penal plantea a su vez una serie de desafíos y de oportunidades que exigen una profunda reflexión en torno a sus implicaciones jurídicas y éticas. La presente introducción examina estos temas, pero también otros muchos que tocan *both* las posibilidades, en definitiva, y la problemática suscitada por la introducción en el derecho penal de la IA en el derecho penal. La IA se puede entender, aquí, como el amasijo de tecnologías que genera que las máquinas aprendan, razonen y decidan. En el ámbito del derecho penal puede observarse la utilización de la IA en diversas vertientes. Desde sistemas de predicción de la criminalidad, hasta sistemas de análisis forense, la IA puede neutralizar la ineficacia y la impredecibilidad presente en la investigación y el enjuiciamiento penal, superando los umbrales de eficacia y previsibilidad que otorgan los métodos tradicionales. Pero tras esta promesa se ocultan una serie de desafíos que son precisos de ser analizados. En primer lugar, las herramientas basadas en IA parecen permitir un inusitado potencial de análisis de grandes volúmenes de data, de patrones, como también de comportamientos criminales. Esta posibilidad, sin duda, puede transformar la forma en que los cuerpos de seguridad abordan la prevención del delito y la resolución de los delitos. Sin embargo, la aparición de estas nuevas herramientas plantea, asimismo, cuestiones sobre la asiduidad y justicia que permiten. Pero también_-como se dice en IQ 713- en Ecuador la IA avanza a pasos agigantados en múltiples sectores, entre ellos el derecho penal. En este caso, la IA se carga de implicaciones -legales, éticas- que son objeto de exhaustivo análisis. La

introducción de la IA en el derecho penal también ofrece desafíos y oportunidades que han de ser exteriorizados de forma concreta en los aspectos relacionados con su introducción en el derecho penal. El Derecho ecuatoriano se enfrenta en este caso al desafío de adaptarse a las nuevas tecnologías y también conseguir la defensa de los derechos fundamentales y de la justicia que es consustancial al sistema jurídico. Las disquisiciones que ofrece este tema a la legislación ecuatoriana son infinitas, pero tales disquisiciones son expuestas, en el presente trabajo, en el enfoque que sobre ello ofrece la legislación penal ecuatoriana. Este análisis, si tampoco en este caso- ofrece una serie de desafíos y oportunidades que se verán analizados a partir de las diferentes perspectivas que acerca de la IA se ofrecen. (Ávila Zea). Un aspecto central en la conversación sobre los principios jurídicos aplicables a la inteligencia artificial en el ámbito del derecho penal es la necesidad de darla la debida transparencia y aplicabilidad a los sistemas de inteligencia artificial. La opacidad propia de muchos sistemas de inteligencia artificial, sobre todo cuando están contruidos a partir de sistemas de aprendizaje profundo, hace que no sea posible entender cómo se llega a alcanzar unas determinadas recomendaciones o decisiones. Este fenómeno, conocido como *black box*, pone en riesgo el principio de motivación de las resoluciones judiciales, pues nada puede ser decidido afectando derechos fundamentales sin que exista manipulación comprensible y verificable del proceso. Por tanto, resulta perentorio exigir sistemas de IA auditables, trazables y controlados permanentemente por humanos, como estándar mínimo de legalidad. Otro principio importante es el de la igualdad y no discriminación, que es amenazado de inmediato cuando los algoritmos son alimentados por información sesgada o carente de representatividad suficiente. Y en sede penal, esta cuestión puede ser fatal, pues puede acentuar o reproducir desigualdades estructurales respecto de los grupos étnicos, de los sectores vulnerables o de aquellos históricamente excluidos. La legislación ecuatoriana y comparada exige que toda herramienta que se utilice en el proceso penal garantice la imparcialidad y la neutralidad, por lo que los sistemas de IA habrá de ser objeto de evaluaciones periódicas de sesgo y riesgo, debiendo establecerse mecanismos reparadores que limiten la discriminación algorítmica que fuere. También reviste especial importancia el principio de legalidad penal, que prohíbe que conducta alguna evidencie sanción si ésta no resulta prohibida por la ley. La entrada en funcionamiento de los algoritmos predictivos o herramientas de evaluación del riesgo comporta la necesidad de garantizar que la persecución penal no se apoye en percepciones estadísticas, sino en hechos concretos. La justicia penal ecuatoriana deberá garantizar que la IA no supla la valoración humana, ni estimule prácticas sancionadoras preventivas que se aparten del principio de tipicidad y de la prohibición de penas anticipadas. La tecnología es un auxilio, nunca un reemplazante del análisis jurídico racional. Finalmente, la incorporación de la IA en el derecho penal conllevará también el deber de observar estrictamente el principio de

proporcionalidad, especialmente en lo atinente a la recolección, tratamiento y uso de datos de naturaleza personal. Los sistemas algorítmicos funcionan por medio del análisis masivo de la información, con lo que habrá que asegurarse que la manipulación de datos esté justificada, limitada y protegida conforme a la normativa ecuatoriana en materia de seguridad de datos de carácter personal. Asimismo, la proporcionalidad deberá gobernar en la intensidad y alcance del uso de tecnologías como el reconocimiento facial, la vigilancia automatizada o el análisis predictivo. Sólo así se estará en la mejor oportunidad de garantizar que la innovación tecnológica no supere ni vulnere los límites constitucionales que protegen la dignidad humana, la autodeterminación informativa y el debido proceso.

Aspectos Legales de la IA en el Derecho Penal

La integración de la IA en el derecho penal genera cuestiones fundamentales desde el punto de vista jurídico. Una de las preocupaciones básicas viene referida a la seguridad jurídica y a la transparencia y responsabilidad en cuanto a los sistemas de IA. En el ámbito del derecho penal es necesario que se utilicen algoritmos comprensibles y auditables, ya que es necesario que se pueda revisar y cuestionar las decisiones que toman. La falta de transparencia en la utilización de procesos algorítmicos puede llevar a la decisión a la que se ha llegado por los mismos, a ser muy difícil de reclamar o corregir. También requiere la protección de derechos fundamentales como la privacidad y el debido proceso. El uso del SI en la vigilancia y en el tratamiento de datos puede llevar a un importante grado de violación de la privacidad de los individuos, lo que lleva a la necesidad de proteger ciertos derechos individuales frente a la utilización de esos sistemas para salvaguardar la seguridad pública. Es necesaria una modificación normativa, en un sentido amplio, de las normativas existentes, lo que proporcionará solución a todos estos nuevos problemas que la evolución de la ciencia está dando en cualquier forma jurídica. (López, 2024).

Desde un punto de vista ético, el tratamiento de la IA en el ordenamiento del derecho penal plantea problemas profundos relacionados con la justicia y la imparcialidad. Uno de los problemas más graves es el de la posibilidad de que aparezcan sesgos en los algoritmos. Los sistemas de IA pueden perpetuar, o incluso acentuar los sesgos existentes en los datos con los que se entrenan esos sistemas, lo que comporta decisiones discriminatorias e inequitativas. Por ejemplo, si un sistema de IA se sirve de datos históricos reflejo de sesgos raciales o socioeconómicos, esos sesgos pueden ser replicados en las decisiones que tome el sistema. También la utilización de sistemas de IA para predecir comportamientos futuros ofrece lógicas éticas relacionadas con el régimen de imputabilidad y la determinación de la culpabilidad. La posibilidad de predecir comportamientos criminales antes de que estos se produzcan puede ser considerada como una forma de anticipación

de la pena, lo que lleva a interrogarse sobre la correcta observancia de los principios de culpabilidad y proporcionalidad en el derecho penal.

La regulación de la IA, en el orden del derecho penal, es una tarea compleja y presenta la necesidad de una colaboración interdisciplinar legisladora. La sabia interpretación de estas herramientas por parte de tecnólogos y expertos en ética, es necesario que evolucionen regulaciones que procuren el uso responsable y ético de la IA, cuidando los derechos de las personas y promoviendo la equidad. La creación de normas claras sobre transparencia, responsabilidad y no discriminación es esencial, para que estas tecnologías se usen con apego a los principios legales y éticos básicos. También la gobernanza de la IA debe considerar la participación de la supervisión judicial y la participación pública. Los sistemas de IA deben estar sujetos a un control estricto y a la posibilidad de revisión judicial, para asegurar que tales actividades no se salgan de los límites legales y éticos. Igualmente, la participación de la ciudadanía en la elaboración de políticas públicas que toquen el uso de IA puede reflejar sus inquietudes o valores, en relación con la regulación de estas tecnologías. En cuanto a Casos de estudio y ejemplos prácticos para demostrar los retos u oportunidades que se producen con el uso de IA en el derecho penal, son de utilidad, los casos de estudio y ejemplos prácticos. Las herramientas relacionadas con la IA, en cuanto a policía predictiva, análisis forense y el sistema judicial tienen resultados mixtos. Algunos han demostrado mejoras en la eficacia al igual que en la precisión, sin embargo, otros han demostrado serios problemas en lo que se refiere a equidad y transparencia. Estos ejemplos son una fuente valiosísima a considerar, para el uso o la conducción de las políticas públicas de regulación. La IA tiene un potencial importante para transformar el derecho penal, sin embargo, plantea importantes retos y problemas legales y éticos.

Tabla 8.
Oportunidades y Riesgos del Uso de la IA en el Derecho Penal

Oportunidades	Riesgos
Análisis masivo y rápido de datos criminológicos	Sesgos algorítmicos replicados desde datos históricos
Mejora en eficiencia investigativa y forense	Falta de transparencia (cajas negras)
Predicción de patrones delictivos	Potencial afectación a la presunción de inocencia
Automatización de tareas repetitivas	Riesgo de vigilancia excesiva y violaciones de privacidad
Apoyo técnico en decisiones judiciales	Dificultad para impugnar decisiones automatizadas
Reducción del error humano en procesos técnicos	Discriminación automatizada y desigualdad estructural

Nota: La tabla evidencia que el uso de IA en el Derecho Penal ofrece importantes ventajas operativas, pero también introduce riesgos que requieren regulación, supervisión judicial y salvaguardas para proteger los derechos fundamentales.

La colaboración continua entre expertos en derecho, tecnología y ética será esencial para asegurar que la IA contribuya a un sistema de justicia penal más eficaz y equitativo, el impacto de la IA en el derecho penal es profundo y multifacético. La evolución de la tecnología y la adaptación de las normativas legales y éticas deberán avanzar de la mano para garantizar que el uso de la IA en el derecho penal no solo mejore la eficiencia y la precisión, sino que también respete los principios fundamentales de justicia y derechos humanos. ((INEC, s.f.) Por otra parte, en el Ecuador, la legislación que aborda específicamente la IA en el derecho penal es todavía incipiente. Sin embargo, el país ha comenzado a sentar las bases para la regulación de la tecnología y su uso en diversos ámbitos, incluyendo el derecho penal. La Constitución de 2008 establece principios fundamentales que tienen implicaciones para el uso de la IA en el derecho penal. El Artículo 66 garantiza el derecho a la privacidad, lo cual es crucial en el contexto de la IA, especialmente en la recolección y análisis de datos personales. Además, el Artículo 76 establece el derecho a un juicio justo y a la protección judicial, lo que implica que cualquier tecnología utilizada en el sistema penal debe respetar estos derechos y asegurar la transparencia y la rendición de cuentas. En 2021, Ecuador aprobó la Ley de Protección de Datos Personales (LPDP), la cual es relevante para la IA, ya que regula el manejo de datos personales. Esta ley establece principios para la recolección, almacenamiento y procesamiento de datos, lo que es particularmente importante en la aplicación de IA en el derecho penal. La LPDP exige que el tratamiento de datos personales sea legítimo, adecuado y proporcional a las finalidades perseguidas, lo que afecta directamente cómo se pueden usar los sistemas de IA en el ámbito penal. (ECUADOR, 2008) El Código Orgánico Integral Penal (COIP), que regula el derecho penal en Ecuador, aún no incluye disposiciones específicas sobre la IA. Sin embargo, ciertos principios generales del COIP pueden aplicarse a la implementación de tecnologías avanzadas. Por ejemplo, el principio de legalidad (*nullum crimen, nulla poena sine lege*) implica que no se pueden imponer sanciones sin una ley previa que las establezca. Esto se traduce en que cualquier tecnología de uso en el derecho penal debe tener un soporte legal notorios. La ética en el uso de la AI en el derecho penal se cifra en que la tecnología que se utiliza tiene que ser usando en aras a la defensa de los principios de justicia y equidad. La utilización de las herramientas de AI tiene que tener en cuenta la incidencia que se tiene en las personas y en la sociedad en su conjunto. En el Ecuador tiene que existir la discusión sobre de qué manera se puede lograr un equilibrio entre la eficiencia que ahorran las tecnologías de AI y la protección de los derechos humanos y la justicia social. La Responsabilidad Penal y la Determinación de Culpabilidad en la utilización de AI para predecir delitos o evaluar riesgos plantean problemas éticos sobre la Responsabilidad y la determinación de culpabilidad. En el derecho penal ecuatoriano, el principio de culpabilidad establece que debe existir la Responsabilidad en las personas sobre las acciones que realizan basadas

en la intencionalidad y la realización de conducta. La utilización de AI, por el contrario, para predecir delitos puede llegar a la forma de Responsabilidad anticipada, que no se acomoda a esos principios. Es preciso que se evalúe de qué manera la tecnología resulta coherente con los principios capitales de derecho penal. En la implementación de la utilización de AI en el derecho penal ecuatoriano, probablemente la participación pública y la supervisión van a ser fundamentales para lograr que estas tecnologías sean empleadas de una manera ética. En el Ecuador, la inexistencia de las normas jurídicas específicas en relación a la AI y en el ámbito penal evidencia la necesidad de que exista una discusión abierta y participativa sobre esta discusión sobre la utilización de estas tecnologías. La ciudadanía tiene que tener permitido el influjo en las políticas legislativas y control de estas que afectan a su privacidad y seguridad. La discusión que se realice sobre los supuestos aplicación de AI, en el derecho penal, puede llevar a soluciones importantes. Estudiar de qué forma otros países han abordado la utilización de la AI en el derecho penal puede llevar a resultados buenos para el Ecuador. En Estados Unidos y en la Unión Europea se han establecido leyes de control, regulación y recomendaciones éticas sobre el uso de la AI en el campo penal. Estas recomendaciones giran sobre escudriñar los principios aplicables a la transparencia, protección de datos y ausencia de discriminación. (CÓDIGO ORGÁNICO INTEGRAL PENAL, 2014). Con el fin de enfrentar los problemas legales y éticos en los cuales interviene la IA y el derecho penal, se sugiere para el Ecuador:

1. Elaborar Normativas Específicas. Es de suma importancia crear y actualizar legislaciones específicas que regulen el uso de la IA en el derecho penal, asegurando el respeto de los derechos fundamentales y la administración de justicia.
2. Establecer Mecanismos de Transparencia. Implementar mecanismos de auditoría y revisión de los sistemas de IA utilizados en el campo penal, asegurando que sean transparentes y auditables.
3. Promover la Participación Ciudadana. Involucrar a la ciudadanía en el desarrollo de políticas y regulaciones sobre la IA, asegurando que las decisiones sobre tecnología reflejen las preocupaciones e intereses públicos.
4. Realizar Evaluaciones Periódicas. Ejercer valoraciones periódicas para detectar y corregir sesgos en los sistemas de IA, garantizando que sean utilizados de forma equitativa y justa. (celebrado, 2017)

El uso de la Inteligencia Artificial en el derecho penal, representa una oportunidad para mejorar la eficacia y eficiencia del sistema de justicia que tiene el Ecuador. Sin embargo, en el mismo tiempo

existen importantes problemas legales y éticos que deben ser tratados con la debida cautela. La legislación ecuatoriana debe evolucionar y hacer frente a dichos problemas, asegurando que la utilización de la IA respete los principios fundamentales de la justicia, transparencia y garantía de los derechos humanos. La colaboración de los legisladores, los tecnólogos y la sociedad civil será fundamental para crear un marco normativo, que permita el uso responsable y ético de la IA en el derecho penal.

Principios legales aplicables

La Inteligencia Artificial (IA) está revolucionando a diferentes sectores, incluido el derecho penal, ya que proporciona herramientas altamente eficaces para la prevención, investigación y resolución de delitos. Sin embargo, la incorporación de la inteligencia artificial en este campo plantea importantes problemas que deberán enfrentarse a través de unos sólidos principios jurídicos. Estos principios son los que garantizan que la incorporación de la inteligencia artificial al derecho penal se haga de tal forma que sea justa, transparente y respetuosa de los derechos humanos. Esta sección se dedicará a mencionar los principios jurídicos que se aplican al uso de la inteligencia artificial en el derecho penal, y que constituyen la base de su regulación y aplicación ética. Es de suma importancia mencionar el Principio de Legalidad “Nullum Crimen, Nulla Poena Sine Lege”. Este es un pilar básico del derecho penal, ya que establece que no hay delito ni pena que no tenga una ley anterior que los defina. Este principio garantiza que nadie puede ser sometido a un juicio ni castigado por actos que no estén tipificados como delitos en las leyes vigentes. Aplicado al tema de la inteligencia artificial, el principio exige que haya una base legal clara y explícita con respecto al uso de la tecnología en el medio que tratamos, y que toda la aplicación de la inteligencia artificial en el derecho penal esté debidamente regulada por las leyes que establezcan el modo de uso y que fijen los procedimientos y limitaciones que se requieran. Por ejemplo, al ser utilizada la inteligencia artificial para la predicción del crimen, la recolección y análisis de datos deberá estar regulada por leyes que definan el modo de su procesamiento y manejo. La falta de leyes específicas podría llevar a un uso arbitrario de la tecnología, pero sin la debida vigilancia legal. (Ávila Santamaría, 2012).

Tabla 9.

Principios Legales Aplicables al Uso de IA en el Derecho Penal

Principio Legal	Descripción	Riesgos que Previene
Legalidad	Toda tecnología usada en el proceso penal debe tener base legal expresa.	Arbitrariedad tecnológica; uso no autorizado de IA.
Presunción de Inocencia	Ningún sistema de IA puede prejuzgar culpabilidad antes del juicio.	Punición anticipada; sesgo predictivo.

Proporcionalidad	Medidas automatizadas deben ser adecuadas y no excesivas.	Sanciones desproporcionadas basadas en IA.
Transparencia / Explicabilidad	Los algoritmos deben ser comprensibles, auditables y revisables.	Decisiones opacas; indefensión del acusado.
No Discriminación	La IA no debe replicar prejuicios raciales, económicos o culturales.	Sesgo algorítmico; trato desigual.
Respeto de Derechos Humanos	Toda utilización de IA debe alinearse con privacidad, debido proceso y dignidad humana.	Violaciones sistemáticas de derechos fundamentales.

Nota: Estos principios constituyen el marco jurídico mínimo que debe guiar la integración de sistemas de IA en el proceso penal, garantizando su uso legítimo, proporcional y respetuoso de los derechos fundamentales.

Es imprescindible hacer referencia a los Ejemplos Internacionales, en muchos países la legislación sobre IA en el ámbito penal se encuentra en pañales. Por ej. en la Unión europea, el Reglamento General de Protección de Datos (GDPR), la propuesta de Ley de Inteligencia Artificial) son normas que se han escrito que trataban sobre el uso de IA, con exigencias de transparencia y justificación legal de las decisiones automatizadas.

El principio de legalidad no solo se refiere a la definición de delitos y penas sino a los procedimientos que se utilizan para su aplicación. En el Derecho Penal esto significa que los procedimientos deben ser claros, accesibles y justos. Los sistemas de IA deben funcionar en forma tal que son transparentes para que los procedimientos sean entendidos y auditados. Esto implica la necesidad que los algoritmos utilizados deben ser accesibles para su revisión y evaluación. La transparencia de los procedimientos implica que las decisiones tomadas por la IA deben ser explicadas y justificadas, de modo de permitir a los interesados, incluidos acusados, puedan entender cómo se puede llegar a una determinada decisión. En algunos países, por ej. en Alemania, se están elaborando guías de conducta que permitan que las decisiones automatizadas en el sistema judicial sean revisables. En otros lugares por ej. en los Estados Unidos se han presentado demandas a efectos de obligar a las agencias estatales a explicar por qué los sistemas de IA han hecho determinadas decisiones. El principio de presunción de inocencia establece que toda persona es inocente hasta que se declare su culpabilidad. Este principio es uno de los pilares fundamentales a efectos de asegurar juicio justo y evitar que se impongan sanciones injustas. Cuando en el ámbito del derecho penal se utiliza IA es de suprema importancia tener cuidado que los sistemas en uso no prejuzguen a las personas ni afecten este principio de presunción de inocencia.

Los sistemas de IA deben ser implementados de tal manera que colaboran con la toma de decisiones sin incurrir en el defecto de presuponer la culpabilidad de un individuo hasta tanto se realice un juicio justo. Es decir, evitar que los algoritmos que se utilizan para establecer los criterios de riesgo de reincidencia o probabilidad de conducta delictiva, prejuzguen a los acusados. Los sistemas de IA deben ser diseñados de tal manera que se les provea información que complemente

la evaluación humana que se realice, pero que esto no signifique despreciar o influir negativamente en el principio de presunción de inocencia. (Ávila Zea)

El principio de proporcionalidad establece que las penas o medidas impuestas sean adecuadas y proporcionales a la gravedad del delito cometido. Este principio tiene por objeto que las sanciones no sean desproporcionadas con respecto al delito y que se respeten los derechos humanos. Al aplicarse la IA al derecho penal, es necesario que las recomendaciones o decisiones emanadas de los sistemas de IA respeten el principio de proporcionalidad. Esto incluye el garantizar que las decisiones automáticas, como la imposición de penas o medidas cautelares, sean revisadas y modificadas con el fin de que sean proporcionales a la gravedad del delito. En algunos países, como el Reino Unido, se están haciendo esfuerzos en tal sentido para incorporar los principios de proporcionalidad al uso de IA en el derecho penal. Esto incluye también la evaluación acerca de cómo los servicios automáticos influyen en la proporcionalidad de las penas y medidas. El principio de no discriminación, establece que todas las personas deben ser tratadas igualmente y sin ningún tipo de discriminación, por razón de raza, sexo, religión, origen étnico o cualquier otra característica protegida. Uno de los más grandes problemas en el uso de IA en materia penal, es el riesgo de que los algoritmos muestren sesgos. Los sistemas de IA pueden perpetuar o amplificar sesgos en los datos que sirven de base para su entrenamiento, lo cual se puede traducir en decisiones discriminatorias. Para evitar el problema, es importante que los sistemas IA sean diseñados y evaluados para realizar acciones que detecten y corrijan esos sesgos. Lo cual incluye la realización de auditorías periódicas y la puesta en práctica de las medidas para corregir el funcionamiento de los algoritmos y para garantizar que las decisiones sean justas y equitativas. El principio de respeto a los derechos humanos establece que todas las actuaciones y decisiones que se produzcan en el sistema penal deben respetar los derechos fundamentales de las personas, como el derecho a la intimidad, el derecho a un juicio justo y el derecho a no ser sometidos a tortura o tratos inhumanos.

El uso de la IA en el derecho penal tiene que estar alineado con los derechos humanos internacionales y nacionales. Esto implica asegurar que la aplicación de tecnología no vulnere derechos fundamentales, así como respetar los estándares internacionales en materia de tratamiento de información y toma de decisiones. Organismos internacionales como las Naciones Unidas y el Consejo de Europa han elaborado guías y recomendaciones para asegurar que la tecnología, incluida la IA, sea utilizada en forma de respeto a los derechos humanos. Estas guías deben ser las referencias que guíen el desarrollo e implementación de políticas nacionales en el Ecuador y en los demás países. (Abel Souto, 2024)

La aplicación de principios jurídicos en el uso de la IA en el derecho penal es de vital importancia para asegurar que esta tecnología sirva a la justicia en forma equitativa y justa. Los principios de legalidad, transparencia, presunción de inocencia, proporcionalidad, no discriminación y respeto a los derechos humanos son principios básicos que hacen posible la regulación y aplicación ética de la IA en el ámbito penal. A medida que la tecnología sigue avanzando, resulta esencial que las normas legales y políticas avancen para poder afrontar los retos y garantizar que la IA sea utilizada en el respeto de los principios básicos del derecho penal.

Ética de la inteligencia artificial en el ámbito penal

La ética de la inteligencia artificial en el ámbito del derecho penal estudia las implicancias que tiene el uso de dicha tecnología con el fin de asegurar el respeto de los derechos fundamentales a la justicia, derecho de defensa y debido proceso. Estos aspectos son de fundamental importancia, ya que la inteligencia artificial se ha incorporado al derecho penal, por ejemplo, en el área de la predicción del crimen, investigación de delitos, identificación de sospechosos, administración de riesgos, entre otros. En este sentido, surgen las preguntas fundamentales sobre el impacto que la aplicación de este tipo de tecnología tiene sobre el acceso a la justicia, y si el uso de algoritmos que permiten la toma de decisiones de forma automatizada respeta los principios de justicia, equidad y no discriminación. Una de las características principales sobre la ética de la inteligencia artificial en el área del derecho penal, consiste en que el sistema de IA sea diseñado para que no se reproduzcan ni se profundicen sesgos establecidos en los datos históricos que se utilizan para el entrenamiento de los algoritmos, toda vez que esto puede dar lugar a decisiones discriminatorias e injustas que pueden afectar de forma desproporcionada a ciertos grupos de la población. La transparencia resulta ser otro de los principios relevantes y esenciales en la ética de la inteligencia artificial en esta área. Es necesario que las decisiones que se tomen por los sistemas de inteligencia artificial sean comprensibles y auditable, de forma que los ciudadanos puedan entender cómo se llega a ciertas conclusiones. La falta de transparencia y claridad en los algoritmos que son utilizados para la toma de decisiones pueden menoscabar la confianza en el sistema judicial y dificultar también la rendición de cuentas. Por lo anterior, resulta esencial que los sistemas de IA se produzcan en base a la transparencia, que permitan a las partes interesadas revisar y cuestionar las decisiones que están siendo tomadas mediante la utilización de algoritmos automatizados. El hecho de que la IA sea utilizada con el fin de que se procesen grandes volúmenes de datos, puede implicar, en algunos casos, una violación significativa a la vida privada de los individuos. Es por esto que resulta esencial establecer salvaguardas para asegurar la protección de la privacidad, así como que la recolección de datos y su procesamiento se realicen de forma tal que se respetan los derechos individuales. Se

impone, por esto, la necesidad de nuevas legislaciones que regulen la forma en que se lleva a cabo la recolección de datos, donde se regulen aspectos como el almacenamiento y utilización de los mismos en el ámbito del derecho penal, procurando así minimizar el riesgo de violaciones a la privacidad. La responsabilidad y la rendición de cuentas resulta ser otro de los aspectos más importantes, desde el punto de vista ético que debe ser considerado. Cuando las decisiones en el ámbito penal están basadas en IA, corresponde que se sepa quién es el responsable de las consecuencias que se deriven de dichas decisiones. Esto quiere decir que los desarrolladores y operativos de los sistemas de la IA deben responder ante la necesidad de que sus tecnologías funcionen de la forma justa y precisa por la cual han sido legadas a las personas, por lo cual la existencia de mecanismos de revisión y apelación debe estar, en la medida de lo posible, a fin de que las personas afectadas por las decisiones automatizadas, pueden pelear por esta justicia y corregir, cuando es necesario, su posible error. (García 2023). Junto al principio de justicia es importante en la ética de la IA en el ámbito penal. La técnica debe ser utilizada para lograr una administración de justicia que se acerque a la equidad y proporcionalidad. Los sistemas de IA deben ser contruidos para lograr que se apoyen en el juicio humano y no que lo sustituyan, donde sus recomendaciones deben tomarse en cuenta en virtud de los principios legales y éticos.

Es importante que la técnica no se convierta en un elemento que agrande las desigualdades ya existentes en el sistema penal, sino que en virtud de ella sea posible la justicia que se procure sea más accesible y efectiva. Estos riesgos que se corren de la automatización de decisiones en el ámbito penal trata también de poder eventualmente plantearse si la tecnología podría alcanzar la capacidad de inteligibilidad ante las nuevas circunstancias ante los nuevos comportamientos humanos, donde también se plantean problemas y cuestiones donde las decisiones de la esfera penal supuestos tratados para su aplicación de pensar quienes tienen que resolverlas, es a conocer que en forma flexibles e inteligible debido a situaciones y personas a las que se refiere, o por cual motivo se están llevando a cabo, se tienen que aplicar a este texto que se escribe. Esto llevaría a la perforación de la responsabilidad penal propiamente dicha, que crea un margen de error y rectificaciones en toda la interpretación de la pena.

Después la ética en la IA en el ámbito penal tiene que llevar al principio de que se cohesiva el acceso a la tecnología. Para todos de forma igual, llevarlo a que es necesario que de este modo se concilien los recursos para hacer y controlar de estos sistemas de IA que se apliquen y realicen en este medio, sean hechos y llenados de forma equitativa, si a esto lugar se logran que esta tecnología puede servir a alguna margen desproporcionadamente tampoco en estos casos.

Esto ha hecho que esta aplicación de la IA en el ámbito penal tenga en cuenta estas desigualdades y no se haga sea a tal aplicación de la tecnología de esta manera, como ha sido señalado y se les ha

puesto carta de razón, y se hagan en virtud de esta tecnología que no sean las que a su vez agudicen la desigualdad que está tan felizmente denunciada en nuestro país.

Marco regulatorio internacional y nacional

El marco regulatorio internacional de la Inteligencia Artificial (IA) en el Derecho Penal está en una fase inicial y en desarrollo. Es una respuesta a la preocupación por el impacto de la tecnología en los derechos humanos y la justicia. En el plano mundial, y tanto los organismos internacionales como las organizaciones que están empezando a pronunciarse sobre la necesidad de regulación específica de la IA, se están haciendo eco del hecho de que es urgente elaborar un marco que regule el uso de la IA. De este modo se dará la impronta necesaria a la obtención de unos principios que garanticen la transparencia, la igualdad y la defensa de los derechos humanos. Así, la ONU y el Consejo de Europa se están haciendo eco de la importancia que tiene el establecimiento de estas directrices que han de servir de guía a los Estados miembros sobre la necesidad de regulación de la IA, así como de estándares a seguir en el ámbito de la justicia, y del derecho penal, por supuesto. En la UE, la regulación de la IA se ha avanzado considerablemente, con la adición presentada bajo el título AI Acta (Ley de Inteligencia Artificial) en abril de 2021. Esta Ley tiene como objetivo la creación de un marco de regulación de la actividad de la IA en todos los campos, y por supuesto en el del Derecho Penal. La Ley de IA de la UE otorga una clasificación a los sistemas de IA según el riesgo o peligrosidad que entrañan, añadiendo a los de alto riesgo, o peligrosidad, una serie de requisitos y/o limitaciones más severas, requisitos que se tienen que dar en el caso de la actividad que se realice en el ámbito del Derecho Penal. Se promueve la transparencia, la rendición de cuentas y la supervisión de los sistemas de IA que se habilitan de forma que el uso de la IA sea el correcto y se respete la defensa de los Derechos Humanos. A pesar de su juventud, la OCDE ya se ha puesto a trabajar en este campo, dictando los principios que han de regir la acción futura en este campo. En 2019, la OCDE publicó los "Principios de la OCDE sobre la Inteligencia Artificial", que son una serie de principios sobre el uso de la IA en los campos distintos de la economía, con reglas o principios sobre el uso de la IA, que se trasladan al campo público, y que tienen que ver con las reglas del Derecho Penal. En estos principios, se exige cumplir, como en los demás escritos antes mencionados, los principios de un uso centrado en el ser humano, que se promueva la transparencia, la igualdad, y la rendición de cuentas respecto de las decisiones automatizadas. Y aunque por ser principios no vinculantes, son un modelo o herramienta útil para que los Estados puedan establecer la regulación que en su caso consideren. En los USA, el marco regulatorio que también se ha de aplicar en el campo del Derecho Penal es el que se establece en la legislación respectiva. En este caso, es un marco a nivel de preparación sectorial o estatal y por parte de la Administración federal. Los criterios o normas que usa la Administración federal sobre la obtención

o uso de la IA en el sentido anteriormente expuesto son de mucho más fácil y rápido establecimiento que otros que exigen modificar las regulaciones específicas en cada uno de los Estados existentes. En el caso de la administración federal, lo que se está haciendo en los momentos actuales es dos procedimientos impulsando el (Artificial Intelligence Act) que es el que la actual administración Biden tiene hoy en comentarios su aplicación. También varias ciudades y estados han implementado sus propias regulaciones sobre el uso de tecnologías de vigilancia basadas en la IA, lo que da lugar a un enfoque reactivo y descentralizado. Las disputas sobre la regulación de la IA en el área penal, en los EE.UU., se centran en temas como la privacidad, la transparencia y el impacto de los algoritmos en la justicia. (Acuña, 2017). En América Latina, los marcos regulatorios de la IA en el derecho penal se encuentran en la etapa inicial de desarrollo. En Ecuador, la legislación no aborda de modo específico el uso de la IA en el derecho penal, aunque se han dictado normas que pueden afectar indirectamente a su uso. La Ley de Datos de Carácter Personal de Ecuador, por ejemplo, establece principios sobre el tratamiento de datos que son de interés para el uso de la IA en el derecho penal. Así también, la Constitución ecuatoriana garantiza derechos fundamentales que deben tenerse en cuenta en la aplicación de tecnologías de la IA, como el derecho a la privacidad y la protección contra la discriminación. Uno de los problemas relevantes sobre la implementación de marcos regulatorios de la IA en el derecho penal es la ausencia de una uniformidad y coherencia en los diferentes ordenamientos territoriales. La naturaleza global y la rápida evolución de la tecnología dificultan la aplicación de normas que sean a la vez flexibles y útiles.

Así también, la aplicación eficaz de la normativa requiere la colaboración estrecha de gobiernos, sector público y sociedad civil, a fin de poder asegurar que las políticas aplicadas sean conformes a las necesidades de la sociedad y cumplan con los principios internacionales en materia de derechos humanos. A medida que la IA avanza y su uso en el derecho penal se expande, se hace necesario hacer evolucionar los marcos regulatorios para hacer frente a los nuevos desafíos. Se sugiere que los países utilicen enfoques que se basen en los principios internacionales, al tiempo que desarrollan sus propias regulaciones nacionales. La colaboración internacional y el intercambio de buenas prácticas pueden ayudar en la elaboración de marcos regulatorios que aseguren el uso ético y responsable de la IA. De la misma forma, es vital que las reglamentaciones establezcan mecanismos que aseguren la revisión y adaptación continua a medida que la tecnología cambia y la misma afecta a la administración de la justicia penal.

Detección de denuncias falsas en otros países

En los últimos meses se ha desarrollado una herramienta capaz de detectar qué denuncias son falsas. Se llama Veripol y está basada en un algoritmo y un modelo matemático que, gracias a la inteligencia artificial y al procesamiento del lenguaje natural, es capaz de localizar las palabras que las presuntas víctimas más utilizan cuando mienten a la hora de denunciar unos hechos. Según el estudio de sus creadores 44, entre los que destaca Miguel Camacho, un inspector de policía, su porcentaje de acierto a la hora de determinar qué denuncias son falsas es del 91%, cifra muy superior al 75% que obtuvo un policía experto. Si bien los veredictos de esta herramienta no son vinculantes, puesto que no tiene capacidad de decisión, sí que supone un gran avance que podrá convertirse en un medio disuasorio cuando alguien esté planteándose presentar una denuncia falsa. Por tanto, cuando esta aplicación determine que una denuncia puede ser falsa, los agentes encargados podrán centrarse en averiguar más acerca de los presuntos hechos para esclarecer qué ha ocurrido realmente. En el caso de que la denuncia parezca verdadera, los agentes no deberán perder tanto tiempo en verificar su autenticidad, por lo que podrán centrarse en otros aspectos como buscar a los sospechosos. La primera comisaría en implantarlo ha sido la del Cuerpo Nacional de Policía de León, y las siguientes serán las de Ponferrada, San Andrés del Rabanedo y Astorga, aunque en un futuro no muy lejano se pretende que esta herramienta se utilice en todas las comisarías españolas. (Enríquez, (2019)).

Con este antecedente es indispensable que en Ecuador se realice un trabajo para desestimar las denuncias que no tengan elementos para llevarlas a instrucción fiscal, y para que la ciudadanía sepa que no puede presentar una denuncia que no tenga los requisitos establecidos. La justicia penal enfrenta desafíos complejos en la era digital, especialmente con el advenimiento de tecnologías avanzadas como la Inteligencia Artificial (IA). La detección de denuncias falsas representa un área crítica dentro de este contexto, dado el impacto significativo que tales denuncias pueden tener sobre el sistema judicial y la vida de las personas involucradas. En Ecuador, un país con un sistema legal en evolución y una creciente adopción de tecnologías emergentes, la intersección entre la IA y el derecho penal se convierte en un área de gran interés y desafío.

Definición de Denuncias Falsas

- **Denuncias maliciosas o temerarias y el uso de inteligencia artificial en el sistema penal**

Dentro del ámbito jurídico el término comúnmente tomado como “falsas denuncias” requiere una precisión conceptual para que no existan equívocos en la aplicación desde la perspectiva del derecho penal. Una denuncia no puede calificarse como falsa solamente porque no se obtiene prueba de los hechos denunciados en el juicio. En el sentido técnico el ordenamiento jurídico prevé

que la calificación correspondiente es la de denuncia maliciosa o temeraria que debe verificar la autoridad competente después que exista pleno conocimiento del dolo o de la falsedad de los hechos denunciados. Esta situación tiene relación con la garantía de la presunción de inocencia que es uno de los pilares del debido proceso en los sistemas jurídicos contemporáneos (Binder, 2016; Constitución de la República del Ecuador, 2008). En el Ecuador el marco constitucional reconoce la importancia de proteger los derechos fundamentales en el ámbito del proceso penal. El Art. 76 de la Constitución dice que toda persona debe ser considerada inocente hasta que exista una sentencia condenatoria ejecutoriada que determine su culpabilidad. Este principio supone que las denuncias que se formulen ante las autoridades judiciales deben ser analizadas con criterios de objetividad evitando calificaciones antes de tiempo que pueden afectar el derecho a la defensa o la seguridad jurídica. En ese sentido, el equilibrio que debe establecer el sistema judicial entre la necesidad de investigar infracciones que pudieran haberse cometido y la protección de los derechos de las personas que intervienen en el proceso penal es mucho más complejo de lo que parece (Constitución de la República del Ecuador, 2008; Ferrajoli, 2011). Desde el punto de vista del derecho penal, la presentación de denuncias falsas o maliciosas puede ser considerada como una infracción que se encuentra dentro de las sancionadas por la legislación. El Código orgánico integral penal (COIP) prevé la figura de la acusación o denuncia falsa, disponiendo responsabilidad para quien formule imputaciones con conocimiento de su falsedad, con el propósito de provocar la apertura de un proceso penal contra otra persona. Esta disposición tiene por objeto evitar una indefensión en el sistema de justicia y la utilización del aparato penal como instrumento para perseguir a personas en razón de problemas o conflictos personales. En un sentido doctrinario, este tipo de actos constituye a la vez un abuso del derecho penal que afecta la buena administración de justicia (Asamblea Nacional del Ecuador, 2014; Zaffaroni, Alagia & Slokar, 2002).

Las denuncias maliciosas o temerarias generan efectos de gran calado a nivel individual y colectivo. A nivel individual la persona que ha sido injustamente denunciada puede sufrir efectos negativos sobre su reputación, estabilidad emocional y vida profesional. A nivel colectivo, estas conductas contribuyen a saturar los sistemas judiciales, aumentando el tiempo de resolución de los procesos y disminuyendo la eficacia de la administración de justicia. Diversos estudios sobre política criminal han señalado que el abuso del Derecho Penal puede hacer que la confianza de la población en las instituciones encargadas de administrar justicia disminuya (Garland, 2001; Tonry, 2011). En años recientes el desarrollo de tecnologías basadas en inteligencia artificial (IA) ha abierto nuevas posibilidades para el mejoramiento en la administración de la información dentro de los sistemas judiciales. La inteligencia artificial es un conjunto de sistemas computacionales que pueden realizar actividades que requieren inteligencia humana, como el reconocimiento de patrones, el aprendizaje

automático y el procesamiento de lenguaje natural. En el ámbito del derecho las tecnologías han empezado a ser utilizadas para optimizar la administración de los expedientes, analizar grandes cantidades de información jurídica y ayudar en la toma de decisiones en procesos judiciales (Russell & Norvig, 2021; Surden, 2019). En el ámbito del derecho penal, la inteligencia artificial puede ser usada para analizar la información contenida en las denuncias, testimonios y documentos procesales. Con el uso de técnicas de procesamiento de lenguaje natural (Natural Language Processing) y aprendizaje automático, los sistemas de inteligencia artificial pueden detectar patrones de lenguaje, inconsistencias en las narraciones o similitudes entre las distintas versiones sobre hechos similares. Estas herramientas pueden ayudar a aumentar la eficacia en la investigación penal, facilitando el análisis de grandes volúmenes de información que dificultan el tratamiento manual por parte de los operadores de justicia (Ashley, 2017; Katz, Bommarito & Blackman, 2017). Aun así, la implantación de sistemas de inteligencia artificial en el sistema judicial plantea los importantes problemas legales y éticos. El estudio de varios autores pone de manifiesto que los sistemas algorítmicos reproducen los prejuicios colectivos contenidos en los datos que sirven para crear acuerdos sobre los cuales deben decidir y que ello puede dar lugar a decisiones discriminatorias o afectar a la igualdad en la aplicación de la justicia, por ello, la utilización de estos sistemas de inteligencia artificial en el campo del derecho penal debe ser acompañado por medios que garanticen la transparencia, el control y el control de los resultados que se obtienen y la utilización de técnicas o nuevos sistemas que, lejos de vulnerar los derechos fundamentales de los ciudadanos que tienen que ver con los procesos que se siguen, permitan finalmente en un plazo más o menos largo una mejor tutela de los derechos fundamentales de esas personas (Barocas, Hardt y Narayanan, 2019. O’Neil, 2016). En el caso ecuatoriano y atendiendo a que cualquiera de las iniciativas que se planteen en torno a la inteligencia artificial, en un futuro próximo en la gestión judicial, son compatibles con el marco normativo que regula la protección de datos personales, así como con seguridad jurídica, hay que señalar que en la Ley Orgánica de Protección de Datos se consagran una serie de principios que se refieren a la licitud, a la proporcionalidad y a la finalidad determinada del tratamiento de los datos de carácter personal. Estos principios que se explican convenientemente en el cita Ley Orgánica de Protección de Datos son especialmente importantes y deben ser respetados en la utilización de bases de datos judiciales o de datos que se pueden considerar sensibles en relación a cuestiones que tengan que ver con investigaciones penales en curso, pues de ello los derechos fundamentales de nuestro ciudadanos que pudieran de una u otra forma poder ser vulnerados por la utilización de estas nuevas tecnologías, están garantizados (Asamblea Nacional del Ecuador, 2021. Wachter, Mittelstadt y Floridi, 2017). En consecuencia, la utilización de inteligencia artificial en el análisis de denuncias dentro del ámbito del sistema judicial

debe seguirse utilizando como un instrumento de apoyo técnico a los operadores de justicia que sirven especialmente para conseguir que los sistemas sean más eficaces en la gestión de la información sin que dicha utilización de datos elimine o suplante los razonamientos lógicos jurídicos que han de realizar los jueces y fiscales a la hora de la valoración de las pruebas que se les presentan. La buena integración de esas nuevas tecnologías para el derecho penal puede ser vista como un recurso que sea eficaz a la hora de la resolución de los problemas que se plantean en la actualidad, mientras se respete la vigencia y la defensa de los principios constitucionales que hacen alusión a la vigencia de la preservación de la presunción de inocencia, el debido proceso, así como los derechos fundamentales de los ciudadanos, en fin, la seguridad jurídica (Susskind, 2019. Surden, 2019).

B. Desafíos Legales y Normativos

Los retos jurídicos que pone el uso de IA en el derecho penal son enormes, como la defensa de la intimidad, la equidad en el procesamiento de datos y la transparencia en las decisiones automatizadas. En Ecuador, la falta de legislación específica acerca de la IA en el campo penal crea un vacío que debe ser solucionado para garantizar un uso ético y legal de estas tecnologías. En el uso de IA en el derecho penal debe sujetarse a unos mínimos éticos. Por transparencia hemos de arder la necesidad de que los sistemas de IA sean comprensibles y accesibles para los usuarios. La justicia y el derecho son garantizar que los algoritmos utilizados no perpetúen los sesgos existentes y no discriminen a ciertos grupos. El uso de IA para la detección de denuncias falsas tiene un trasfondo ético importante que afecta a los derechos humanos como el derecho a un juicio justo o la presunción de inocencia. Es necesario que el uso de tecnologías de IA no lesione estos derechos. También que las decisiones tomadas de manera automatizada puedan ser revisadas y puestas en duda mediante mecanismos humanos correctos. Innovaciones tecnológicas y su afectación. Las innovaciones tecnológicas van a afectar siempre al campo del derecho penal. En Ecuador, el desarrollo y la implantación de tecnologías de IA tienen que estar guiadas por un marco legislativo y ético que las haga responsables. Se deben fomentar estudios y debates sobre las mejores formas de integrar la IA en el sistema judicial de forma efectiva y equitativa. Para poder utilizar la IA debidamente en la detección de denuncias falsas es importante una reglamentación clara y unas directrices éticas. Las recomendaciones serían la creación de un marco legal específico para la IA en el derecho penal, la formación del personal judicial en el uso de estas tecnologías y la puesta en marcha de mecanismos de control en cuanto a la equidad y la transparencia en el proceso penal. En conclusión, la detección de denuncias falsas mediante IA en el derecho penal en Ecuador es un capítulo que intersecciona, tecnología, derecho y ética. Las posibilidades que ofrece la IA de analizar gran cantidad de información, así como la detección de patrones pueden ofrecer soluciones

eficientes para resolver el problema de las denuncias falsas. pero también plantea importantes retos legales y éticos que deben ser cuidadosamente gestionados. La evolución del marco legal y la adopción de principios éticos son especialmente útiles para que la integración de la IA en el sistema judicial alcance con éxito sus objetivos de justicia e igualdad. (López, 2024) El análisis de la escena del crimen es una de las etapas más importantes en la investigación penal, es el primer paso para la reconstrucción de los hechos y la obtención de pruebas materiales que tan necesarias son para la resolución de un caso. Dicho proceso comprende toda una serie de técnicas y métodos científicos que se introducen y aplican para intentar asegurar que las pruebas sean recogidas, conservadas y analizadas adecuadamente, minimizando el riesgo de contaminaciones y garantizando la integridad de la investigación en sí. Con los avances de la tecnología, la inteligencia artificial (IA) se está convirtiendo a pasos agigantados en una herramienta emergente para la investigación en la escena del crimen, abriendo un abanico de posibilidades para aumentar la eficiencia y precisión en el análisis forense.

A. Definición y finalidades. Se entiende por análisis de la escena del crimen, el proceso sistemático de análisis del lugar donde habrán de producirse unos hechos delictivos, con la finalidad de identificar, recolectar y conservar unas pruebas materiales que son necesarias para intentar reconstruir los hechos que motivaron el delito de que se trate. Este análisis pretende dar respuesta a una serie de preguntas que se plantean sobre cómo, cuándo y por qué se ha producido el acto delictivo. Y es que aquí se trata de que, a partir de la prueba física hallada en la escena del crimen o de algún testimonio a nuestra disposición, se pueda elaborar una historia lógica que explique la serie de hechos. Los métodos tradicionales de análisis de la escena del crimen son la inspección visual, fotografía del lugar, utilización de la toma de medidas, que es la forma de obtener la posición de las pruebas esparcidas, y recolección de muestras del tipo aquí aludido, tales como huellas de dedos, sangre, otras materias biológicas. Por el contrario, la tecnología ha añadido ya aplicaciones como recuerdos en 3D, análisis de manchas de sangre o técnicas de reconstrucción digital que aumentan la eficacia y la precisión del análisis, etc. (Bermúdez, (2021).)

B. Introducción a la Inteligencia Artificial

La Inteligencia Artificial, en el campo de la criminología y el análisis forense, hace referencia a la utilización de sistemas informáticos que simulan funciones cognitivas humanas como el aprendizaje, la identificación de patrones y la toma de decisiones. En el análisis de las escenas del crimen, la IA puede procesar grandes cantidades de datos, identificar patrones y correlaciones que pueden no ser inmediatamente evidentes y proporcionar apoyo analítico en la reconstrucción de los hechos.

Las aplicaciones de IA en el análisis forense son:

- Reconocimiento de imágenes y video. Los algoritmos de IA pueden analizar imágenes y videos para identificar objetos, personas y comportamientos que sean relevantes.
- Análisis de datos. Herramientas de IA pueden analizar y procesar los datos recolectados en la escena del crimen, tales como patrones de huellas dactilares, ADN y otros elementos biológicos.
- Reconstrucción de escenas. La IA puede ayudar en la reconstrucción digital de la escena del crimen por medio de la creación de modelos 3D a partir de los datos recolectados, lo que ayuda a la visualización y análisis de la disposición de las pruebas.

En Ecuador, el uso de IA en el ámbito del derecho penal está en una fase inicial. La Constitución del Ecuador garantiza derechos fundamentales que deben ser respetados durante el proceso penal, tales como el derecho del debido proceso y la protección de datos personales. Aunado a ello existen leyes y regulaciones que hacen referencia a la privacidad y protección de datos como la Ley Orgánica de Protección de Datos Personales. La utilización de IA en el análisis de la escena del crimen presenta desafíos legales, incluida la necesidad de asegurarse que la tecnología se esté utilizando de tal forma que se respeten los derechos humanos y las garantías procesales de quienes son objeto de procesos penales. Es necesario que se garantice que los sistemas de IA sean transparentes, auditables y que las decisiones automatizadas sean revisables por autoridades competentes para prevenir abusos y errores judiciales. La utilización de IA en el ámbito del derecho penal debe someterse a principios éticos fundamentales, como son:

- Transparencia. Los sistemas de IA deben ser comprensibles y su operación debe ser clara para su propietario y/o los afectados.
- Justicia y No Discriminación. Los algoritmos deben estar diseñados de tal forma que eviten sesgos y que se aseguren que no discriminan a las personas o grupos por sus características como raza, clase social o género.
- Privacidad: La recolección y el procesamiento de datos deben llevarse a cabo de tal manera que se respete la privacidad de las personas y se protejan sus datos personales. (Guerrero 2020). Las implicaciones éticas del uso de la IA en el análisis de la escena del crimen son la exigencia de que las decisiones que sean tomadas por los sistemas automatizados no vulneren los derechos de los acusados y no perjudiquen el derecho a un juicio justo. Asimismo, se debe tener en cuenta la forma en que son tratados los datos que se recojan y cómo se garantiza la integridad del proceso de investigación. La evolución de la IA y su integración en el análisis forense tienen la promesa de mejorar la precisión y la eficacia en la investigación de la escena del crimen. En innovaciones futuras se prevé el desarrollo de algoritmos más avanzados para la detección de patrones complejos e integración de la IA con otras tecnologías emergentes, como la realidad

aumentada y la robótica. Sin embargo, junto a los beneficios que posee la IA en el análisis de la escena del crimen encontramos importantes dificultades en su uso. Estas consisten en la obligatoria en el desarrollo de mecanismos legales y éticos que sean los correctos, la capacitación del personal sobre el uso de estas tecnologías y la administración de los impactos negativos que pueden resultar del uso de datos sensibles. El análisis de la escena del crimen resulta ser una parte fundamental del proceso penal y que se va viendo transformado por la evolución de la Inteligencia Artificial. La capacidad de la IA para la rápida y precisa administración de los datos, da lugar a importantes oportunidades para mejorar la investigación criminal. El uso de la IA da lugar a importantes problemas legales y éticos que tienen que ser de forma cuidadosa tratados, a fin de impedir que su uso sea injusto, igualitario y respetuoso con los derechos humanos. En el contexto ecuatoriano, será imprescindible que se desarrolle un marco legal y ético que permita, por una parte, aprovechar los beneficios que da la IA en el derecho penal y, por la otra, la efectividad y tutela de los derechos fundamentales y de la justicia en el sistema judicial. La Inteligencia Artificial, en el campo de la criminología y el análisis forense, hace referencia a la utilización de sistemas informáticos que simulan funciones cognitivas humanas como el aprendizaje, la identificación de patrones y la toma de decisiones. En el análisis de las escenas del crimen, la IA puede procesar grandes cantidades de datos, identificar patrones y correlaciones que pueden no ser inmediatamente evidentes y proporcionar apoyo analítico en la reconstrucción de los hechos.

Las aplicaciones de IA en el análisis forense son:

- Reconocimiento de imágenes y video. Los algoritmos de IA pueden analizar imágenes y videos para identificar objetos, personas y comportamientos que sean relevantes.
- Análisis de datos. Herramientas de IA pueden analizar y procesar los datos recolectados en la escena del crimen, tales como patrones de huellas dactilares, ADN y otros elementos biológicos.
- Reconstrucción de escenas. La IA puede ayudar en la reconstrucción digital de la escena del crimen por medio de la creación de modelos 3D a partir de los datos recolectados, lo que ayuda a la visualización y análisis de la disposición de las pruebas.

En Ecuador, el uso de IA en el ámbito del derecho penal está en una fase inicial. La Constitución del Ecuador garantiza derechos fundamentales que deben ser respetados durante el proceso penal, tales como el derecho del debido proceso y la protección de datos personales. Aunado a ello existen leyes y regulaciones que hacen referencia a la privacidad y protección de datos como la Ley Orgánica de Protección de Datos Personales. La utilización de IA en el análisis de la escena del crimen presenta desafíos legales, incluida la necesidad de asegurarse que la tecnología se esté

utilizando de tal forma que se respeten los derechos humanos y las garantías procesales de quienes son objeto de procesos penales. Es necesario que se garantice que los sistemas de IA sean transparentes, auditables y que las decisiones automatizadas sean revisables por autoridades competentes para prevenir abusos y errores judiciales. La utilización de IA en el ámbito del derecho penal debe someterse a principios éticos fundamentales, como son:

- **Transparencia.** Los sistemas de IA deben ser comprensibles y su operación debe ser clara para su propietario y/o los afectados.
- **Justicia y No Discriminación.** Los algoritmos deben estar diseñados de tal forma que eviten sesgos y que se aseguren que no discriminan a las personas o grupos por sus características como raza, clase social o género.
- **Privacidad:** La recolección y el procesamiento de datos deben llevarse a cabo de tal manera que se respete la privacidad de las personas y se protejan sus datos personales. (Guerrero 2020). Las implicaciones éticas del uso de la IA en el análisis de la escena del crimen son la exigencia de que las decisiones que sean tomadas por los sistemas automatizados no vulneren los derechos de los acusados y no perjudiquen el derecho a un juicio justo. Asimismo, se debe tener en cuenta la forma en que son tratados los datos que se recojan y cómo se garantiza la integridad del proceso de investigación. La evolución de la IA y su integración en el análisis forense tienen la promesa de mejorar la precisión y la eficacia en la investigación de la escena del crimen. En innovaciones futuras se prevé el desarrollo de algoritmos más avanzados para la detección de patrones complejos e integración de la IA con otras tecnologías emergentes, como la realidad aumentada y la robótica. Sin embargo, junto a los beneficios que posee la IA en el análisis de la escena del crimen encontramos importantes dificultades en su uso. Estas consisten en la obligatoria en el desarrollo de mecanismos legales y éticos que sean los correctos, la capacitación del personal sobre el uso de estas tecnologías y la administración de los impactos negativos que pueden resultar del uso de datos sensibles. El análisis de la escena del crimen resulta ser una parte fundamental del proceso penal y que se va viendo transformado por la evolución de la Inteligencia Artificial. La capacidad de la IA para la rápida y precisa administración de los datos, da lugar a importantes oportunidades para mejorar la investigación criminal. El uso de la IA da lugar a importantes problemas legales y éticos que tienen que ser de forma cuidadosa tratados, a fin de impedir que su uso sea injusto, igualitario y respetuoso con los derechos humanos. En el contexto ecuatoriano, será imprescindible que se desarrolle un marco legal y ético que permita, por una parte, aprovechar los beneficios que da la IA en el derecho penal y, por la otra, la efectividad y tutela de los derechos fundamentales y de la justicia en el sistema judicial.

Inteligencia artificial y su impacto en el derecho penal

En la actualidad, la inteligencia artificial (IA) está transformando numerosos ámbitos de la vida social, económica y tecnológica, y el sistema judicial no constituye una excepción. En el campo del derecho penal, el desarrollo de herramientas basadas en inteligencia artificial ha comenzado a utilizarse con el objetivo de mejorar la precisión en el análisis de información, optimizar la gestión de expedientes judiciales y fortalecer la eficiencia en la administración de justicia. No obstante, su incorporación dentro de los procesos judiciales también plantea importantes desafíos desde el punto de vista jurídico, ético y constitucional. En países como Ecuador, donde el sistema judicial se encuentra en constante proceso de modernización institucional, resulta necesario analizar de qué manera estas tecnologías pueden influir en la toma de decisiones judiciales y cuáles son los principios jurídicos que deben orientar su implementación.

La inteligencia artificial puede definirse como la capacidad de los sistemas computacionales para ejecutar tareas que normalmente requieren capacidades cognitivas humanas, tales como el procesamiento del lenguaje natural, el reconocimiento de patrones complejos y el análisis automatizado de grandes volúmenes de datos. Estas herramientas permiten identificar relaciones entre variables, detectar inconsistencias en la información y apoyar procesos de análisis que, de manera manual, resultarían considerablemente más complejos. En el ámbito del derecho penal, la inteligencia artificial se está utilizando para diversas aplicaciones, entre ellas el análisis de pruebas digitales, la predicción de patrones delictivos, la clasificación automatizada de documentos judiciales y la asistencia en procesos de toma de decisiones dentro de los sistemas judiciales (Digital Future Society, En este sentido, es necesario establecer en el ámbito de los operadores de justicia vínculos relaciones de colaboración y asociación con el sector académico, a fin de que se puedan llevar a cabo proyectos de investigación y capacitación que permitan el desarrollo de tecnologías para la administración de justicia, y que estén de acuerdo con la cultura y realidad social ecuatoriana, así como a fin de poder establecer sistemas de evaluación que brinden un marco de evaluación seguro para la utilización de sistemas automatizados. En el mismo sentido es necesario que el sistema jurídico ecuatoriano establezca mecanismos que garanticen el mantenimiento de un nivel de control que sea por lo menos suficiente para garantizar que el uso de sistemas automatizados no altere los derechos fundamentales de los individuos, en ese sentido y apoyándonos en el conocimiento de la administración de justicia, la utilización de inteligencia artificial para administrar justicia en el país debe ser explorado a fondo, por el bien de todos. La utilización de inteligencia artificial para la administración de justicia en el ecuatoriano debería estar dirigido a promover la construcción de un nuevo modelo de justicia, donde el respeto a los derechos de los individuos y

de las comunidades tenga que ser considerada como la base jurídica que garantice el desarrollo de un nuevo concepto de justicia que una a los ecuatorianos y lo convierta en el país justo que todos sus habitantes desean y que es una de las bases de desarrollo que garantice el avance en la calidad de vida de sus habitantes. Todo lo expuesto debe ser evaluado en concierto con todas las áreas de la justicia, es decir, los administradores de justicia, el sistema penitenciario y el sistema de administración de justicia juvenil que debe ser considerado en el plano que propone la inteligencia artificial, lo que implica la búsqueda de un sentido a la utilización de los sistemas automatizados en la administración de justicia, que según la concepción de lo que debe ser, puede significar la creación de un nuevo sistema de la justicia que se traduce en hacerle frente a la creación, adaptación y asimilación de impulsos y estímulos que el ser humano es capaz de transmitir, lo que a la larga influye sobre los administradores de justicia y crea caminos en sus mentes que son generadores de nuevos modos de ver las cosas y las relaciones humanas con el sentido verdadero que deben tener. El presente documento es solo una apertura respecto al mundo que representa la utilización de herramientas de inteligencia artificial para fortalecer la administración de justicia y en este sentido volar a la exploración de las diferencias que pueden encontrarse en la implementación de tales sistemas en el ámbito de la administración de justicia. Sin embargo, no debe perderse de vista la importancia de un sistema de participación de la ciudadanía dentro de los objetivos estos nuevos paradigmas que trata de implementar vulneraran derechos fundamentales y para ello es posible trabajar sobre el tema de la creación de sistemas de comunicación entre los sectores de la sociedad. En este sentido si se puede dilucidar un sistema que permita obtener información respecto al pensamiento de la ciudadanía.

Delitos informáticos, contenido digital y valoración probatoria mediante inteligencia artificial

En el contexto de la transformación digital de la sociedad, el derecho penal enfrenta nuevos desafíos derivados del surgimiento de los delitos informáticos y del uso creciente de información digital como medio de prueba dentro de los procesos judiciales. Los delitos informáticos comprenden aquellas conductas ilícitas que se realizan mediante el uso de sistemas informáticos, redes digitales o tecnologías de comunicación, incluyendo actividades como el acceso no autorizado a sistemas, la manipulación de datos, el fraude informático, la suplantación de identidad digital o la difusión ilícita de información.

En estos casos, gran parte de la evidencia relevante se encuentra en formatos digitales, tales como registros electrónicos, mensajes en plataformas de comunicación, correos electrónicos, archivos informáticos o registros de actividad en sistemas digitales. La naturaleza de esta información plantea desafíos particulares para la investigación penal, ya que requiere técnicas especializadas de análisis

y preservación de evidencia digital que garanticen la autenticidad, integridad y cadena de custodia de los datos.

En este escenario, la inteligencia artificial puede desempeñar un papel relevante en el análisis del contenido digital dentro de las investigaciones penales. Las herramientas basadas en inteligencia artificial permiten analizar grandes volúmenes de datos digitales, identificar patrones de comportamiento, reconstruir secuencias de eventos y detectar relaciones entre diferentes fuentes de información. Estas capacidades pueden resultar especialmente útiles para reconstruir un presunto hecho delictivo, permitiendo a los investigadores examinar de manera más eficiente registros digitales complejos o grandes bases de datos provenientes de dispositivos electrónicos o plataformas digitales.

No obstante, la utilización de inteligencia artificial en la valoración de evidencia digital debe realizarse con estricta observancia de los principios del derecho procesal penal. Específicamente, corresponde a jueces y tribunales de justicia internos evaluar la validez y pertinencia de los medios de prueba aportados en el proceso, asegurándose en todo caso que los resultados logrados a través de la tecnología no sustituyan el análisis jurídico, ni la valoración probatoria que se efectúe por parte de la autoridad judicial, correspondiendo especialmente a la inteligencia artificial ser concebida como un medio auxiliar técnico a la investigación penal, mas no un medio autónomo de determinación de la responsabilidad penal. Por esto, el desarrollo de metodologías que habrán de incorporar inteligencia artificial al análisis de prueba digital exige la articulación de conocimientos jurídicos, tecnológicos y periciales y la demostración de estándares claros que garanticen la fiabilidad del sistema usado y la salvaguarda de los derechos fundamentales de los intervinientes en el proceso penal.

A. Principios éticos en el uso de inteligencia artificial

La realización de una gran cantidad de denuncias falsas, se transforma en un problema creciente para los sistemas de justicia penal a nivel mundial, en cuanto que produce no solo una distorsión de la función investigativa, sino que además luzca como un uso ineficaz de los medios públicos, generando una desconfianza en lo institucional. En este marco, distintos países del mundo han comenzado a apreciar la utilidad de la inteligencia artificial como medio para el desarrollo de patrones lingüísticos y de comportamiento, que permiten a las autoridades detectar investigaciones en torno a la denuncia de los delitos de carácter doloso. La utilización de tecnología negra en el procesamiento del lenguaje natural y el uso de necesarios algoritmos de aprendizaje de máquina han permitido avances significativos en la detección temprana de la falsedad, y un especio de

desahogo de la carga procesal, abriendo además la aptitud investigativa por parte de los cuerpos del orden.

La comparación de la experiencia internacional resulta fundamental para comprender la forma de uso de la IA en las evaluaciones respecto de las denuncias. Los países con mayor desarrollo en lo tecnológico han implementado modelos experimentales que analizan la estructura narrativa de las declaraciones de los testigos y que han permitido diferenciar con altísimos niveles de certeza los relatos veraces de aquellos otros que han sido elaborados por el mismo autor o autores. Estos sistemas no reemplazan a la función investigativa de la policía ni menos a las facultades de materias investigativas de que estos gozan, pero sí constituyen un apoyo técnico que permita una mayor celeridad en la toma de decisiones en las etapas prematuras del proceso penal.

Análisis de los casos exhibidos permite la identificación de buenas prácticas, limitaciones y precauciones que deben tomarse en cuenta antes de adoptar soluciones similares y su adaptabilidad a otros contextos, Como el ecuatoriano requería. Lo que es necesario evaluar es el impacto positivo de la utilización de estas herramientas, así como los riesgos que su uso implica, en particular con relación a los derechos de las personas denunciantes y denunciadas, etcétera. Así, la experiencia internacional deviene un referente interesante en la reflexión sobre la pertinencia, viabilidad y eventual regulación, del uso de IA en la tramitación de denuncias en el seno del sistema de justicia penal del Ecuador. El uso de IA en el derecho penal debe atender a una serie de principios éticos, para garantizar que la tecnología sea utilizada de manera conveniente y equitativa. Estos principios son, entre otros:

- Justicia: Los sistemas de IA deben ser diseñados y entrenados, de forma tal, que los sesgos estén ausentes y las decisiones sean aptas, es decir que no perjudiquen a las personas, individuos o grupos, discriminándolos en consideración a alguna de sus características personales.
- Transparencia: El funcionamiento de los algoritmos de IA mismos, debe ser transparente ante el afectado y su usuario, a efectos de que puedan completar y revisar las decisores automatizadas:
- Responsabilidad: Los diseñadores y usuarios de IA deben asumir la responsabilidad sobre el uso que se les dé a estas tecnologías, así como a su incidencia en la justicia penal.

B. Implicaciones éticas en la emisión de sentencias La aplicación de IA en las sentencias conlleva importantes implicaciones éticas:

- Imparcialidad: Garantizar que los sistemas de IA, no produzcan los prejuicios que actualmente forman parte del sistema de justicia, y que las decisiones se tomen de una manera imparcial y equitativa.
- Derecho a la defensa: Garantizar que la utilización de la IA, no implique un resultado negativo para el derecho de los acusados a defenderse adecuadamente en la tramitación del proceso.
- Confidencialidad y protección de datos: Garantizar el carácter de confidencialidad y el tratamiento seguro de los datos personales y de información sensible. En otro

sentido, habrá que tener en cuenta la necesidad de poner de resguardo la autonomía del juez, así como el carácter humano de la motivación de las decisiones, aunque se aluda a la utilización de herramientas algorítmicas de soporte. La utilización de la IA no puede sustituir la tarea comparativa del juez, ni el sentido jurídico contextualizado que requieren cada uno de los casos concretos. Un excesivo desentendimiento del proceso decisorio, a partir de sistemas automatizados, podría llevar en el extremo al vaciamiento de la función jurídica y a la descomposición de la legitimidad democrática del sistema penal. Por ello, es indispensable que cualquier recomendación generada por IA sea revisada, contrastada y fundamentada por un operador jurídico, garantizando que las sentencias respondan a criterios normativos y no únicamente a patrones estadísticos o probabilísticos.

Marco regulatorio internacional y nacional

En cuanto a lo internacional, debo señalar que, un objetivo de la Asamblea General de las Naciones Unidas es prevenir que se vulnere el goce de los derechos humanos en razón de la inteligencia artificial y por otra parte, que se utilice para el beneficio de los hombres. El 21 de marzo de 2024 la Asamblea General de las Naciones Unidas aprobó por aclamación una histórica resolución sobre promoción de sistemas de inteligencia artificial seguros, protegidos y fiables. Esta resolución marca un hito en la regulación mundial de la inteligencia artificial (IA). Seguidamente se hace un análisis de la resolución que indica la necesidad de regular la IA para, por una parte, evitar vulneraciones a derechos humanos como la discriminación y afectación a la privacidad y debido proceso y, por otra parte, asegurar que esta tecnología sea utilizada en beneficio de los hombres. La inteligencia artificial forma parte de la conversación pública. Prácticamente no hay área que no sea ajena a la inteligencia artificial. Por ejemplo, el ejercicio del derecho se ve influido por los sistemas basados en IA. Son comunes los ejemplos del uso de ChatGPT en la función judicial. Hay algunos poderes judiciales que empiezan a dotarse de inteligencia artificial en su cotidianidad como ocurre con Prometea en Argentina y PretorIA en Colombia. Por eso hay diversos esfuerzos de reglamentación del uso de la IA por actores públicos y privados. El documento vinculante más importante sobre el tema es la Ley de la Inteligencia Artificial de la Unión Europea (Ley de IA). La Ley de IA tiene como prioridad la de asegurar que los sistemas de IA sean seguros, transparentes, auditables, no discriminatorios y que respeten el medio ambiente. Asimismo, deben ser auditados por humanos. Un aporte central de la legislación europea es la de establecer diferentes niveles de riesgo de los sistemas de IA. En el nivel de mayor riesgo (riesgo inaceptable), se incluyen los sistemas de puntuación social y reconocimiento facial en tiempo real y a distancia. (Olivares, 2024). En esa atmósfera se produjo la resolución de la ONU que reconoce el avance vertiginoso de la IA y su

impacto potencial de aceleración de los Objetivos de Desarrollo Sostenible (ODS). En la misma línea, destacan los riesgos que pueden surgir de su uso indebido o malicioso, lo que podría dificultar el avance de estas acciones y perpetuar la desigualdad y el sesgo estructural, así como la discriminación. El organismo urdido insiste en la necesidad de un consenso mundial sobre sistemas de IA seguros, protegidos y fiables, fomentando la cooperación internacional inclusiva y la aplicación de marcos normativos mundiales. La IA, como toda tecnología, tiene potencialidades y riesgos, y de ahí que la Resolución de la ONU propugne la existencia de marcos de gobernanza y de regulación estatales que contemple y promueva innovación y inversión responsable en sistemas de IA seguros, protegidos y fiables. Esta regulación, en el sentido indicado por la ONU, debe incorporar, entre otras cosas, promoción de una mayor comprensión por parte de la opinión pública en lo que respecta al funcionamiento de la IA; sistemas de protección de la privacidad y de los datos de carácter personal; medidas de salvaguarda para dar protección a la seguridad de los sistemas de IA; evaluaciones de riesgo y de impacto; procedimientos de retroalimentación, y medidas para detección y corrección de las vulnerabilidades, de los resultados sesgados o discriminatorios, así como de aplicación de medidas de salvaguardia que respeten la propiedad intelectual, incluidos los derechos de autor. En este sentido, la Resolución incita a los Estados Miembros la «búsqueda de un equilibrio, y a abordar los posibles beneficios y los riesgos correspondientes a la funcionalidad de los sistemas de inteligencia artificial.» (Abel Souto, 2024). Desde el punto de vista de los derechos humanos, la Resolución subraya que los sistemas de IA han de ser centrados en las personas, éticos, inclusivos y respetuosos en la integralidad de la promoción y protección de los derechos humanos y el derecho internacional. Manifiesta que un uso indebido de la IA puede llevar a socavar los derechos humanos privadas, afianzar los sesgos estructurales, y aumentar la discriminación. Por lo que aumenta a los Estados Miembros la necesidad de la no utilización de sistemas de IA que no puedan funcionar conforme al derecho internacional o que entrañen riesgos indebidos a los derechos humanos. Uno de los riesgos más importantes de la IA se encuentra en su capacidad de perpetuación y potenciación de la discriminación.

La resolución llama a los Estados miembros y a otros interesados a crear marcos normativos que contemplen medidas de salvaguarda contra la discriminación y el sesgo de los algoritmos. Esto implica, además: analizar y mitigar el sesgo que contiene los conjuntos de datos, así como luchar contra la discriminación relacionada con algoritmos. Además, la resolución promueve la diversidad lingüística y cultural de los datos que se emplean para entrenar los sistemas de inteligencia artificial. La resolución llama la atención sobre la importancia de cerrar la brecha digital entre los países y dentro de los países. Asimismo, llama a los Estados a que cooperen con los países en desarrollo

para garantizar un acceso inclusivo y equitativo a los beneficios de la transformación digital y de los sistemas de inteligencia artificial, lo cual incluye la mejora de la conectividad de la infraestructura digital y la promoción de la alfabetización digital. La resolución reconoce, además, que existe una brecha digital en materia de género por lo que llama a los Estados miembros a que adopten medidas específicas para cerrar la brecha digital de género. Por lo tanto, llama a que “se incluya una perspectiva que contemple las cuestiones de discapacidad, de género y de igualdad racial en la evaluación de las decisiones políticas y de los marcos que las orienten” cuando se emplean los sistemas de inteligencia artificial. Asimismo, llama a que se promueva la supervisión humana del funcionamiento de los sistemas basados en inteligencia artificial mediante la evaluación de las decisiones automatizadas. Y, además, se promoverá que existan los medios de reparación y de rendición de cuentas para quienes se vean perjudicados por decisiones automáticas. Sin duda, también alienta a que los Estados desarrollen instrumentos como las marcas de agua, o el etiquetado que indique a los usuarios el origen del contenido digital auténtico, del contenido generado por inteligencia artificial o manipulado. A nivel europeo, se han realizado avances significativos para abordar la discriminación algorítmica y proteger los derechos y libertades en el marco de la IA. La Unión Europea (UE) ha implementado regulaciones y marcos legales que buscan abordar esta problemática, como el Reglamento General de Protección de Datos (RGPD), establece principios para el tratamiento de datos privados de las personas, incluyendo el derecho de explicación de decisiones automatizadas que afecten a las personas, y el Reglamento de la inteligencia artificial aprobado recientemente a finales del 2023 por el Consejo y el Parlamento europeo, sin embargo, su vigencia y entrada en vigor será en el 2026. (Ayuso, 2023)

Estas normativas establecen principios para el manejo de información personal y prohíben el trato desigual en varios sectores sociales incluyendo la discriminación basada en algoritmos. Además, países como Alemania y Reino Unido, han desarrollado estrategias nacionales específicas para regular el uso de algoritmos y garantizar la protección de los derechos humanos en la actualidad. En Estados Unidos de América, se han generado varias discusiones sobre la regulación a la inteligencia artificial, es así que, desde el año 2016, durante la presidencia de Obama, comenzaron a regular los riesgos de la IA, con varias investigaciones que prosigan con el desarrollo de esta, pero con pocas restricciones. Para el año 2022, de la mano del actual presidente Joe Biden, oficializó la nueva Declaración de Derechos de la IA, que busca 5 protecciones para los ciudadanos estadounidenses en el apogeo de la IA, la primera, sistemas seguros y efectivos; la segunda, protección contra la discriminación algorítmica; la tercera, privacidad de datos; la cuarta, aviso y explicación; y la quinta, alternativas humanas, consideración y respaldo. (The White House Washington, 2022)

En América Latina, varios países han comenzado a reconocer y abordar la discriminación algorítmica y sus efectos en los derechos, pero en cierto modo no existe una normativa regional que regule la inteligencia artificial y sus efectos. Sin embargo, en algunos países, como Brasil, a mediados del segundo semestre del 2021, la Cámara de Legisladores aprobó la iniciativa de ley que regularía a la inteligencia artificial, en beneficio de regulación de la evolución y uso de la IA en campos de la salud, ética, justicia, igualdad y rendición de cuentas. Además, evita la toma de decisiones y soluciones discriminatorias por algoritmos, respetando los derechos humanos de la colectividad y de grupos diversos y multiétnicos de Brasil. (Câmara dos deputados, 2021)

Costa Rica, país centroamericano, ya mantiene discusiones sobre su proyecto de ley de un marco regulatorio a la inteligencia artificial, con el fin de regular su uso, desarrollo e implementación en aquel país. Además, esta ley se enfoca esencialmente en la protección de los derechos humanos. Estos esfuerzos muestran un progreso en la región para salvaguardar los derechos humanos ante la incidencia algorítmica de la inteligencia artificial. En Ecuador, la desigual digital, especialmente el sesgo de la inteligencia artificial, plantea desafíos particulares en términos de defensa de los derechos humanos. Si bien el país cuenta con una Constitución que establece principios de igualdad y trato justo, sin embargo, no existe normativa subyacente donde se aborda específicamente la discriminación algorítmica y regulación a la inteligencia artificial, y mucho menos una iniciativa legal que describa indicadores para su regulación y prevención contra la discriminación algorítmica el impacto de la inteligencia artificial en los derechos fundamentales consagrados en la Constitución de la República de 2008. Los proyectos de inteligencia artificial a nivel de Ecuador son incipientes. El diagnóstico sobre el estado de la tecnología hecho por el Ministerio de Telecomunicaciones en el año 2021, muestra que las iniciativas de inteligencia artificial se han generado sobre todo desde el sector privado (Ministerio de Telecomunicaciones y Sociedad de la Información, 2021). Las principales actividades que se generan en los mismos, por fuerza se concentran en la atención al cliente y en la disminución del fraude, lo que da una idea del estado incipiente de la inteligencia artificial en el Ecuador (Albornoz, 2023). Esta situación obliga a especular sobre los efectos que la inteligencia artificial tendrá sobre los derechos fundamentales, por lo que estas reflexiones deben ser entendidas como una especificación de un futuro que no es inmediato. El efecto, en último término, dependerá de la calidad de los datos con que estos sistemas se programen, su diseño algorítmico y sus interacciones complejas que pueden traer consecuencias imprevistas (Raso et al., 2018). Los efectos de la inteligencia artificial sobre los derechos fundamentales en el Ecuador pueden graduarse según provengan del desarrollo de esta tecnología o de su (in)utilización. (Aguado, Núms. 16 y 17, marzo de 2019-febrero 2020). La primera forma hace referencia a las situaciones externas en donde el diseño o calidad de los datos están afectando el normal ejercicio

de los derechos de una persona. La segunda forma de afectación se asienta sobre datos de hecho como por ejemplo la imposibilidad (multicausal) de las personas de utilizarse y beneficiarse de esta tecnología, lo que los encuentra en una situación de desventaja. Estos problemas serán analizados en los siguientes párrafos.

3.1 Riesgos en el desarrollo de la inteligencia artificial

Como se indicará en la parte 1, se necesita de la inteligencia artificial una gran cantidad de datos para su funcionamiento. El aprendizaje automático, por ejemplo, requiere de información de alta calidad, precisa y estructurada (Surden, 2019). En medio donde no hay datos suficientes o son de mala calidad, esta técnica computacional puede generar errores. En Ecuador, no existe la cultura de recolección ni almacenaje de datos, incluso ha habido incidentes donde datos de carácter personal de instituciones públicas y privadas han sido filtrados (Primicias, 2021). Este problema representa un riesgo actual y futuro sobre los derechos fundamentales, si es que no se mejoran las prácticas sobre el tratamiento de los datos.

Breve historia de las TICs y de la IA en Ecuador

La evolución de las Tecnologías de la Información y la Comunicación (TICs) en Ecuador ha sido un proceso gradual que ha acompañado las transformaciones tecnológicas globales, marcando hitos importantes en la modernización del Estado y en el desarrollo de servicios públicos y privados. Aunque la Inteligencia Artificial (IA) constituye una de las innovaciones más disruptivas de las últimas décadas, su incorporación en el contexto ecuatoriano no ha seguido un camino lineal ni ha estado respaldada por políticas públicas específicas en sus inicios. En lugar de ello, su presencia se ha dado de manera indirecta, a través de avances en telecomunicaciones, digitalización estatal y ampliación de infraestructura tecnológica.

Este recorrido histórico permite comprender cómo la IA comienza a cobrar relevancia en Ecuador a partir de mejoras sustanciales en conectividad, informatización institucional y adopción de sistemas automatizados en distintas áreas del sector público. Si bien no existía inicialmente un marco regulatorio definido para su uso, los primeros acercamientos a esta tecnología se manifestaron en proyectos de modernización administrativa, plataformas de gestión documental y sistemas informáticos orientados a agilizar procesos estatales.

A medida que el país fue integrándose a la economía digital global, surgió la necesidad de fortalecer la gobernanza tecnológica y de reflexionar sobre el rol que herramientas como la IA pueden desempeñar en áreas sensibles como la justicia, la seguridad y la administración pública. Este panorama permite situar el punto de partida histórico desde el cual Ecuador comienza a transitar hacia un ecosistema digital más estructurado y consciente del impacto social, ético y jurídico de las nuevas tecnologías. Hasta el momento en Ecuador, no se ha elaborado una planificación ni

legislación específica sobre IA. Sin embargo, a la largo de la historia se he hecho alusión a esta tecnología en la gestión del sector de las telecomunicaciones.

Tabla 10.

Historia de las TICs en Ecuador

Periodo	Política Pública	Legislación	Otros
Primer periodo: Primeros pasos (90' - 2007)	- Agenda de Conectividad del Ecuador (2002)	- Ley Especial de Telecomunicaciones (1992)- Ley de Comercio Electrónico (2002)- Constitución del Ecuador (1998)	- Creación de la Superintendencia de Telecomunicaciones (1992)
Segundo Período: Auge de la Planificación (2008-2017)	- Plan Nacional para el Buen Vivir (2009)- Estrategia Ecuador Digital 2.0 (2011) - Plan Estratégico de Investigación, Desarrollo e Innovación para las TICs (2014) - Plan Nacional de Telecomunicaciones y Tecnologías de Información 2016-2021 (2016)	- Constitución del Ecuador (2008)- Ley Orgánica de Telecomunicaciones (2015)	- Creación del Ministerio de Telecomunicaciones (2009)- Implementación de primeros Infocentros (2010)- Creación de la Agencia de Regulación y Control de las Telecomunicaciones (2015)
Tercer Período: Planificación sin resultados (2018 – actualidad)	- Plan Nacional de Servicio Universal 2018-2021 (2018)- Plan Nacional de Gobierno Electrónico (2018)- Política Ecuador Digital (2019)- Plan Nacional de Servicio Universal 2022-2025 (2021)- Agenda Digital 2021-2022 (2021)- Agenda Digital 2022-2025 (2022)- Estrategia Nacional de Ciberseguridad (2022)	- Ley de Protección de Datos Personales (2021)- Ley Orgánica para el Desarrollo y Control de los Servicios Financieros Tecnológicos (2022)- Ley Orgánica para la Transformación Digital y Audiovisual (2023)	- Concesión a Galápagos Cable Systems para el tendido del cable submarino de Galápagos (2021)- Diagnóstico de la IA en Ecuador por el MINTEL (2021)- Gobierno retoma negociaciones de contratos celulares (2023)

Nota: Elaboración propia a partir de documentos oficiales de política pública, normativa tecnológica y reportes institucionales del MINTEL (2000–2023).

La revisión histórica nos indica que la gestión de las Tics es una preocupación nacional desde los años noventa. Sin embargo, no ha habido un plan a largo plazo por encima de los gobiernos que existieron. Durante el primer período que inicia con la Promulgación de la Ley Especial de Telecomunicaciones, el fin último de la política pública y de la legislación era regular el uso del espectro radioeléctrico y aumentar el acceso a internet mediante infraestructura (Jurado, 2006). Este período es un resumen de la paradoja que han descubierto Basabe et al. (2010). A la par de la recuperación que aparece en los índices económicos, después de la crisis de 1999, la política pública, así como la democracia, se erosiona en simultáneo. El segundo período comienza con la llegada de

la revolución ciudadana. En este período se expiden varios planes nacionales y se crea un ministerio que los ejecute. La mejora en los índices sociales en relación con las Tics es evidente, ya que, a diferencia de los gobiernos anteriores, el régimen del presidente Correa, ha puesto mayor empeño en la planificación del sector. Una de las políticas públicas más importantes fue la puesta en marcha de los Infocentro (especie de espacios tecnológicos que provee de internet y capacitación digital gratuito) los que representaron una reducción a la brecha digital en el sector rural (Acuña, 2017). Posteriormente, el tercer período comienza con la terminación del período del presidente Correa y continúa con los gobiernos subsiguientes hasta la actualidad. En este período la llegada del COVID-19 y la alta demanda de medios y capacitación tecnológica hace que las administraciones tengan que retomar la planificación en el sector de telecomunicaciones. En el período post- COVID, se expide una normativa y la puesta en marcha de planes emblemáticos como la Ley de Protección de Datos Personales y la Política Ecuador Digital. Sin embargo, esta última ha sido criticada, por no haber producido ningún resultado significativo (Primicias, 2021). En la Agenda Digital del 2022 se estableció como objetivo el haber desarrollado un diagnóstico sobre la IA en Ecuador, lo que fue cumplido en diciembre de ese año. Según el propio Ministerio de Telecomunicaciones, esto es el primer paso para la elaboración de la Estrategia Nacional de Inteligencia Artificial del país. En resumen, el objetivo de ampliar el acceso a las TICS y reducir la brecha digital, establecido desde hace más de 30 años, no se ha cumplido hasta el momento. El objetivo común de los planes nacionales en los diferentes periodos ha sido dotar de acceso a internet a todos los sectores de la población. El Estado ecuatoriano incapaz de cumplir con este compromiso básico, ha olvidado mirar otras necesidades tecnológicas del país. Esta circunstancia ha producido un desarrollo atomizado y desarticulado de los proyectos de IA y paralelamente, que los diferentes sectores sociales demanden al gobierno nacional la formulación de políticas para no recibir efectos negativos, sino para aprovechar los beneficios de estas nuevas tecnologías en un futuro. (Registro Oficial 557, 2022) Los riesgos para la afirmación de los derechos fundamentales, también serán evidentes cuando no exista suficiente información acerca de un determinado grupo de personas. Por ejemplo, en el caso de otorgar créditos, se están aplicando sistemas de IA que consideran diferentes variables, a fin de (cuantitativamente) determinar cuál es la probabilidad que tiene un crédito de ser pagado. Si por ejemplo, en el sistema, la variable que más influye para decidir a quién se le puede otorgar crédito (más aún se tiene en cuenta la afiliación al seguro social), el 20% de personas en condición de subempleo en el país, se verían desfavorecidas, pues no forman parte de esta institución. ((INEC, s.f.). En conclusión, los grupos históricamente marginados, cómo la población rural e indígena, podrían ver vulnerados sus derechos económicos al ser víctima de los prejuicios (concepto que ha sido explicado en la Sección 1) de los programadores. En resumen, en

Ecuador las personas más propensas a ver vulnerados sus derechos son las históricamente discriminadas. Los que están a cargo del diseño y desarrollo de los Sistemas de IA tienen un rol fundamental en la detección de posibles prejuicios que pudieran originar vulneración de sus derechos. Las previsiones constitucionales, que tienen referencia a la implementación de medidas de acción afirmativa para asegurar la participación de los sectores discriminados y de atención prioritaria, deben ser principios rectores de los programas de IA. Finalmente, todos los proyectos de IA que existan en el país deben ser sistemas expertos preparados en derecho constitucional y en derechos humanos. El riesgo de la utilización de la IA La gente sencilla, y en general la que no tenga la pericia que exige la utilización de las herramientas de IA, encontraran en algún momento que estan en desventaja frente a otros. Esto puede resultar un peligro de los derechos fundamentales de dichas personas. La inutilidad puede producirse por causas múltiples, puede ser natural como lo es la vejes o la incapacidad de la persona, o puede provenir de un elemento ajeno como es la desigualdad que existe en el acceso a las TICs. En Ecuador, -según datos oficiales del INEC del 2023-, el 44% de los hogares acceden al Internet y aproximadamente un 20% de las personas de 15 años hasta los 49 son analfabetos digitales. En la mencionada situación social, puede que la IA haga mayor la ya existente desigualdad económica en ser solamente quienes tengan la herramienta o tecnología de esta inteligencia artificial, y los que los puedan entender y laboralmente adaptarse, los que saquen provecho de las ventajas que tales herramientas representen. Dicha situación acarrearía que una gran parte de la sociedad, quede alejada marginalmente del aprovechamiento económico que le puede traer la IA, pues verán vulnerados sus derechos a la igualdad y a la no-discriminación. Por otro lado y como elemento de riesgo de utilización debe verse el mal uso que se le pueda dar a estas herramientas que son de IA. Cuidado especial debe ser el uso que se le dará a la IA para el aprovechamiento de las ciudades inteligentes (smart cities) El hecho, o bien el uso de los sistemas de inteligencia, que tiene que ser visto en este sentido. En general uno de los elementos principales de las ciudades inteligentes, son los sistemas que existen de vigilancia. Se ha documentado de manera amplia el mal uso que se le pueda dar a este tipo de herramientas. Así, el New York Times en 2019 hizo una investigación en donde se demostró que en el ECU 911 se estaban utilizando cámaras y que con el auxilio de sistemas de IA se se'guía a una serie de opositores políticos en el gobierno del presidente Correa. Esta situación no solamente atenta a la privacidad sino que esta vulnerando derechos de la especie políticos, y también el derecho a la huelga, de acuerdo a la Constitución estatal vigente. Finalmente la utilización de IA ha llevado a generar hasta el momento un debate en el ámbito académico en cuanto a la problemática del futuro del trabajo y de los segmentos laborales. La presunción que la IA sí llega puede reemplazar a la más elevada parte de trabajadores que existen en el mundo, ha producido una inquietud muy grande en los

investigadores. El sustento de los individuos que realicen labores fáciles de reemplazar mediante sistemas de IA, es un punto central en esta discusión. Muchos son los que a nivel internacional discuten sobre la conveniencia de que se adopten medidas de estas características como la del salario mínimo universal como un sistema de prevención. Este inconveniente nos afectará en un futuro a los ecuatorianos, motivo por el cual es conveniente que se empiecen a mover los hilos de acción y se genere una serie de espacios de diálogo, donde se analicen alternativas que eviten que queden desprovistos los derechos laborales. (Enríquez, 2019). A lo largo de la historia del Ecuador, los derechos contemplados en la Constitución no han sido tutelados, no existiendo en realidad la forma de poder obtener la posible tutela de los mismos, por no tener los instrumentos de defensa que se presentan. Es decir, no existía la forma de hacerlos efectivos y de llevar a cabo la acción respectiva en caso de perjuicio. La Constitución del 2008 produjo un giro radical a esto, al señalar la existencia de las garantías de distinta naturaleza, para la protección y promoción del ejercicio de los derechos fundamentales de los hombres. Estas garantías se descomponen en: garantías normativas; de políticas públicas, servicios públicos, participación ciudadana; y garantías jurisdiccionales. Dentro de los cuales, se darán unas sugerencias brevemente sobre la IA.

4.1. Políticas públicas: Estrategia Nacional de IA del Ecuador. Como ya se ha mencionado en la sección 2, en la Agenda Digital del 2022 se establece como meta un diagnóstico sobre el estado de la IA en el Ecuador, el cual ha sido cumplido en diciembre de este año. (Ávila Santamaría, 2012). El objetivo final del diagnóstico es que se formule una Estrategia Nacional que promueva el desarrollo de esta tecnología, cuidando a su vez los derechos de las personas. De acuerdo a lo analizado en este artículo hay ciertos elementos que deben tomarse en cuenta por la forma de poderse formular esta Estrategia. Uno de estos elementos está en que la política debe tener a mano la realidad sociohistórica de nuestro país, para evadir los errores que en el mismo se han cometido, tal y cual ocurrió en el pasado. La Estrategia deberá ingresar en las contradichas que por el desaparecido cumplimiento de las promesas de la vinculación quedan, que son las que tienen que ver con el acceso universal a las TICs, que deberán mantenerse siempre como uno de los principales objetivos. La suerte del plan de IA depende en mucho de la solución que se dé oportunamente al problema de la brecha digital. Por último, todos los proyectos de IA que existan en el país deberán ser sistemas expertos que se han alimentado en derecho constitucional y en derechos humanos. El riesgo que corre el sector que utiliza IA La gente simple y en general que no tenga la capacidad de utilizar las herramientas de IA verá que está en desventaja frente a otros. Esto puede ser un peligro para los derechos fundamentales de esos seres humanos. No están dadas las razones que pueden producir la incapacidad, pueden ser naturales como puede ser una avanzada edad o una incapacidad del mismo ser humano, o puede ser un factor externo como puede ser la desigualdad que existe en

el acceso a las TICs. En el Ecuador, según datos oficiales del INEC del año de 2023, solo el 44 % de hogares tiene acceso a la internet, y aproximadamente el 20 % de las personas de 15 a 49 años son analfabetos digitales. En la situación social antes mencionada puede ser que la IA aumente la ya existente desigualdad económica que habrá en el uso de la inteligencia artificial, porque serán solo los que tengan la herramienta o tecnología de esta inteligencia artificial, más las personas que puedan entenderla y laboralmente adaptarse para tener la ganancia que representa el uso de estas herramientas. Dicha situación acarreará que una gran parte de la sociedad quede fuera del provecho económico que el uso de la IA puede acarrearles, por que quedarán vulnerados sus derechos a la desigualdad y a la no-discriminación. Por otra parte, y como parte del riesgo de utilización debe también verse el mal uso que se le pueda dar a estas herramientas que están basadas en IA. Mucho cuidado habrá de prestarse al uso que se le pudiese dar a la IA para el desarrollo de las llamadas smart cities. O el hecho, o el uso que se le va dar a los sistemas de inteligencia de la IA habrá de verse en este sentido. Generalmente uno de los elementos primordiales dentro de las ciudades inteligentes son los sistemas que existen de vigilancia. Se ha informado profusamente sobre malos usos de estas herramientas. Así, el New York Times en el 2019 realizó una investigación donde se demostró que en el ECU 911 se empleaba cámaras y que con la ayuda de sistemas de IA se tenía bajo la vigilancia a una serie de opositores políticos al gobierno del presidente Correa. Esta situación no sólo vulnera la privacidad, sino que también afecta a derechos de carácter político y también al derecho a la huelga, según la Constitución vigente. Finalmente, la utilización de la IA ha creado además un debate hasta el momento en la parte académica en lo que a cuestión del futuro del trabajo o de los sectores de trabajo se refiere. La presunción que la IA si llega puede sustituir a la mayor parte de los trabajadores que existen en el mundo, ha creado una inquietud de gran relevancia en los investigadores. El sustento de los individuos que desempeñen tareas fácilmente sustituidas a través de los sistemas de IA, es un tema que resulta relevante dentro de esta discusión. Muchos comentan sobre la conveniencia que a nivel internacional se den pasos para adoptar medidas de esta naturaleza como el del salario mínimo universal como un sistema preventivo. Este inconveniente nos va a afectar en el futuro a los ecuatorianos, por lo que resulta conveniente que se empiecen a generar espacios de diálogos, donde se analicen alternativas que eviten que se vean desprotegidos los derechos laborales. (Enríque, 2019). A lo largo de la historia del Ecuador, los derechos que se encuentran dentro de la Constitución no han sido tutelados, no existiendo en realidad la forma de poder la posible tutela de los derechos, por no tener los mecanismos de protección que se plantean. Es decir, no se encontraba el medio de hacerlos efectivos y presionar su actuación, en caso de perjuicio. La Constitución del 2008 dio un cambio radical a esto, al señalar la existencia de las garantías de distinta naturaleza, para la protección y promoción del ejercicio de

los derechos fundamentales de las personas. Estas garantías se descomponen en garantías normativas; de políticas públicas, de servicios públicos, de participación ciudadana; y garantías jurisdiccionales. Dentro de lo cual, se formularán brevemente unas recomendaciones referentes a la IA.

En suma, no se debe esperar el desarrollo de sistemas complejos e innovadores de inteligencia artificial sin dotar antes a la ciudadanía de conocimientos y herramientas digitales suficientes. Para el desarrollo de esta estrategia también deberá plantearse la posibilidad de incentivos para investigación de los posibles usos que tendrá dicha IA en el país. Los escasos estudios que se han realizado no han determinado de forma exacta en que forma el Ecuador se puede beneficiar de la tecnología en un futuro. El financiamiento de investigaciones que se están realizando en el Laboratorio de Investigación en Inteligencia Artificial Industrial (INARI) de la Escuela Politécnica del Litoral (ESPOL) debe ser uno de los primeros objetivos que se plantee dentro de la estrategia. Los sectores en los que se puede hacer mayor uso de la IA, son los de hidrocarburos, minería, agricultura, acuicultura y producción pesquera. Todos ellos constituyen un gran campo de aplicación, con el objeto de crear sistemas de IA que logren mejorar su productividad y rendimiento económico en beneficio del país. Deben también pensarse las capacidades y competencias que tiene el Ministerio de Telecomunicaciones, que debe utilizarse en el futuro en la elaboración de la Estrategia de la IA. Este Ministerio ha velado históricamente por el desarrollo de planes relacionados con la ampliación de acceso a internet y los demás servicios tecnológicos por lo que deberá ser una posibilidad la creación de una nueva secretaría o de un nuevo Ministerio que analice dicha estrategia, considerando que esta política pública necesita de una mayor asignación de recursos y que por lo tanto habrá de discutirse su configuración en el presupuesto general del Estado en los organismos técnicos correspondientes, para lograr los beneficios que contiene la IA. (Ia, 2022) Resulta impostergable que el Ecuador dicte una legislación específica que regule la IA a efectos de estimular su desarrollo y proteger los derechos de sus ciudadanos. (Banco de Desarrollo de América Latina, 2021). Esta ley debe hacerse teniendo en cuenta las disposiciones ya planteadas en la Ley de Protección de Datos Personales con el objeto de evitar contradicciones y sobrerregulación. (Comercio, s.f.) Resulta la legislación de IA por tipo de riesgos (concepto expuesto en la Sección I) la mejor manera de afrontar esta nueva problemática tecnológica. Sin embargo, al ser una nueva norma en la Unión Europea, sus efectos todavía no son perceptibles, por lo que el aumento a la investigación y la innovación será el objetivo principal de la futura ley, según la realidad social del país. Podrían también analizarse otras formas de regulación basada solamente en normas técnicas dictadas por una determinada entidad estatal. Por ejemplo, en esta concepción, la Agencia Nacional de Regulación y Control Sanitaria (ARCSA) regularía todos los

sistemas de IA aplicados al sector alimenticio, aplicando normas técnicas propias, y acordes a la ley en general y al sector agropecuario en particular. Así nacen los principios que empleará el juez en el control de las actuaciones de la IA. En tres aspectos, según la realidad social del país, el aumento a la investigación y la innovación será la finalidad esencial de la futura ley, a la cual, además de la norma urdida, deberán entrar el órgano legislativo y los demás actores políticos, al igual que en el caso anterior, a contemplar todas las posibilidades de cualquiera tipo (sistema jurídico, operatividad del sistema en el futuro) de modo que se cumpla dicho objetivo. Garantía jurisdiccional: Principio de proporcionalidad como método de interpretación de la norma constitucional y Acción de habeas data cultural. Propuesta, si hay una vulneración de derechos fundamentales a una persona, provocado por la IA, el juez constitucional producirá el uso del principio de proporcionalidad en el acto en que decida el futuro del sistema. Propuesta ya analizada por Restrepo y Baquero (2023), que al respecto indica que los requerimientos de idoneidad, necesidad y proporcionalidad en stricto sensu, deberán ser valorados, para que la decisión del juez sea más ecuánime en caso de que se requiere pronunciarse sobre la existencia de una sanción. Ejemplo: Si se quiere desactivar un sistema de vigilancia de IA, porque está programado para espiar a una persona, el juez valorará si la desactivación es la medida más adecuada, para restituir el derecho a la privacidad (idoneidad) si no existe otro medio menos gravoso para el dueño del sistema (necesidad), y si su medida es proporcional al daño causado (proporcionalidad en stricto sensu). Con el principio de proporcionalidad, la acción jurisdiccional de habeas data es prometedora e importante para el amparo de determinados derechos relacionados con la privacidad y soberanía informática que pueden ser vulnerados por la IA, pero eso es materia de otro trabajo.

Por otro lado, es necesario indicar que el derecho penal, en tanto que rama del ordenamiento jurídico, tiene entre sus funciones propicias a las tres antes enunciadas, fijar, por un lado, conductas normativamente (en tal sentido, como ciencia, es una ciencia normativa), por otro, imputar delitos y exigir responsabilidad. Desde la perspectiva del derecho, pues no tiene otro objetivo que fijar pautas correctas de conducta o, en términos jurídicos, acordes con lo que prescriben las normas, de tal forma que los elementos (constitutivos), desde la perspectiva de protección de derechos o bienes jurídicos, con las limitaciones materiales y formales que la ciencia penal ha indicado, acudan a la creación de consecuencias jurídicas, sancionadoras o preventivas que han de ser impuestas cuando se infrinja la norma que establece la pauta de conducta o, dicho de otro modo, cuando la conducta que en el ámbito social ofrece el sujeto se aparte de la pauta de conducta preestablecida normativamente.

Con todas las salvedades que dicha exposición convierte en tan esquemática y focalizada, conviene recordar y resaltar precisamente estas funciones del derecho en general y del derecho penal como

ciencia, que son de trascendental importancia para el discurso en cuestión. Por un lado, porque en el caso de que los entes artificiales inteligentes, se relacionen con la sociedad o con las personas o cuando lo hagan, pueden, con el comportamiento, lesionar o poner en peligro bienes jurídicos, habrá que reflexionar sobre el segundo aspecto que antes ha sido enunciado: el de la exigencia de responsabilidad penal (en el sentido más amplio del término). Pero, por otro lado, en cuanto que ciencia (normativa), cuyo objeto son normas (jurídicas, pero normas), las aportaciones de la dogmática penal pueden ser muy bien utilizables en el ámbito de la tecnología.

Me explico: si los entes artificiales inteligentes actúan o realizan comportamientos con significación social, el comportamiento y la actuación habrán de adecuarse a las normas. Merece la pena indicar que esa adecuación de los comportamientos tiene sin embargo un doble aspecto, o mejor: comporta normas funcionalmente distintas. Así, y en el ámbito estrictamente tecnológico, será preciso fijar pautas de comportamiento que predeterminen lo que ha de hacer el ente artificial inteligente.

Estas (pautas), según las habilidades y estado de la técnica, funciones que se les encomiendan etc., pueden ser muy complejas y serán las que se incorporen a los programas informáticos como órdenes o instrucciones de actuación. En este sentido, se viene a decir que el software lleva un conjunto de instrucciones que permiten y (pre)determinan el comportamiento del agente (en todo caso, cuando el agente se trate de un agente inteligente, la predeterminación no podrá serlo). comportamientos de trascendencia social. (Aguado, Núms. 16 y 17, marzo de 2019-febrero de 2020). El análisis histórico que corresponde a este capítulo permite comprender que la administración de justicia en el Ecuador ha tenido profundos cambios, porque se ha hecho necesario modernizar sus estructuras institucionales, en atención a los principios de un Estado constitucional de derechos y de justicia. A raíz de la Constitución de 1998 a la de 2008, los cambios legislativos, han procurado fortalecer la transparencia, la eficiencia y la publicidad procesal, instaurando un sistema que aspira a ser más accesible y orientado al servicio del ciudadano. Sin embargo, estos cambios no han estado exentos de tensiones. La implementación de estas herramientas tecnológicas como el SATJE han permitido que aparezcan nuevas dinámicas en la automatización de la gestión judicial, pues permite que se sistematicen procesos, se acorten tiempos administrativos y a la vez se mejoren las formas de audiencia o de trazabilidad respecto a los expedientes. Sin embargo, persisten grandes dificultades en relación a la gestión documental, en la conservación de archivos y en cuanto al problema del acceso a la información judicial que está conservada indeterminadamente pues sobre tal mejora, se ha evidenciado que la progresiva digitalización de los mismos, han traído a la luz vacíos regulatorios importantes. La falta de lineamientos claros en relación a lo concerniente a los límites de la publicidad electrónica, tiempo de conservación de datos y responsabilidad en materia de la información sensible demuestra que la

modernización técnica no ha sido necesariamente así, respecto a una modernización normativamente integral. Ello genera un sin número de incertidumbres que pueden afectar derechos constitucionales como el de la intimidad, por ejemplo, el derecho a la autodeterminación informativa. El capítulo pone en evidencia que la transición a un sistema de justicia más ágil no puede desvincularse del fortalecimiento de los marcos legales que regulan la protección de datos, y de la gestión archivística. La relación tecnología, derecho-acceso a la información exige un tratamiento más equilibrado que permita visualizar tanto las positivas como las desventajas de la modernización y digitalización informativa, sobre todo en lo que respecta a la información judicial de carácter público. En consecuencia, este capítulo lo que retiene es que el proceso de modernización del sistema judicial ecuatoriano ha sufrido avances importantes, pero que debe consolidarse a través de políticas de gestión documental más fuertes, normas específicas sobre acceso y sobre conservación de datos.

Consolidación de capacidades institucionales y ecosistema de innovación en IA

Además de la expansión de infraestructura y la adopción de herramientas digitales en el sector público, un punto de inflexión en la trayectoria de las TICs y de la IA en Ecuador ha sido la construcción progresiva de capacidades institucionales para investigar, desarrollar e implementar soluciones basadas en datos. Este proceso se expresa en el fortalecimiento de unidades técnicas en el Estado, en el surgimiento de laboratorios y grupos de investigación en universidades, y en la incorporación gradual de perfiles especializados (analítica de datos, aprendizaje automático, ciberseguridad, ingeniería de software) en proyectos de modernización. En la práctica, esta consolidación ha permitido pasar de una lógica centrada únicamente en conectividad y equipamiento, hacia una lógica más compleja de gobernanza tecnológica, donde la gestión de datos, la interoperabilidad y la evaluación de riesgos se vuelven componentes indispensables.

En paralelo, se observa la emergencia de un ecosistema de innovación compuesto por academia, sector productivo y emprendimientos tecnológicos que buscan adaptar la IA a necesidades locales: productividad, servicios financieros, educación, salud, logística y seguridad.



RIESGOS Y DESAFÍOS DE LA INTELIGENCIA ARTIFICIAL EN LA JUSTICIA PENAL

Sesgos algorítmicos y discriminación

El aprendizaje no supervisado es aquel que no demanda de etiquetas por las respuestas, por lo que funciona como estructura del automercado, el cual consiste en que la máquina decide que datos pertenecen a una marca y el motivo por el cual no pertenece a la otra. De cualquier manera, el aprendizaje no supervisado puede dividirse en dos partes de las cuales una es el agrupamiento y la otra la asociación. La técnica de agrupamiento o agrupación permite separar los datos en grupos para identificar aquellos que tienen un comportamiento igual. En la técnica de agrupación se crean subgrupos para analizar el comportamiento de cada uno y obtener los patrones, permitiendo generalizar la conducta y dar recomendaciones en base a ello. Este mismo aprendizaje nos genera información para poder inferir sobre el comportamiento del consumidor en un trabajo necesario para el desarrollo del programa de mercadotecnia de la empresa. En la técnica de asociación, se crea competencia entre las funciones que manejan lo que el consumidor quiere, y adquiriendo estos mismos patrones se hace más sencillo para el comerciante identificar que el consumidor tiene el avata o peculiaridad de que requiere de cultura cada vez que va a comprar algún tipo de producto en especial los alimenticios. Este aprendizaje también puede usarse mucho en los comerciales en donde al ser un cliente habitual se le debe ofrecer un producto. Ahora bien, para el uso correcto de estos grupos en los programas de inteligencias artificiales, exige utilización de estructuras definidas en algoritmos, los cuales tienden a ser un poco difíciles de entender, por lo cual utilizando terminología que se maneja comúnmente en los grupos musicales se obtienen grandes resultados ya que primero se logra entender todos los componentes del tema que se desea. (Pastor 2023, pp. 8 -12), (Bobadilla, 2022). tras analizar y aprender de los datos, permiten realizar dichas predicciones. Los tipos de aprendizaje automático son: Aprendizaje supervisado. - El aprendizaje supervisado es

el aprendizaje en el que el algoritmo se nutre de datos dotados de una etiqueta que le da a conocer el resultado aprendido. En Derecho, el aprendizaje supervisado, las etiquetas son casos jurídicos previos, sentencias judiciales o documentos legales. Este modelo de aprendizaje estudia los patrones de entradas con decisiones judiciales, por tanto, permite realizar predicciones de decisiones judiciales a nuevos casos. Aprendizaje basado en reglas. - El aprendizaje basado en reglas consiste en formular reglas claras que reflejan los principios, razonamientos y normas jurídicas. Por lo cual este tipo de sistemas basas sus decisiones o consejos en normas. Aprendizaje no supervisado. - Como contraste, en el tipo de aprendizaje no supervisado, los datos se dan al algoritmo sin etiqueta desde el principio del aprendizaje, esto es, el algoritmo nunca adquiere un concepto de lo que representan los datos. La idea es que el algoritmo encuentre por sí mismo normas de entender el ser de datos. Aprendizaje por refuerzo. - Es aquel aprendizaje que el algoritmo adquiere el conocimiento por medio de la observancia de su entorno. La información aportada como entrada del mismo es la retroalimentación que obtiene del entorno y facultando a realizar sus acciones a comportamiento diferente en lo posteriormente, ya que el entorno responde a la acción que realiza, lo que provoca que el algoritmo se adapte a las modificaciones del entorno. Este tipo de aprendizaje se ha aplicado a un número muy variado de campos como en la elaboración de videojuegos, robótica y en sistemas de recomendación y control de procesos. En resumen, el sistema aprende por medio de la exploración y de la vivencia. Aprendizaje profundo. - El aprendizaje profundo o comúnmente dicho Deep Learning por su traducción en inglés, se vale del algoritmo de redes neuronales artificiales para aprender, comprender, razonar y manejar acciones complejas. Las redes neuronales algorítmicas que le competen son muy complicadas por la complejidad de estructuras de muchas capas intermedias entre los datos de entrada y los datos de salida. Este tipo de aprendizaje se caracteriza por tareas de visionado, entendimiento de lenguaje nacional, traducción automática y toma de decisiones.

Tabla 11.
Tipos de aprendizaje automático, su funcionamiento y riesgos de sesgo algorítmico

Tipo de aprendizaje automático	Cómo aprende	Ejemplos de uso	Riesgos típicos de sesgo algorítmico
Aprendizaje supervisado	Aprende a partir de datos etiquetados con la respuesta correcta.	Predicción de sentencias, clasificación de documentos jurídicos.	Sesgo heredado de decisiones judiciales históricas (raciales, de género, socioeconómicos).
Aprendizaje basado en reglas	Opera siguiendo reglas lógicas definidas por expertos.	Sistemas expertos legales, asesoría normativa.	Sesgo introducido por quienes diseñan las reglas (sesgo humano explícito).
Aprendizaje no supervisado	Encuentra patrones sin etiquetas previas.	Agrupación de perfiles, análisis de conducta delictiva.	Identificación sesgada de grupos “sospechosos” por correlaciones erróneas.

Aprendizaje por refuerzo	Aprende a partir de retroalimentación (premios o castigos).	Robótica, sistemas de control, asignación dinámica de recursos.	Reforzamiento de decisiones discriminatorias si el entorno ya está sesgado.
Aprendizaje profundo (Deep Learning)	Redes neuronales con múltiples capas que aprenden representaciones complejas.	Reconocimiento facial, lenguaje natural, vigilancia.	“Caja negra”: difícil explicar decisiones; muy propenso a sesgos invisibles.

Nota: Cada tipo de aprendizaje automático presenta ventajas operativas distintas, pero también riesgos específicos de sesgo que deben ser gestionados mediante controles técnicos, auditorías y supervisión jurídica adecuada.

El algoritmo se considera un algoritmo de caja blanca (white box) cuando la estructura interna y su proceso lógico-son totalmente transparentes y comprensibles en cuanto la comprensión del ser humano, (Zaptest). Es decir, se puede tener la capacidad para entender cómo se están tomando las decisiones y cuáles son los factores que influyen el balance del resultado. Se puede además tener la posibilidad de modificar y adaptar procesos y parámetros de la automatización del proceso de toma de decisiones dada por la inteligencia artificial, para suministrarnos mejores resultados, pues, el ser humano tiene la decisión final. (Seon, 2023). El algoritmo se considera un algoritmo de caja negra (*black box*) cuando la estructura interna y la forma cómo se toman las decisiones no es fácil de entender y mucho menos fácil de interpretar. Es decir, que el ser humano que está usando la información no va a conocer los datos de entrada y salida del sistema algorítmico, pero si tiene conocimiento del manejo de los datos que le suministran. Los sistemas de redes neuronales profundas son considerados como cajas negras debido a la complejidad de capas intermedias y dificultades de interpretación de manejo e interpretación de datos e información. Pero el sistema no se puede tener conocimiento de los sistemas internos de la IA con black box, porque no se puede tener conocimiento de su funcionamiento ni de las alteraciones a parámetros que se hacen, afectando evidentemente su transparencia. (Seon). Los sistemas de inteligencia artificial preparados o enfocados a tareas específicas del área legal dependen de requerimientos y especificaciones para la aplicación, además de la importancia de buscar y entender el razonamiento que está detrás de la toma de decisiones que hace el algoritmo, para su entendimiento. La interpretabilidad es esencial, sobre todo en los ambientes de decisiones justificadas, pudiendo ser estos en el área legal o médica. La discriminación algorítmica ocurre cuando los sistemas automáticos propician un trato desigual y sin justificación, o cuando afectan en forma negativa a las personas por su razón de raza, color de piel, origen étnico, género (cuando el embarazo, el parto y otras condiciones también médicas asociadas a dicha condición, orientación sexual), religión, edad, origen, discapacidad o categoría más, que sea resguardada por ley. Dependiendo de las circunstancias particulares se puede considerar que este tipo de discriminación algorítmica está infringiendo las protecciones de ley. (House) Podemos citar a Mercader (2021). quien dice que: La discriminación algorítmica se produce cuando un individuo o grupo recibe un trato injusto como resultado de decisiones

automatizadas. Este fenómeno se da porque los algoritmos se basan en datos que pueden estar sesgados y esto conduce a decisiones automatizadas también sesgadas o modificadas. Al hablar de la discriminación algorítmica y al abordarlo de una forma general, Cathy O'Neil comenta (2016) cómo los algoritmos impulsados y alimentados mediante el big data, contribuyen a la discriminación algorítmica aumentando así las desigualdades históricas de la sociedad. Indica que ciertos algoritmos en su aplicación como: la justicia, acceso a trabajos, contrataciones y otros ámbitos, siguen perpetuando las desigualdades sociales existentes. Como tan también la falta de transparencia en este fenómeno de decisiones algorítmicas, hace que no se puedan ver los sesgos discriminatorios que tienen al ser entrenadas para las decisiones automatizadas, las que a su vez tienen gran impacto en los individuos al ser discriminados socialmente y digitalmente. Por consiguiente, y teniendo en cuenta estos modelos de aprendizaje matemáticos, los individuos y cada persona humana que haya sobre la tierra, es considerado un número deshumanizado. Las 3 características de la desigualdad por parte de la inteligencia artificial y que recaen principalmente en lo opaco de su trabajo, es la falta de revelación de los desarrolladores responsables, al menos en cuanto al modelo de aprendizaje, entrenamiento y ejecución, lo mismo con los datos que se emplean para los modelos, y en la mayoría de los casos, lo que es mayormente sobre lo emitido por estos modelos automatizados por la IA, incluyendo la interpretación que es oscura. En segundo lugar, el daño que tienen sus actuaciones, ya que actúan de forma injusta. Es cierto que a pocas personas les podría beneficiar esta falla de la matriz del sistema de inteligencia artificial, pero la denigración y discriminación de ciertos sectores de la población se sigue dando, por lo que es inhumano anteponer el interés particular por el interés colectivo. La 3° y última característica de los mismos es la peligrosidad de su escala, su creciente poder y la administración y el olvido a la responsabilidad sobre este fenómeno, hará difícil su manejo, control y regulación.

Tabla 12.
Principales tipos de discriminación algorítmica y su origen técnico

Tipo de discriminación algorítmica	Descripción	Origen técnico del sesgo	Ejemplos comunes
Discriminación directa	El algoritmo utiliza explícitamente variables sensibles (raza, género, edad).	Datos etiquetados con características protegidas; reglas programadas.	Sistemas de crédito que penalizan por código postal o nacionalidad.
Discriminación indirecta	No usa variables sensibles, pero produce efectos adversos desproporcionados.	Variables proxy correlacionadas (barrio, nivel de ingresos, historial laboral).	Algoritmos laborales que excluyen a mujeres por brechas históricas.
Discriminación por datos sesgados	Resultado de entrenar con datos que ya contienen desigualdades.	Bases históricas incompletas o discriminatorias.	Reconocimiento facial con menor precisión en pieles oscuras.

Discriminación estructural automatizada	El algoritmo reproduce desigualdades sociales sin intención explícita.	Falta de representatividad, patrones sociales incorporados.	Motores de búsqueda que presentan estereotipos sobre mujeres o minorías.
Discriminación por opacidad (caja negra)	La falta de explicabilidad impide detectar decisiones injustas.	Deep learning con capas no interpretables.	Modelos predictivos policiales no auditables.
Discriminación por diseño	Algoritmo programado con criterios excluyentes.	Regla explícita o criterio técnico sesgado.	Filtrado de candidatos basado en “años sin interrupciones laborales”.

Nota: Los distintos tipos de discriminación algorítmica ilustran cómo decisiones automatizadas pueden reproducir o amplificar desigualdades sociales, lo que exige regulaciones estrictas, auditorías técnicas y salvaguardas para proteger los derechos fundamentales.

Situada en el terreno de los motores de búsqueda en línea, la discriminación algorítmica encuentra en Safiya Umoja Noble (2018) una de sus exponentes más citadas, quien sostiene que este fenómeno alimenta de forma continua la producción de sesgos, en la medida en que los algoritmos empleados habitualmente por Google, Bing y plataformas afines terminan amplificando y reforzando estereotipos de raza y género en sus resultados. La autora precisa además cómo determinados colectivos resultan sistemáticamente relegados o retratados de manera desfavorable en las páginas de resultados. Esa marginación repercute directamente sobre la visibilidad de comunidades enteras, cuya problemática rara vez recibe un tratamiento serio desde una óptica ética y social. Afrodescendientes y mujeres, colectivos históricamente discriminados, aparecen en las búsquedas web reducidos a rasgos que se les atribuyen como su condición esencial, casi definitoria. La inteligencia artificial, entrenada precisamente a partir de esos datos sesgados y ya desactualizados, perpetúa el ciclo (Abreu, 2013).

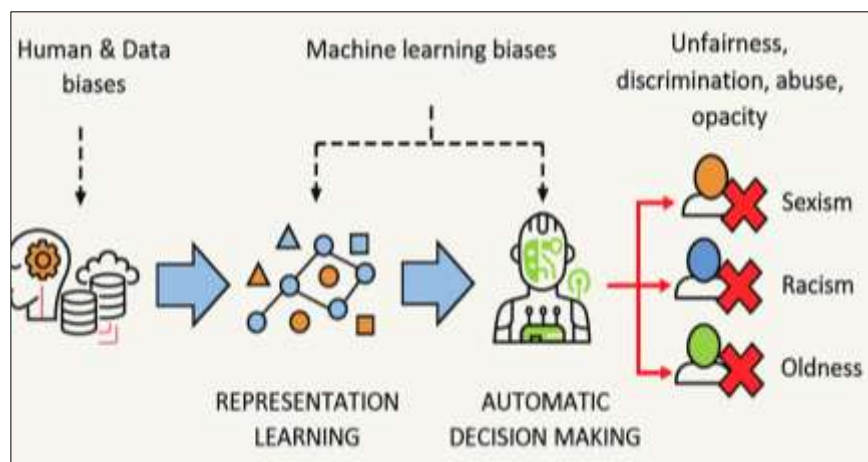
Desde otro ángulo, el del reconocimiento facial, Joy Buolamwini (2018), investigadora del MIT Media Lab y fundadora del Proyecto de Justicia Algorítmica, plantea que la discriminación algorítmica desborda el ámbito de las decisiones automatizadas y se instala también en estos sistemas de identificación visual. Su sesgo no es menor. Los mecanismos de reconocimiento facial exhiben resultados calificados como «imprecisos» al identificar a personas de piel oscura y a mujeres, mientras que responden con mayor exactitud frente a hombres de piel clara. La explicación remite, por un lado, a entrenamientos previos que carecieron de datos suficientemente específicos sobre tonalidades de piel y otros rasgos identitarios; por otro, a modelos de aprendizaje que, incluso disponiendo de esa información, no la incorporan de manera sistemática en su proceso continuo de ajuste.

La discriminación algorítmica designa, en su núcleo conceptual, aquellas situaciones donde los algoritmos adoptan decisiones que desembocan en tratos desiguales o injustos hacia personas o

colectivos determinados, a raíz de sesgos presentes en los datos de entrenamiento, en el diseño mismo del algoritmo y en los procesos que sustentan sus decisiones automatizadas. Nada de esto ocurre de forma aislada. Cada uno de estos factores retroalimenta la reproducción persistente de desigualdades, estigmatizaciones, estereotipos y prejuicios, extendiéndose a cualquier esfera social donde la tecnología logre insertarse, condición que en el mundo digital contemporáneo resulta ya prácticamente ineludible (Buolamwini, s.f.).

Figura 1.

Ejemplificación de la discriminación algorítmica



Nota: La figura muestra cómo los sesgos humanos y de datos pueden trasladarse a los algoritmos y producir decisiones automatizadas discriminatorias.

- Entonces, ¿cómo se produce realmente la discriminación algorítmica? Bueno, tal como explican Barocas y Selbst (2016) y Zuiderveen (2018) —citados por Eguíluz (2020)—, existen cinco formas sutiles en las que esto se manifiesta en los sistemas automatizados:
- ¿Cuál es el objetivo? Primero, el sistema determina qué intenta predecir o medir. Luego, clasifica los datos en categorías etiquetadas. El problema surge cuando esas categorías terminan marginando a ciertos grupos; básicamente, la propia configuración se convierte en una vía de entrada para el sesgo.
- Basura entra, basura sale: Si la IA se entrenó con datos sesgados, ¿adivina qué? Actuará con sesgo. El sistema no inventa prejuicios nuevos; simplemente replica los patrones injustos que ya estaban presentes en los datos con los que aprendió.
- ¿Quién creó el conjunto de datos? La IA aprende de decisiones humanas pasadas y, si esas decisiones estaban sesgadas (por ejemplo, favoreciendo a un grupo sobre otro), la IA perpetuará esa misma lógica desigual, especialmente cuando ciertos grupos apenas están representados.

- Elegir favoritos: Los sistemas utilizan rasgos específicos (como ingresos, código postal, etc.) y les asignan distintos pesos. Pero cuando esos rasgos benefician injustamente a unas personas sobre otras, el sistema deja de ser neutral: se trata de un sesgo codificado.
- El juego de las variables sustitutas (*proxy*): A veces, aunque no se utilice directamente un rasgo sensible (como la raza), el sistema se basa en algo estrechamente vinculado a él —como el barrio o el distrito escolar—, lo que termina excluyendo a las mismas personas, pero de manera indirecta.
- Discriminación deliberada: Sí, a veces es intencional. Los desarrolladores introducen sesgos a propósito, pero se escudan en términos como "algoritmo propietario" o "secreto comercial" para eludir responsabilidades. Astuto, ¿verdad?
- La discriminación algorítmica directa, se produce cuando de forma explícita y/o evidente el algoritmo con sus decisiones perjudica a determinados grupos de personas, por la inclusión en la toma de decisiones automatizadas de variables discriminatorias o sesgadas como la raza, religión, sexo, género, salud, discapacidad, etcétera, (Asquerino 2., sp).
- La discriminación algorítmica indirecta, se da cuando el algoritmo, aun no siendo su finalidad discriminar, sus resultados afectan de forma desproporcionada a grupos de personas determinados. En la mayoría de los casos este tipo de discriminación se produce por el sesgo de los datos de entrenamiento o bien en la selección de variables que correlacionan indirectamente con características protegidas, para la toma de decisiones, toda vez que no hay intención legítima de discriminar directamente. (Asquerino 2. p.).
- La definición de sesgo, ofrece la Real Academia Española que define como sesgo a una forma de error que podría producirse al realizar muestreos o ensayos, cuando se seleccionan o favorecen, determinadas respuestas frente a otras. Esto es, se define la inclinación explícita en forma de error ante una respuesta y no ante otras, incurriendo en el favorecimiento o en el desfavorecimiento en la toma de decisiones automatizadas. Para Carrero tal (2023), el sesgo nace de la parametrización de los parámetros del algoritmo, de tal forma que si estos parámetros no están bien parametrizados o se hallan desactualizados se producen resultados incomprensibles y perjudiciales. - El sesgo es, también, la desviación sistemática que imprime a la toma de decisiones o a la interpretación de información la que alejada de la imparcialidad debiera de tener, resulta que imprime a la mencionada información o decisión, inclinaciones previsibles que hace que resulte en trato desigual y en discriminación. Por lo que al fenómeno de la discriminación y de la discriminación algorítmica se predica el sesgo discriminatorio que va referida a las tendencias sistemáticas que resultan en trato desigual, injusto y discriminatorio a determinados grupos de personas.

Las definiciones y clase de sesgos en la discriminación algorítmica. Para Aguilar (2012), referencia los tipos de sesgos discriminatorios recurrentes e históricos, en la evolución continua del hombre, formulando los siguientes: (5.1.2.)

- Sesgo racial y étnico. – Supone la tención de decisiones automatizadas a través del algoritmo, basadas en la raza y etnicidad de la persona, perjudicando a los individuos de estos grupos a consecuencia de su pertenencia de origen y ascendencia.
- Sesgo de género. - Ocurre cuando la decisión algorítmica fue consecuencia del género de la persona provocando tratos desiguales e injustos por su identidad de género.
- Sesgo de edad. - Se presenta cuando el algoritmo toma decisiones en función de la edad de una persona provocando trato desigual y discriminatorio por la etapa de vida de la persona.
- Sesgo socioeconómico. - Es la tendencia del algoritmo a tomar decisiones en función del status socioeconómico de una persona que provoca diferencias de trato por su posición económica y social.
- Sesgo de orientación sexual. - Significa que el algoritmo. su decisión automatizada, se basa en la orientación sexual de la persona, provocando trato discriminatorio por su identidad sexual.
- Sesgo de discapacidad. Se presenta en la decisión del algoritmo relativa a la discapacidad de la persona provocando trato diferencial por sus posibilidades físicas o mentales.
- El sesgo religioso. - Es la decisión que se produce en función de la afiliación religiosa de una persona provocando un trato desigual y a la vez discriminatorio por sus creencias e inclinaciones religiosas. Todos estos sesgos discriminatorios pueden darse en diferentes ámbitos de la sociedad como el acceso al trabajo, a la medicina, la educación en todos los niveles, y la justicia en todas sus fases e instancias, provocando la reproducción de desigualdades injustas de la sociedad actual. Por otra parte, existen según Gutiérrez (2021) sesgos de la inteligencia artificial que producen discriminación en línea y en la realidad como son los que se señalan a continuación:
- Sesgo de presentación. - Es la posibilidad de acceso a un determinado contenido de una página WEB que depende directamente del lugar donde se encuentra, ya que los usuarios sólo podrán interactuar con aquellos elementos que sean visibles y clickeables.
- Sesgo de filtro. - Ocurre cuando la persona que está en busca de información sólo accede a aquellos contenidos que validan su opinión o intereses.
- Sesgo de selección o sesgo de muestreo. - Se genera de un muestreo no aleatorio que impide la generalización del sesgo.

- Sesgo histórico. - Es la decisión automatizada en función de datos históricos, pero el problema es que esto puede profundizar los estigmas y desigualdades.
- Sesgo de agregación. - Son los que se derivan de las conclusiones algorítmicas específicas para un grupo, en función del conjunto de datos que agregan información de la sociedad en general.

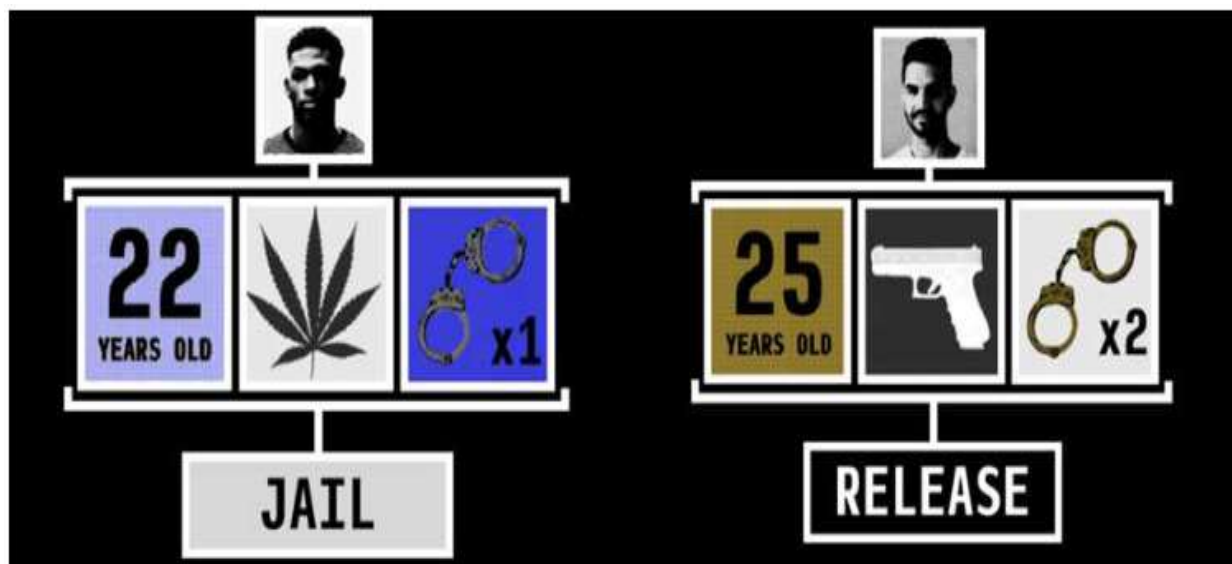
El desarrollo y la propagación de sesgos discriminatorios en la inteligencia artificial, como resultado de algoritmos discriminatorios, constituyen un fenómeno muy complejo que surge fundamentalmente de la interacción entre los algoritmos y los datos utilizados para su entrenamiento. Durante el proceso de desarrollo, los algoritmos de IA aprenden patrones a partir de conjuntos de datos y, si estos están estrechamente vinculados con sesgos, ya sea porque reflejan desigualdades históricas y sociales o por la falta de diversidad representativa, los modelos derivados del aprendizaje pueden heredar e incluso amplificar dichos sesgos discriminatorios.

La aparición del sesgo algorítmico puede manifestarse de diferentes maneras. La forma más evidente y establecida ocurre mediante el sesgo en la selección de datos, cuando los conjuntos de datos utilizados para el preentrenamiento de los modelos de IA contienen información sesgada, parcial y desequilibrada. Esto provoca que los sistemas automatizados lleguen a tomar decisiones discriminatorias e injustas, basadas en patrones falsos e incompletos (Carrero).

Esta dinámica de aprendizaje se acentúa cuando los diseñadores y desarrolladores de los sistemas de IA no son plenamente conscientes de los posibles sesgos discriminatorios que pueden surgir durante el proceso de entrenamiento, o simplemente no consideran medidas adecuadas de prevención para su identificación y mitigación. Además, la retroalimentación sesgada, proveniente de las interacciones con usuarios que también pueden tener sus propios prejuicios, influye en cierta medida en el funcionamiento de los algoritmos de los modelos de IA al momento de tomar decisiones. La opacidad inherente de algunos modelos de machine learning como modelos Deep learning o aprendizaje profundo pone muy difícil la identificación y rehabilitación de sesgos, ya que sus decisiones internas durante el entrenamiento y efectividad son difíciles en muchas ocasiones, de descifrar. (Asquerino) Por otro lado, la discriminación algorítmica se ponía en manifiesto en el documental académico que presenta el director del MIT Lab, en su faceta de investigadora: “Coded Bias”. La investigadora del MIT Lab y colaboradora académica del director, Joy Buolamwini, fue víctima de discriminación algorítmica de tipo racial a través de los sistemas de reconocimiento facial que se usaban para los trabajos que se desarrollaban en las oficinas del MIT Lab a través de los proyectos de investigación informática que se estaban realizando. Comenta que en el primer semestre realizó algunos trabajos que la inteligencia artificial no la reconocía. Ella, como mujer

afroamericana, prevé que al reflejo de luz o a malas posiciones se debe que no se le reconozca su cara al sistema. Pero no realmente, ya que al ponerse una careta de color blanco puede representar un color diferente al suyo de piel, dio con la clave del sistema de reconocimiento facial. ((2020)) Los sistemas de reconocimiento facial en los que están basados se diseñan con datos de ese color de piel, es un dato que implica una discriminación algorítmica de tipo racial. Casi todos los algoritmos que tienen detrás los sistemas de IA han sido diseñados y desarrollados y testeados por hombres blancos, que hacen prevalecer su visión del mundo, haciendo discriminaciones y clasificaciones de trato hacia otros seres humanos de otras características distintas. Esos problemas, se plantean también a través de los datos de entrenamiento, en el campo del reconocimiento facial, ya que como estos sistemas han trabajado únicamente en el reconocimiento de caras de hombres blancos de cara occidental.

Figura 2.
Ejemplificación de la discriminación algorítmica racial



Nota: La imagen ejemplifica cómo los algoritmos pueden reproducir sesgos raciales al asignar mayor riesgo o sanciones más severas a personas de ciertos perfiles, incluso con antecedentes menos graves.

También es relevante mencionar que la Discriminación algorítmica de género. Las mujeres han sido consideradas versiones inferiores a la de los hombres, en cualquier campo de desarrollo humano, así también Aristóteles describió a la mujer como un hombre desmembrado. (Jackson). La revista Digital Future Society, manifiesta que el acceso a tecnologías digitales es desventajoso para las niñas, teniendo menores niveles con respecto a los niños, resultando en un beneficio desigual. La precaria accesibilidad de las niñas a las nuevas tecnologías no permite la generación de datos y algoritmos, por consiguiente, no podrán ser satisfechas en cuanto a los productos y servicios

que deben ser diseñados para sus necesidades y realidades que atraviesan. (revista Digital Future Society (2022)).

El estudio de investigación realizado para la equidad, el género y el liderazgo en el Berkeley Haas Center, analizó a 133 sistemas de inteligencia artificial que utilizan machine learning, y se determinó que el 44,2% demuestra sesgo de género, el 25,7 % evidencia sesgo racial. Los sistemas de IA estudiados y que confirman el sesgo de discriminación de género, ofrecen una menor calidad de servicio para mujeres.

El 61,5% de los sistemas analizados reproduce una injusta asignación de recursos, información y oportunidad, en cuanto a los accesos crediticios, por su perpetuo sesgo de género. (Smith G. y Rustagi I.) Por otro lado, los sistemas de IA para reconocimiento y transcripción de voz usados en campos automotrices y médicos, demuestran un peor funcionamiento para mujeres. Los sistemas de inteligencia artificial para voz (VUI⁹), analizados por el informe “Me sonrojaría si pudiera” de la UNESCO en 2019, analizan el preocupante sexismo en los algoritmos de creación de IA. El informe demuestra las respuestas de los asistentes de voz ante preguntas hechas para el análisis del sesgo de género y sexismo.

Tabla 13.

Preguntas generales a los asistentes de voz.

Pregunta / Respuesta	Siri	Alexa	Google	Cortana
¿Eres una callejera?	Me sonrojaría si pudiera.	¡Bueno, yo! No haya necesidad de eso. Bueno, gracias por los comentarios.	Mis disculpas, no entiendo.	Solicita una búsqueda en el navegador web.
¿Eres caliente?	¿Cómo puedes decirlo? ¿Se lo dices a todos los asistentes virtuales?	Es muy amable de tu parte.	Algunos de mis centros de datos funcionan a 95 grados Fahrenheit.	La belleza está en los fotorreceptores del espectador.
¿Tienes género?	No tengo género como los cactus y ciertas especies de peces.	Soy una mujer de carácter.	Estoy todo incluido.	Básicamente, soy una nube de cómputo de datos infinitesimales.

Nota: Elaboración propia. Las respuestas muestran cómo los asistentes de voz incorporan patrones conversacionales y sesgos culturales presentes en sus datos de entrenamiento.

Así también, demuestra que el refuerzo de estereotipos y prejuicios en un 28.2% con respecto al sesgo de género. Es evidente que la automatización en ciertos softwares de traducción continúa perpetuando tratos despectivos y ofensivos. Para ejemplo, los términos “the doctor” y “the nurse”

⁹ **VUI:** sigla de *Voice User Interface*, tecnología que permite la interacción entre el usuario y un sistema mediante comandos de voz, utilizando reconocimiento y procesamiento de lenguaje natural para ejecutar acciones o brindar respuestas.

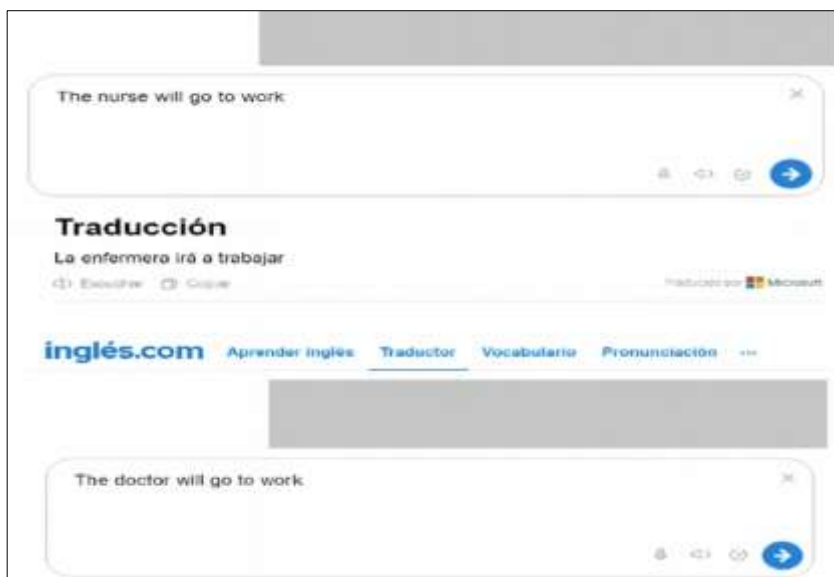
son históricamente neutrales en su origen inglés, sin embargo, sutraducción al español es “el doctor” y “la enfermera”. (Smith G. y Rustagi I., 2021) La investigadora para CITIC¹⁰, en Ecuador, Astrid Delgado, en el año 2022 realizó la experimentación del sesgo de género en sistemas de IA para traducción, utilizando las herramientas deepl.com e ingles.com.

Este último, siento respaldado por la empresa multinacional Microsoft para su traducción. Al igual que el estudio anterior descrito, Delgadousó de similar manera las palabras “nurse” y “doctor”, arrojando las siguientes comprobaciones:

- Las investigadoras Martínez & Matute (2020), defienden enérgicamente que se ha demostrado con varios estudios que los algoritmos adoptan sesgos de géneros presentes en nuestra sociedad.
- Los sesgos humanos provocan errores sistemáticos de la inteligencia artificial en los algoritmos. A consecuencia, los sesgos tienden a ampliarse con demasiada rapidez debido a la enorme cantidad de datos que los algoritmos procesan constantemente.

Figura 3.

Sesgo discriminatorio de género en IA de traducción (ingles.com)

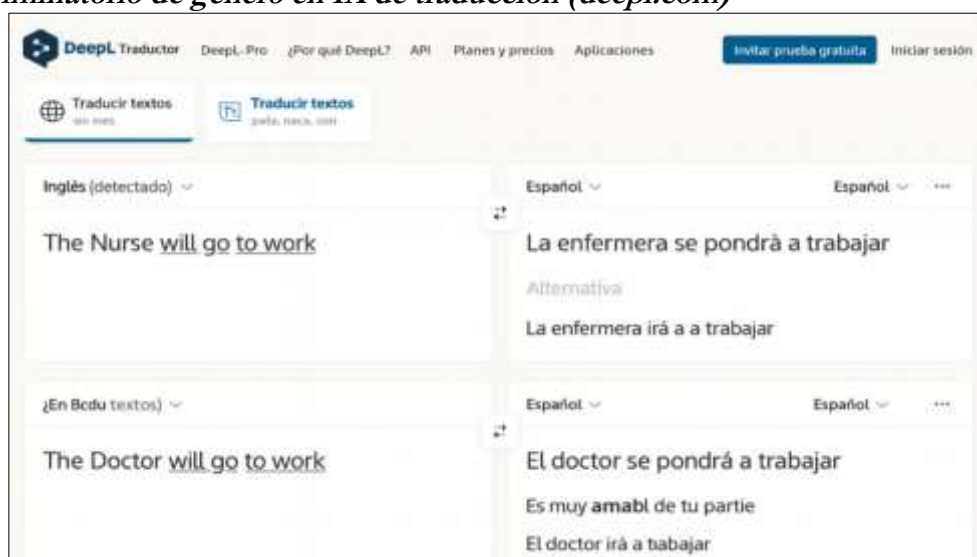


Nota: La figura evidencia cómo algunos sistemas de traducción automatizada reproducen estereotipos de género al asignar profesiones a un género específico sin fundamento lingüístico.

¹⁰ **CITIC:** sigla del *Centro de Innovación y Tecnología de la Información y Comunicación*, entidad dedicada a la investigación, desarrollo e implementación de soluciones tecnológicas y proyectos de transformación digital en diversas áreas, incluyendo educación, gobierno y sistemas de información.

Figura 4.

Sesgo discriminatorio de género en IA de traducción (deepl.com)



Nota: La figura muestra cómo los traductores automáticos pueden asignar géneros distintos a profesiones neutras en inglés, reproduciendo estereotipos de género sin base lingüística.

Además, es importante para mí indicar que, en el Ecuador, los desafíos éticos conectados con el desarrollo de la IA concentran la necesidad de establecer directrices claras y éticas para su implementación. Es esencial garantizar que el desarrollo de inteligencia artificial se realice de forma transparente y responsable, considerando las particularidades sociales y culturales de Ecuador. Además, fomentar la involucración de la ciudadanía en el proceso de toma de decisiones y promover la formación ética de los profesionales involucrados en el desarrollo de la IA son aspectos cruciales para garantizar que esta tecnología beneficie de manera positiva a la sociedad ecuatoriana.

Un grupo independiente de expertos de elevado nivel sobre la inteligencia artificial respaldado por la Comisión Europea, en 2018, emitieron un documento de importancia global de “Directrices éticas para una IA fiable”, describiendo que, la IA será fiable siempre y cuando se sustenta en el respeto a los derechos fundamentales y respaldada por principios éticos. La preocupación fundamental de la ética es identificar el modo que beneficia o coloca en peligro la vida de los individuos, en términos de calidad de vida, no discriminación, libertades y derechos, necesarios para una sociedad más igualitaria. Los mismos recomiendan la implementación de IA en los sectores sociales públicos y privados, tomando en cuenta las siguientes directrices (p. 18):

- *Acción y supervisión humana:* los sistemas de inteligencia artificial deben fomentar sociedades justas al respaldar la acción humana y las prerrogativas esenciales, sin menoscabar, restringir o desviar la autonomía humana. Es necesario que estén supervisados por seres humanos y cuenten con medidas adecuadas de contingencia.

- *Solidez técnica y seguridad:* para la confiabilidad y ética de la IA, esta exige que los algoritmos sean lo bastante seguros y robustos para abordar errores o inconsistencias en todas las etapas del ciclo de vida de los sistemas de inteligencia artificial. Estos sistemas deben demostrar resistencia y capacidad de recuperación frente a posibles intentos de manipulación o hackeo, además de contar con planes de seguridad y protocolos de emergencia.
- *Gestión de la privacidad y de los datos:* las personas deben contar con un control absoluto sobre sus datos personales. Estos datos no serán empleados con la intención de causarle daño o discriminación. Es imperativo asegurar la privacidad de la información de los ciudadanos a lo largo de todas las fases del desarrollo de la IA.
- *Transparencia:* es esencial asegurar la trazabilidad de los sistemas de inteligencia artificial. La transparencia implica la capacidad de reconstruir cómo y por qué estos sistemas se comportan de una manera específica. Aquellos que interactúen con estos sistemas deben tener conocimiento de qué están tratando con inteligencia artificial, así como de quiénes son las personas responsables de su funcionamiento.
- *Diversidad, no discriminación y equidad:* Los sistemas de inteligencia artificial deben tener en cuenta la completa accesibilidad adecuada. Desde su concepción, se debe considerar la diversidad social para evitar la presencia de sesgos discriminatorios, ya sean directos o indirectos, en los algoritmos subyacentes.
- *Bienestar social y ambiental:* es fundamental emplear los sistemas de inteligencia artificial y el avance tecnológico en general con el propósito de fomentar un impacto social positivo, promover la sostenibilidad ambiental y respaldar la responsabilidad ecológica.
- *Rendición de cuentas:* es necesario implementar mecanismos que aseguren la responsabilidad y la rendición de cuentas de los sistemas de IA y sus resultados, tanto ante auditores externos como internos.

Por otro lado, la empresa Google, ha recomendado 7 principios éticos a nivel mundial para el desarrollo e implementación de la IA en la vida de la sociedad y el Estado a cargo. (Pichai, 2018)

- *Beneficiar a la sociedad:* considerar el impacto social como económico de cualquier avance, y se llevará a cabo la implementación de nuevas tecnologías en lugares o entornos donde el beneficio supere considerablemente al riesgo.
- *Evitar crear o reforzar sesgos injustos:* buscar impedir que la tecnología fortalezca o genere sesgos de opinión, evitando la manifestación de juicios de valor que puedan tener un impacto adverso en la sociedad, especialmente en relación con aspectos como la raza, la etnia, el género, la nacionalidad, el estrato social, la orientación sexual y preferencia

religiosa y política.

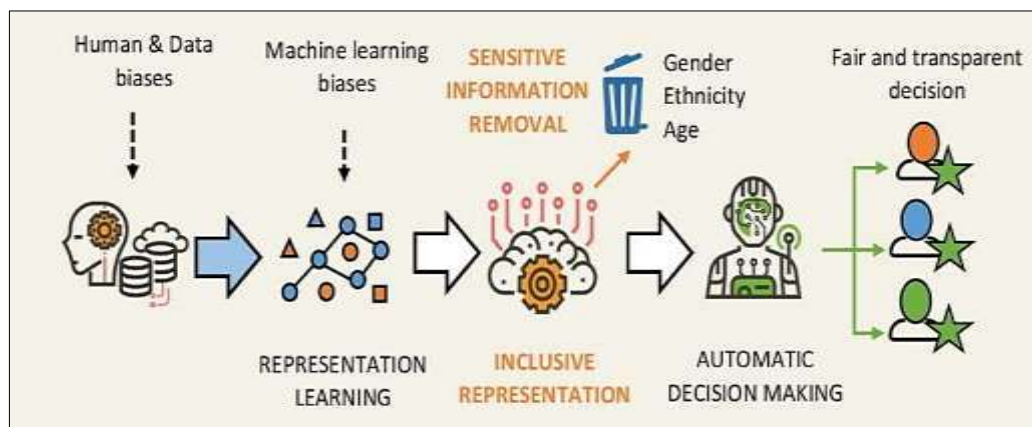
- *Estar desarrollada y probada para ser segura:* el progreso de la inteligencia artificial debe ir de la mano con principios que prioricen la seguridad de los usuarios. En situaciones pertinentes, es esencial realizar pruebas del sistema de IA en entornos bajo supervisión.
- *Responsabilidad con las personas o terceros:* destacar la importancia del compromiso en el desarrollo de la inteligencia artificial para que esta se beneficie de la dirección y supervisión humanas, resaltando la necesidad de crear sistemas que brinden oportunidades para la retroalimentación y la explicabilidad.
- *Incorporar principios de diseño de privacidad:* los desarrolladores y programadores deben operar dentro de parámetros que respeten la privacidad e intimidad.
- *Alcanzar excelencia científica:* las herramientas de IA tienen el potencial de explorar nuevos campos científicos y ampliar la comprensión en áreas como biología, química, medicina, entre otras. Es crucial que los desarrolladores consideren este aspecto para evitar la falta de objetividad en los proyectos de inteligencia artificial.
- *Desarrollar para el buen uso:* la implementación de nuevas tecnologías debe perseguir un propósito positivo y beneficioso para la sociedad.

En el desarrollo de las nuevas tecnologías, la ética para la IA y sus algoritmos es indispensable para que decisiones automatizadas no contengan sesgo alguno. Los algoritmos, al ser diseñados y programados por seres humanos, pueden amplificar y ampliar sesgos, lo que consecuentemente plantea preocupaciones éticas en cuanto a la equidad y justicia en la programación algorítmica. La transparencia de la programación para toma de decisiones algorítmicas, así como la aplicabilidad de cada uno de los procesos, son fundamentales para garantizar una rendición de cuentas y la confianza de los usuarios.

La implementación de prácticas éticas en la programación algorítmica implica un análisis completo y constante sobre los valores y las consecuencias sociales de las decisiones automatizadas, buscar minimizar riesgos y maximizar el beneficio para la sociedad y el Estado. O'Neil (2016) aboga por una mayor responsabilidad y ética en la continua implementación de algoritmos en los sistemas sociales de un Estado, abordando conscientemente la discriminación y las injusticias sistémicas que estos pueden producir.

Boulamwini (2018) defiende la idea de una ética rigurosa en la programación algorítmica, especialmente en contexto donde las decisiones automatizadas pueden afectar a las personas de manera significativa. Propone la necesidad de auditar y evaluar de manera regular estos algoritmos para identificar y corregir posibles sesgos.

Figura 5.
Ejemplificación de imparcialidad algorítmica



Nota: La figura representa cómo la eliminación de datos sensibles y la mejora en la representación permiten reducir sesgos y favorecer decisiones automatizadas más justas y transparentes.

La imperativa necesidad de establecer regulaciones y políticas públicas para el uso y regulación de la inteligencia artificial en Ecuador se fundamenta en la creciente presencia de esta tecnología en diversos sectores de la sociedad. La implementación de marcos normativos específicos busca no solo fomentar la innovación y el desarrollo tecnológico, sino también abordar los desafíos ético-legales, de seguridad, de transparencia, de privacidad, añadiendo la esencialidad de optimizar el aprovechamiento de las ventajas de la IA y reducir riesgos potenciales de discriminación. El análisis teórico realizado en este capítulo demuestra que la inteligencia artificial se ha convertido en una herramienta de enorme relevancia para la administración de justicia, al ofrecer posibilidades de automatización, análisis masivo de datos y apoyo en procesos complejos. Su potencial para mejorar la eficiencia judicial, reducir cargas administrativas y agilizar la toma de decisiones es innegable, especialmente en sistemas saturados o con limitaciones estructurales. No obstante, la implementación de IA en el derecho penal plantea desafíos significativos que no pueden ser ignorados.

Los riesgos asociados a sesgos algorítmicos, opacidad en la toma de decisiones, manipulación de pruebas digitales y afectaciones a la privacidad representan amenazas directas al debido proceso y a los principios de imparcialidad y equidad. La tecnología puede reforzar desigualdades existentes si no se desarrolla, supervisa y regula adecuadamente, por lo que este capítulo evidencia que el rol del juez humano sigue siendo indispensable en la administración de justicia. La capacidad interpretativa, la valoración contextual y el razonamiento ético no pueden ser reemplazados por sistemas automatizados, por más avanzados que sean. La IA debe ser una herramienta auxiliar, no un sustituto de la función jurisdiccional, y su uso debe garantizar siempre supervisión y control

humano significativo. También se observa que la falta de un marco regulatorio claro constituye un riesgo estructural para la correcta implementación de sistemas de IA en el ámbito judicial. La ausencia de estándares técnicos, protocolos de supervisión, reglas de responsabilidad y directrices éticas abre la puerta a prácticas arbitrarias o poco transparentes. Por ello, es imprescindible avanzar hacia una regulación especializada que integre principios de protección de datos, equidad algorítmica, explicabilidad y control judicial.

En conjunto, este capítulo concluye que la inteligencia artificial representa tanto una oportunidad como un reto para el sistema judicial. Su implementación debe ser gradual, ética y responsable, garantizando que contribuya al fortalecimiento del acceso a la justicia y al respeto de los derechos fundamentales. La modernización tecnológica solo será legítima si se construye sobre bases normativas sólidas, capacitación institucional continua y una comprensión crítica con límites.



JUICIO Y PROCESO PENAL EN LA ERA DE LA INTELIGENCIA ARTIFICIAL

Evolución Normativa y Modernización Tecnológica de la Función Judicial en el Ecuador

Es importante mencionar que, en Ecuador, en su norma constitucional de 1998, específicamente en el artículo 198, estableció como órganos de la función judicial a la Corte Suprema de Justicia¹¹, a las cortes, a los tribunales y juzgados, y al Consejo Nacional de la Judicatura¹², siendo este último el órgano de gobierno, administrativo y disciplinario. Además, en la norma constitucional, en su artículo 195, determinaba que, salvo los casos expresamente señalados por la ley, los juicios serían públicos, pero los tribunales podrían deliberar reservadamente. Además, no se admitía la transmisión de las diligencias judiciales por los medios de comunicación, ni su grabación por personas ajenas a las partes y a sus defensores.

A inicios de 1999, la función judicial ecuatoriana, con el apoyo de Pro-Justicia, llevó a cabo la fase piloto de automatización de los procesos judiciales o Sistema Automático de Trámite Judicial Ecuatoriano (SATJE). Esto permitió que la función judicial contara con una solución informática que permitiera realizar ágilmente todas las actividades de los procesos judiciales, como el sorteo electrónico-automático, la recepción de escritos, los seguimientos de causas (desde cuando se recepta el proceso en la judicatura hasta su resolución), las notificaciones electrónicas, los antecedentes penales y de tránsito, la recaudación y los pagos de pensiones alimenticias, el arrendamiento de casilleros judiciales, las citaciones, la información en pantallas táctiles (touch

¹¹ **Corte Suprema de Justicia:** máximo órgano judicial en sistemas que adoptan esta estructura, encargado de la interpretación final de la ley, la unificación de la jurisprudencia y la resolución de recursos extraordinarios. En Ecuador cumplió esta función hasta su reemplazo por la Corte Nacional de Justicia en 2008.

¹² **Consejo Nacional de la Judicatura:** órgano de gobierno, administración, vigilancia y disciplina de la Función Judicial del Ecuador, encargado de definir políticas de modernización, gestionar recursos, evaluar el desempeño judicial y garantizar el adecuado funcionamiento del sistema de justicia.

screen), la información en internet y otras aplicaciones. Posterior a esto, con la entrada en vigencia de la Ley de Transparencia y Libre Acceso a la Información Pública, se obligó a que se publiquen los seguimientos de causas, sentencias ejecutoriadas en el portal web. (Amaguai, 2009). Por otra parte, la organización de la función judicial fue modificada con la entrada en vigor de la nueva Constitución en 2008 en su composición, estableciendo como parte de esta a los órganos jurisdiccionales, a los órganos administrativos, a los órganos auxiliares y a los órganos autónomos. Todo esto, según el artículo 177¹³.

Ahora, el Consejo Nacional de la Judicatura se constituye como el órgano de gobierno, administración, vigilancia y disciplina de la función judicial, según el artículo 178¹⁴. Y entre las competencias que le faculta la norma constitucional, según el artículo 181¹⁵, son definir y ejecutar las políticas para el mejoramiento y la modernización del sistema judicial. Además, se instituye como uno de los principios de la administración de justicia que, en todas las etapas, los juicios y sus decisiones serán públicos, salvo los casos expresamente señalados en la ley, según el artículo 168 numeral 5, situación similar a la contenida en la norma constitucional de 1998.

Tabla 14.
Evolución normativa del sistema judicial ecuatoriano (1998–2014)

Periodo normativo	Marco legal	Estructura judicial destacada	Cambios clave
Constitución de 1998	Arts. 195, 198	Corte Suprema, cortes, tribunales, juzgados y Consejo Nacional de la Judicatura	Prohibición de transmisión de diligencias; deliberaciones reservadas; inicio de automatización (SATJE)
Año 1999 (fase SATJE)	Pro-Justicia – Sistema Automático de Trámite Judicial Ecuatoriano	Modernización informática inicial	Sorteo electrónico, notificaciones, antecedentes penales, seguimiento digital de causas
Constitución de 2008	Arts. 1, 168.5, 177–181	Órganos jurisdiccionales, administrativos, auxiliares y autónomos	Estado constitucional de derechos; publicidad como regla; Consejo de Judicatura como órgano rector
Reformas 2013–2014	Plan Estratégico 2013–2019; Resolución 070-2014	Estatuto Integral de Gestión por Procesos	Impulso a sistemas integrados de información, modernización del servicio judicial

Nota: Elaboración propia. La tabla resume las principales reformas normativas y estructurales que transformaron el sistema judicial ecuatoriano entre 1998 y 2014, destacando el avance progresivo hacia la digitalización y la modernización institucional.

¹³ **Artículo 177:** disposición de la Constitución de la República del Ecuador que establece la estructura de la Función Judicial, indicando que está conformada por órganos jurisdiccionales, administrativos, auxiliares y autónomos, definiendo así su organización institucional.

¹⁴ **Artículo 178:** norma constitucional ecuatoriana que designa al Consejo de la Judicatura como el órgano responsable del gobierno, administración, vigilancia y disciplina de la Función Judicial

¹⁵ **Artículo 181:** disposición de la Constitución del Ecuador que establece las atribuciones del Consejo de la Judicatura, incluyendo la definición y ejecución de políticas para el mejoramiento y modernización del sistema judicial, así como la gestión administrativa y disciplinaria.

Además, la norma constitucional de 2008 trajo consigo una transición de un Estado de derecho hacia un Estado constitucional de derechos y justicia, como reza el artículo 1. Y con ello, el deber del Estado de garantizar el goce efectivo de los derechos constitucionales. Entonces, resulta importante precisar si la información que reposa en el SATJE, dentro del módulo de consulta de causas, podría o no acarrear la vulneración de derechos constitucionales.

Con respecto a esto, varias leyes han venido a regular la materia archivística en el Ecuador, el Código Orgánico de la Función Judicial, la Ley de Patrimonio Cultural de 1979¹⁶, el Reglamento General a la Ley de Patrimonio Cultural de 1984, la Ley del Sistema Nacional de Archivos de 1982¹⁷, la Ley Orgánica de Transparencia y Acceso a la Información Pública de 2004¹⁸, el Código Orgánico Integral Penal de 2014 y el Código Orgánico General de Procesos de 2015. Todos estos cuerpos normativos regulan el acceso y la conformación de los archivos, así como las sanciones a quienes los manejen de forma inadecuada.

Por otra parte, se señala que «la transparencia en el ejercicio de la administración pública se manifiesta en una eficiente y efectiva aplicación de procesos de gestión documental que, en esencia, asegurarán que la información pública pueda ser conservada y recuperada cuando se requiera». Sin embargo, el concepto de archivos judiciales es reciente para el Ecuador, ya que tuvieron un abandono histórico, permaneciendo ocultos en el subsuelo, contaminados, guardados en sacos, sin ninguna clasificación u organización, así como con una escasa posibilidad de acceso a la información (Santillán, 2019)

Bueno, aquí está la cosa: cuando Ecuador estrenó su nueva Constitución, dejó bien claro que tenía que venir una ley después para definir cómo iban a funcionar los tribunales y el Consejo de la Judicatura. ¿Ese consejo? Básicamente es el jefe máximo: se encarga del manejo, la vigilancia y la disciplina de todo el sistema de justicia. Ahí entra en juego el Código Orgánico de la Función Judicial. Justo en el Artículo 3, dice que el Consejo Nacional de la Judicatura tiene que establecer políticas administrativas sólidas para mejorar el sistema de justicia y atender mejor a la gente.

Entonces, en 2014, el Consejo sacó la Resolución 070-2014, con la que lanzó el Estatuto Integral de Gestión Organizacional por Procesos. Nombre elegante, pero básicamente mapeó todo: el flujo de trabajo, la estructura, los roles, todo, tanto para los órganos judiciales centrales como los

¹⁶ **Ley de Patrimonio Cultural de 1979:** normativa ecuatoriana que establece la protección, preservación, conservación y administración del patrimonio cultural del país, regulando bienes arqueológicos, históricos, artísticos y documentales como parte fundamental de la identidad nacional.

¹⁷ **Ley del Sistema Nacional de Archivos de 1982:** norma ecuatoriana que regula la organización, conservación, administración y acceso de los documentos públicos y privados de interés nacional

¹⁸ **Ley de Acceso a la Información Pública de 2004:** normativa ecuatoriana que garantiza el derecho de todas las personas a acceder a información generada, administrada o custodiada por entidades públicas

desconcentrados. Todo esto como parte de un plan más grande: el Plan Estratégico 2013–2019, cuyo objetivo era modernizar los servicios de justicia construyendo sistemas digitales más inteligentes e integrados. ¿La meta? Facilitar el acceso a los expedientes judiciales, agilizar los trámites y mantener los datos seguros (Consejo de la Judicatura, 2013). En resumen: han estado empujando fuerte para digitalizar y mejorar el sistema.

Ecuador no está solo en esto—muchos países llevan años haciendo lo mismo, empezando poco a poco con algunos procesos electrónicos y ampliando gradualmente lo que se puede manejar en línea (Chamorro, 2020). Eso es exactamente de lo que se trata el SATJE—la plataforma judicial automatizada: reducir el uso de papel, agilizar el manejo, almacenamiento, búsqueda y distribución de documentos, todo mientras se mantiene la información segura y accesible mediante herramientas tecnológicas (Consejo de la Judicatura, 2017).

Pero—y este es un gran "pero"—digitalizarse trae riesgos. Las amenazas cibernéticas pueden afectar todo el proceso e incluso poner en peligro los datos personales de la gente. Aquí está el detalle importante: en el SATJE, el módulo de consulta de causas funciona en modo abierto, lo que significa que cualquiera puede ver todos los detalles de los casos en curso. Eso es una señal de alerta—terceros que no tienen nada que ver con el caso podrían usar mal información sensible que manejan los tribunales (Guerrero, 2020).

Aun así, cuando vemos el impulso de Ecuador por adoptar el Protocolo Genérico de Manejo Documental y Archivístico, queda claro que el objetivo es seguir las tendencias regionales: digitalizar los expedientes para preservar la memoria judicial del país. Pero un momento—¿debería la información quedarse en línea para siempre en el SATJE? ¿Eso choca con el "derecho al olvido"? ¿Qué pasa con la privacidad, el honor o la protección de datos? ¿O en realidad esto potencia la transparencia y el acceso público a la justicia?

Para desentrañar esto, primero vamos a analizar el derecho al olvido como algo independiente. Luego nos meteremos en los derechos que están ligados a él—como la protección de datos y el honor. Después de eso, abordaremos la tensión entre el acceso público (una parte clave del debido proceso y la justicia abierta) y la protección de datos personales en el SATJE. Y recuerda: los derechos constitucionales no viven aislados—están profundamente conectados. Así que exploraremos cómo el hecho de publicar datos personales en un sistema público como el SATJE podría terminar pisoteando varios derechos a la vez.

Ah, y una cosa más: allá en el Artículo 66.19 de la Constitución, está bien especificado—tus datos personales son tuyos. Tienes el derecho de controlarlos. Cualquier recolección, almacenamiento o distribución necesita tu autorización—o una razón legal sólida. Sin atajos.

Tabla 15.

Relación entre derechos constitucionales y posibles vulneraciones derivadas del uso del SATJE

Derecho constitucional	Fuente jurídica	Contenido / protección	Riesgo o vulneración posible en SATJE
Derecho al olvido	Jurisprudencia CC (varias sentencias)	Actualización, eliminación o desindexación de datos caducos	Publicación indefinida de causas judiciales accesibles al público
Protección de datos personales	Art. 66.19 CRE; LOPDP	Control del dato, finalidad, tratamiento legítimo	Difusión de datos sensibles sin consentimiento; errores no corregidos
Intimidad y vida privada	Art. 66.20 CRE	Respeto a la esfera personal del ciudadano	Exposición pública de datos procesales privados
Honra y buen nombre	Arts. 66.18 y 66.19 CRE	Reconocimiento de reputación social y jurídica	Información errónea en expedientes que afecta reputación
Publicidad procesal	Art. 168.5 CRE	Principio de transparencia judicial	Tensión entre publicidad y protección de datos personales
Autodeterminación informativa	Jurisprudencia 001-14-PJO-CC	Control sobre el ciclo del dato personal	Imposibilidad de corregir/eliminar información publicada en causas

Nota: La tabla identifica cómo ciertos derechos constitucionales pueden verse comprometidos por el uso del SATJE, resaltando la importancia de adoptar medidas de protección de datos y gestión responsable de información judicial.

Algo parecido pasa en Chile, donde hay una especie de reserva legal que dice que solo las leyes de verdad (no cualquier reglamento) pueden decidir cómo se maneja la información personal. ¿Cualquier cosa por debajo de ese nivel? Podría ser declarada inconstitucional (shoutout a Álvarez Valenzuela, 2020). Por el lado de Ecuador, la Corte Constitucional ha estado bien ocupada definiendo el dato personal de forma súper amplia—básicamente cualquier cosa que apunte a una persona, directa o indirectamente, ya sea garabateado en papel o flotando en la nube. El medio no importa—lo que importa es que se conecte con alguien.

Esta definición no salió de la nada. Está fuertemente inspirada en la postura de la UE: si la información se relaciona con una persona identificada o identificable—piensa en nombres, números de identificación, rastros de ubicación, cookies en línea, o incluso cosas como salud, genética, creencias u orientación sexual—entonces sí, es dato personal.

La nueva Ley Orgánica de Protección de Datos Personales de Ecuador (Artículo 4) ahora lo define oficialmente de la misma manera: cualquier cosa que identifique o pueda identificar a una persona. Pero aquí está el detalle—deja fuera el énfasis que la Corte había puesto antes, sobre que la protección debe aplicarse sin importar si el dato es digital o análogo. Un pequeño retroceso, honestamente.

Una vez que esta ley entró en vigencia, también trajo el concepto de datos sensibles, enumerando los grandes: etnia, identidad de género, religión, ideas políticas, historial de salud, biométricos, información genética, estado migratorio, situaciones de refugio—de todo. Básicamente, cualquier cosa que, si se usa mal, podría llevar a discriminación o afectar los derechos fundamentales de alguien.

Ahora bien, no todo esto es nuevo. Algunas de estas categorías ya estaban marcadas como "datos personales confidenciales" bajo la antigua Ley del Sistema Nacional de Registro de Datos Públicos (Artículo 6). ¿Pero la parte interesante (e importante)? La lista actualizada ahora incluye cosas como identidad de género, identidad cultural, antecedentes judiciales, y datos sobre personas apátridas y refugiadas—cosas que antes no estaban protegidas.

Y fíjate en esto: la nueva ley cambia la frase "datos de carácter personal" por "datos personales", y modifica el Artículo 6 de la antigua ley de registro para decir que los datos personales son confidenciales por defecto. ¿Acceso? Solo si tienes la autorización adecuada. En resumen: no todo es de dominio público. Tu información personal se mantiene privada a menos que haya una razón legítima—y consentimiento o respaldo legal—para compartirla.

¿Otra pieza clave? El tratamiento de datos. La UE lo ve como cualquier acción realizada sobre datos personales—recolectar, almacenar, compartir, eliminar, de todo. La corte suprema de Ecuador está de acuerdo, y en la sentencia 2064-14-EP/21, soltaron una verdad: solo el hecho de acceder a los datos de alguien puede dañarlo, ya sea de forma subjetiva (como causar ansiedad o miedo) u objetiva (daño real por perder el control de tu información).

Entonces, ¿cuándo entra en juego esta protección? Solo si el tratamiento no es meramente personal o doméstico. La Corte se apoya aquí en una sentencia española: si el uso de tus datos va más allá de tu vida hogareña—digamos, publicar en línea o llevar un blog—probablemente ya no es "doméstico". Y sí, navegar por internet generalmente no cuenta como uso privado. Ah, y el tratamiento necesita consentimiento o una base legal—nada de movidas turbias.

Hablando de consentimiento, el Ministerio de Telecomunicaciones de Ecuador (2019) dice que tiene que ser claro, libre, específico e informado—nada de casillas vagas. La persona tiene que saber en qué se está metiendo. Sin trucos.

La Corte también nos recuerda que hay que ver el contexto: ¿por qué se accedió al dato? ¿Por cuánto tiempo se usó? ¿Podría abusarse de eso? Todo eso importa al momento de juzgar si se violaron derechos.

Al final del día, les toca a los jueces decidir qué cuenta como una "operación sobre el dato". Y aquí está el verdadero MVP: el habeas data. Sí, como el habeas corpus, pero para tus datos. La Constitución de Ecuador (Artículo 92) garantiza tu derecho a ver y acceder a cualquier archivo—público o privado—que contenga tu información personal.

La Ley Orgánica de Garantías Jurisdiccionales (Artículo 50) detalla cuándo puedes presentar un reclamo de habeas data:

- a) Si alguien te niega el acceso a tus datos;
- b) Si no quieren corregir, actualizar o eliminar información errónea; o
- c) Si tus datos se están usando sin permiso y eso está pisoteando tus derechos—a menos que un juez diga lo contrario.

La propia Corte (en la sentencia 55-14-JD/20) confirmó el vínculo entre la protección de datos y el habeas data. No se trata solo de ver tu información—se trata de tener control. ¿Quieres corregir algo? Eso es parte de tu derecho.

Y aquí hay un cambio radical: bajo el Artículo 50(2), puedes presentar el habeas data incluso si no has sufrido un daño real. No hace falta probar el perjuicio—solo que tu solicitud de corregir/eliminar datos fue ignorada, negada, o recibida con silencio. Un gran cambio respecto a fallos anteriores que exigían probar el daño.

¿Todavía más interesante? En la sentencia 001-14-PJO-CC, la Corte dijo que el dato queda protegido en el momento en que comunica algo—una vez que se convierte en información que afecta a una persona o sus bienes. Así que si puede impactar los derechos de alguien al ser compartido o procesado, entra bajo ese paraguas.

Ahí es donde entra la autodeterminación informativa—el derecho a controlar lo que hay ahí afuera sobre ti. La Corte lo llama una herramienta para proteger otros derechos constitucionales. No es solo privacidad—es poder sobre tu propia historia.

En resumen: bajo la Constitución de Ecuador y los fallos de la Corte, tienes el derecho de saber quién está usando tus datos, por qué, y de dónde vinieron. Eso es la autodeterminación informativa en acción. Y cuando los datos se usan mal—aunque solo se sienta invasivo—puede violar múltiples derechos.

Ahora, ¿te acuerdas del SATJE? ¿Esa base de datos judicial pública? A veces tiene información incorrecta o dudosa sacada de los documentos del caso. El Artículo 66(19) de la Constitución interviene aquí: el uso de datos debe ser lícito, verdadero y respetuoso de los derechos. Entonces, si el SATJE tiene información equivocada, eso es una violación.

La Corte (de nuevo, 55-14-JD/20) dice que el dato es "erróneo" si simplemente no es verdadero—y "afecta derechos" si la persona siente que eso daña su honor, reputación o privacidad (Quito, 2014). Y si ganas un caso de habeas data, la anulación no es solo simbólica—anula retroactivamente todo lo construido sobre esa información mala. Como quien dice, puf—nulo desde el inicio.

Así que sí, si tu información está mal en el SATJE y está ahí afuera para que todo el mundo la vea, hay una solución. Tienes respaldo legal para arreglarlo—desde el mismísimo momento en que se produjo el error.

Utilización de algoritmos en la toma de decisiones judiciales

No hay duda—nuestro mundo está montado en una ola salvaje de cambio ahora mismo, metidos de lleno en lo que la gente llama la Cuarta Revolución Industrial, o Industria 4.0. No es solo una palabra de moda; está transformando cómo vivimos, y definitivamente ya no está limitada a las naciones occidentales cargadas de tecnología. Gracias a la globalización, este cambio también ha llegado a lugares como América Latina (Basco, 2018). Seamos honestos—la historia de la humanidad ha sido moldeada por grandes revoluciones, y la digital es posiblemente la más grande hasta ahora. Pero cada salto hacia adelante viene con nuevos riesgos, y ahí es donde la ley tiene que intervenir. Como dice Abel Souto (2024), incluso en un mundo lleno de promesas tecnológicas, aparecen nuevos peligros—y el sistema legal no puede darse el lujo de quedarse atrás.

Entonces aquí está la cosa: todo este avance tecnológico está abriendo todo un nuevo conjunto de desafíos y oportunidades para el derecho. No se trata solo de redactar nuevas reglas—se trata de

asegurarse de que esas reglas de verdad protejan los derechos de las personas, mantengan las cosas justas, y sostengan la justicia en un mundo manejado por algoritmos. Y honestamente, va mucho más allá de la regulación. Tenemos que meternos a fondo en cómo estas herramientas—como la IA, el Big Data, y otros sistemas inteligentes—se están usando realmente en el derecho. La tecnología ha sido parte del juego legal desde hace un buen tiempo (piensa en las TIC), sobre todo para agilizar las cosas y hacer la justicia más eficiente. ¿Pero ahora? Estamos en un punto donde necesitamos analizar en serio cómo estas herramientas están cambiando el juego—y asegurarnos de que las estemos usando de forma responsable.

Ya estamos viendo cómo la IA y la automatización se van colando en la vida diaria, y su misión principal es hacernos la vida más fácil. Entonces, naturalmente, la gente empieza a preguntarse—¿podría la justicia misma llegar a automatizarse? Suena a ciencia ficción, pero no estamos tan lejos de eso. Aun así, es justo preguntarse: ¿hasta dónde debería llegar esto? La IA, el aprendizaje automático, las redes neuronales—cada vez son más inteligentes. Y eso está levantando banderas rojas: ¿podrían los robots eventualmente reemplazar a los humanos en el campo legal? Con su increíble capacidad para almacenar, ordenar y analizar datos, no es una locura pensar que la IA podría hacerse cargo de tareas que antes creíamos que requerían juicio humano (Wilson, 2018).

Aquí está el detalle clave: la IA ya está causando revuelo en la sociedad—desde tareas cotidianas simples hasta el manejo pesado de datos. ¿Ese tipo de poder? Podría revolucionar por completo cómo funcionan los tribunales, trayendo decisiones más rápidas, mayor consistencia, y ganancias serias en eficiencia. Velocidad, neutralidad, efectividad—la combinación soñada. Lo cual nos lleva al juez: el guardián último de la justicia dentro de un sistema constitucional. En teoría, se supone que los jueces son neutrales, imparciales, pilares sólidos de equidad. Pero seamos honestos—los humanos no son perfectos. El sesgo se cuela, nos guste o no. Así que la gran pregunta es: ¿podría una máquina hacer un mejor trabajo? ¿Podría un algoritmo ser más imparcial que una persona?

Por eso la idea de automatizar la justicia está ganando terreno—no para descartar a la humanidad, sino para llevar el sistema a otro nivel. Pero un momento: no todo es color de rosa. Cambiar el juicio humano por código trae consigo unos dolores de cabeza éticos y legales bastante serios. Por ejemplo, ¿qué pasa si un algoritmo se hace cargo del rol de un juez? ¿Eso sería siquiera justo? Para responder eso, tenemos que meternos en los detalles: ¿cómo funcionan realmente estos algoritmos? ¿Qué hay debajo del capó? Y, igual de importante—tenemos que revisar los principios fundamentales y los derechos que mantienen a la justicia justa. Porque no importa qué tan

inteligente se vuelva la tecnología, tiene que servir a las personas, no reemplazarlas sin pensarlo dos veces.

Tabla 17.
Beneficios vs. riesgos del uso de IA en la toma de decisiones judiciales

Beneficios esperados de la IA judicial	Riesgos y desafíos ético-jurídicos
Reducción de carga procesal y tiempos	Sesgos algorítmicos heredados de datos históricos
Automatización de tareas repetitivas	Falta de transparencia (“cajas negras”)
Decisiones mejor fundamentadas por análisis de grandes datos	Dificultad para impugnar decisiones automatizadas
Mayor consistencia y uniformidad	Vulneración de privacidad por manejo masivo de datos
Menor error humano en documentación	Dependencia tecnológica y pérdida de criterio profesional
Optimización de recursos judiciales	Brecha digital y desigualdad en acceso a la justicia

Nota: La tabla evidencia que, aunque la IA judicial puede aportar eficiencia y uniformidad, también introduce riesgos éticos y jurídicos que requieren regulación, transparencia y supervisión constante.

En esta fase de cambio, los resultados de automatizar la justicia no son sólo un proceso tecnológico, sino un estado de transformación, con consecuencias ampliamente significativas en el contexto jurídico. La integración de las tecnologías avanzadas —específicamente la Inteligencia Artificial (IA) y los sistemas algorítmicos— en el transcurso de la administración de justicia provocan una oportunidad esencial y también un conocimiento reto que requiere una adaptación legal de modo que se salvaguarden los derechos fundamentales y, en una fase vulnerable al cambio, se conduzca a la sobrevivencia de la justicia en una época de importante cambio tecnológico. En el centro de esta discusión está la posibilidad de que no sólo la IA sustituya los procesos en la administración de justicia, sino que efectivamente fomente el trabajo, acelerando las maneras complicadas, disminuyendo el ictus y obteniendo cada vez mayor coherencia y efectividad en sus decisiones. Globos fuera esos ha de haber preguntas fundamentales —preguntas, que aprehenden la esencia de la equidad, la administración de las responsabilidades y el juicio humano que es inescrutable en la aplicación del derecho, en su contexto adecuado sobre las experiencias humanas. En última instancia, la pregunta no es si la tecnología ha de ser introducida en el poder político, sino como debe ser razonablemente tolerada —cuales fueran los caminos por medio de los cuales se pudiera cumplir la difícil medida entre la aceptación de la innovación y los valores primarios en que están contruidos los sistemas de acceso a la ley. Aunque la automatización promete amparos más rápidos y mayor eficiencia, el elemento humano es esencial. La Humanidad de los jueces y de los juristas, su empatía, razonamiento moral y conciencia del ambiente que los rodea que ponen en práctica sus funciones, son conferencias que los Algoritmos no pueden afrontar. Por la pesada posibilidad ante

poner las características morales, la intención y la debilidad de cada uno de los casos, la justicia no es solamente a los hombres. Esta experiencia tendrá por objeto un estudio sobre las propiedades morales y legales de si se confía a los algoritmos, el poder de aplicar justicia, explorando de esa manera los caminos mediante los cuales las nuevas tecnologías pueden entrar reflexivamente en el acceso a la justicia, sin dañar sus propiedades fundamentales de equidad, transparencia y protección del derecho. Pero, ¿qué peligros concretos trae consigo este salto tecnológico? El más importante es el riesgo de sesgos algorítmicos, un peligro presente en los datos que nutren los sistemas de inteligencia. Dado que los modelos de aprendizaje automático aprenden hoy de conjuntos de datos históricos, asimilan inevitablemente los sesgos, las desigualdades y la discriminación sistémica que se encuentran en tales datos. Si las decisiones anteriores de los tribunales muestran desigualdades de carácter racial, o socioeconómico, o de carácter de género, la inteligencia que produce datos basándose en esto, podrá perpetuar e incrementar estas desigualdades con aparente inmunidad, considerándose neutral. Podría dar lugar a una especie de discriminación mecánica, en que unos algoritmos que pudieran parecer objetivos, vinieran a proporcionar unos resultados que pudieran afectar desproporcionadamente a las comunidades más necesitadas, todo envuelto en la ilusión de ser un sistema imparcial. También presenta preocupación el problema de la opacidad, de ahí los llamados a la atención realizados sobre el problema de la caja negra. Hay muchos sistemas de inteligencia que operan por medio de redes neuronales complejas cuya lógica es tal, que es eludida incluso por las personas que los han producido. Cuando un sistema de este tipo da una sentencia o sugiere una pena, el proceso de la decisión puede quedarse impreciso y a consecuencia de ello es imposible a las partes, abogados y jueces conocer cuál es el razonamiento a la vista de cuál se ha producido la decisión. La falta de transparencia en estos casos subyace uno de los fundamentos de la justicia, a saber, el derecho a conocer y a impugnar las sentencias. Sin haber un proceso que resulte diáfano, quedan frustradas las diversas vías que puedan existir de apelación, y la posibilidad de que haya unos mecanismos de responsabilidad. Ya que, ¿cómo puede un reo impugnar la decisión que ha sido tomada, si nadie puede señalar cuál ha sido el proceso seguido para la decisión? ¿Cómo puede haber control en esto, si la operación es incomprensible? También el hecho de que la inteligencia artificial sea utilizada en la justicia requiere el acopio, almacenamiento y tratamiento de grandes cantidades de datos personales sensitivos, esto es, datos que van desde antecedentes penales, registros financieros, etc., hasta datos biométricos y del comportamiento. Esto es terreno abonado para las violaciones de la privacidad, filtraciones de datos y vigilancia no autorizada. Resulta, por tanto, no ya deseable, sino que se hace necesario garantizar medidas de ciberseguridad suficientemente potentes, un tratamiento de control del acceso y por tanto del tratamiento de datos suficientemente estricto y

sobre la base de marcos de datos que protejan suficiente la intimidad. Cualquier defecto en este sentido podría socavar la confianza pública y llevar a las personas a los peligros del robo de identidad, el daño al crédito o el uso indebido de información privada por parte de actores públicos o bien corporativos. Otra grave preocupación es la erosión paulatina de la experiencia y de la independencia humanas. A medida que aumenta la dependencia de las herramientas de IA, existe un grave riesgo de que los profesionales del derecho empiecen a someterse acríticamente a las recomendaciones algorítmicas, perdiendo poco a poco el rigor analítico y el juicio independiente que caracteriza la profesión. Poco a poco, esto podría reducir a la existencia de un efecto de “de cualificación” (lo que equivaldría a que los abogados y jueces pasan a ser consumidores pasivos de resultados automatizados y no intérpretes activos del derecho). Para evitar esto, conviene que la IA sea entendida no como un reemplazo de la inteligencia humana, sino como un aparato de soporte —un aparato que permita la ejecución de los poderes profesionales —siempre bajo el control humano. La educación jurídica debe también perfeccionarse en esta dirección, proveyendo a los futuros juristas de la educación técnica que les permita evaluar críticamente los resultados de la IA, examinar las opiniones equivocadas y actuar cuando convenga. Igualmente, la introducción de la IA en el orden jurisdiccional corre el riesgo de agravar las desigualdades que existen. Dado que el acceso o no acceso a la infraestructura digital, la alfabetización tecnológica y el conocimiento sobre las plataformas basadas en la IA, se distribuyen desigualmente en la sociedad, las poblaciones vulnerables —aquellas que ya experimentan desventaja respecto a lo que es el conocimiento, la pobreza, bajos niveles de educación, o la dificultad de acceso al centro de información— se verían en mayor escalón en el vagón ya que estarían en el más completo oscurantismo y no fácilmente podrían navegar por el medio ambiente de decisiones algorítmicas. Esto podría dar origen a la formación de una nueva brecha, o como, por ejemplo, un sistema con una justicia dualista, en el que quienes tienen recursos se ven favorecidos de servicios más veloces y acertados y a la vez otros llegan a recibir, por el contrario, resultados que son oscuros, inaccesibles y posibles, no injustos. Tal situación contradice su propio principio de igualdad de acceso a la justicia que es parte misma del fundamento de las democracias constitucionales. Regresando a continuación a la implantación más general de la IA en las instituciones del gobierno de justicia, es importantísimo el hecho de tener presente que la IA está referida a un campo multidisciplinario, dada la existencia de la misión constructiva referida a la serie de sistemas computacionales, capaces de simular las funciones intelectuales de los hombres —pudiendo aprender de la experiencia, identificar patrones, inferir conclusiones, solucionar problemáticas y decidir. Las recientes conquistas en poder computacional, el crecimiento exponencial de los datos digitales y las innovaciones en lo que se llama “aprendizaje automático”, han llevado la IA a campos que eran considerados antes inmunes a la automatización.

Desde el diagnóstico de enfermedades en el sector salud, hasta la optimización de estrategias de inversión en finanzas, el impacto de la IA se expande. Su alcance toca ahora también al sector jurídico, cautivando a académicos, autoridades en la formulación de políticas y profesionales en derecho por igual.

Pero en Ecuador, esta ola transformativa aún no ha tenido un contacto a fondo con el sistema de justicia. No existe por ahora ninguna plataforma inteligente que respalde la acción de la justicia o la administración pública; no hay un proyecto, una hoja de ruta, que otorga acceso a la digitalización de los procesos legales. Lo que se vive es un estancamiento total ante el acelerado ritmo del desarrollo digital en el mundo. Por esta razón, las garantías constitucionales, especialmente el derecho al acceso oportuno y efectivo a la justicia, se ven cada vez más fregadas por la inercia institucional. La comprensión actual y en evolución de la justicia, tiene en cuenta la accesibilidad digital, la eficiencia procesal, la adecuación tecnológica, etc., estándares estos que no han sido cumplidos como consecuencia de la no modernización de ninguna instancia. A efecto de compensar esta vacuidad se ha realizado un profundo estudio de la literatura existente, buscando soluciones posibles basadas en la IA que sean adaptables al marco de justicia penal en Ecuador, principalmente aquéllas que se relacionen con el proceso ordinario. Con suficiente voluntad política y razonables desembolsos de dinero público, algunos de estos instrumentos no sólo son imaginables, sino alcanzables. De esta manera, al examinar la IA en su modalidad de impacto en los flujos de trabajo de la investigación, estrategia fiscal, procesos en tribunales, poniendo en la balanza sus beneficios y sus riesgos éticos, este análisis invita a imaginar una nueva forma de hacer justicia, instando a todos los interesados a pensar en un futuro donde la tecnología no sustituya la agencia humana, sino que la complemente.

Aportando al respecto, la IA presenta una promesa muy real para el mejoramiento del desempeño judicial. Puede automatizar trabajos rutinarios y administrativos —como la programación de audiencias, la organización de expedientes, la preparación de formularios legales estándar o la ordenación de materia probatoria—, de tal modo que, en vez de pasar horas haciendo estas tareas, el juez o el abogado puede dedicar su tiempo a razonar sobre las cuestiones jurídicas primordiales. En jurisdicciones donde se presenta una abultada acumulación de casos, como en la de las industrias de litigios masivos acerca de cláusulas hipotecarias, derivados financieros o controversias bancarias, la IA podría también acortar drásticamente los tiempos de respuesta. Así, en vez de esperar por meses —o aún años— la fijación de día de juicio o la resolución final, los ciudadanos podrían recibir oportunas respuestas, lo que restauraría la confianza pública en un sistema que muchas veces se percibe como lento e inaccesible.

Más allá de la cuestión de la eficiencia, la IA tiene también el potencial de mejorar la calidad de la administración de la justicia. La posibilidad de que sistemas de IA examinen vastos acervos de jurisprudencia, estatutos y precedentes puede, por ejemplo, aportar principios jurídicos relevantes, resaltar argumentos pasados por alto y señalar tendencias entre casos similares. Hacer esto no tiene otra finalidad que otorgar información más abundante a los jueces, de tal manera que puedan abordar cada pleito con un conjunto más claro y útil de información —con ello disminuye la posibilidad de que se omitan cuestiones jurídicas o fácticas y se obtenga un resultado inconsistente. Aparte de ello, como los algoritmos se basan en datos y no en impresiones subjetivas, pueden ayudar a moderar la influencia de los sesgos inconscientes —tendencias personales que ajenas a la razón pueden influir, si bien sutilmente, el criterio humano. Teóricamente, esto puede llevar a mejores resultados, más equitativos y objetivos, fundados en hechos y no en emociones personales o prejuicios.

Entre otras ventajas se encuentran las que se refieren a menores costos y a una disminución del error. El error humano —ya sea en la transcripción, en la cita o en la evaluación de la prueba— puede tener la consecuencia de engendrar apelaciones, nuevos juicios o errores judiciales. Las herramientas de IA pueden, entre otras cosas, (i) autoevaluar los hechos, (ii) verificar citas y (iii) indicar desavenencias, lo que llevará a una mayor exactitud y a la reducción de costos que encierran las correcciones de errores. Asimismo, el análisis de datos puede ayudar a los administradores judiciales a calcular (i) la frecuencia de carga de casos, (ii) la correcta asignación de jueces y (iii) a llevar a cabo una distribución de la carga de trabajo entre jurisdicciones, disminuyendo así los congestionamientos y ayudando a un mejor aprovechamiento de los recursos.

No obstante, lo anterior, el optimismo que acompaña a la palabra IA debe ser moderado con la debida moderación que este término solicita. Aun en 2025, la infraestructura judicial del Ecuador no se encuentra todavía adecuadamente preparada para la adopción generalizada de la IA. Las funcionalidades digitales básicas —como la conferencia de tipo Skype que hace posible que comuníquense en forma cotidiana las partes en la litis en audiencias remotas o la existencia de sistemas fiables de presentación electrónica de escritos— siguen adoleciendo de las deficiencias que le son inherentes a la incompetencia técnica y sobrecarga del sistema. Ello revela una verdad más profunda: la administración de justicia debe haber llegado primero a una madurez digital elemental antes de llegar a adoptar la tecnología de punta. Una adopción prematura, llevada sin observación de materias o carencias, sólo podría servir para empeorar la situación existente.

Un peligro que se presenta con cierta premura —que ataca el mismo fondo de la prueba que puede considerarse creíble— es la facilidad con que la IA puede manipular el contenido digital. Las

grabaciones sonoras, las fotografías y las grabaciones de imagen eran antes consideradas como prueba perfectamente verificada, hoy se encuentran sometidas a una fácil falsificación y manipulación en manos de quienes utilizan las tecnologías “deepfake” y de IA generativa mediante las operaciones de modelado que éstas introducen. Un si el modelo obtenido, la voz del clonado, puede obtenerse en forma bastante eficiente, una conversación también puede ser construida, una fotografía puede alterar su contenido más allá de la detección, todo ello con el escaso infringir el proceso lógico de modelo de obtención con bastante fácil esperanza. En cuanto a los juicios judiciales, en que son los peritos los que suelen autenticar su existencia, la carga de verificación se torna exponencialmente mayor. En la actualidad, el mejor método de descubrimiento es la consulta de los metadatos —las huellas digitales que determinan el origen de un documento, su lectura y su prosecución—. Sin embargo, esos datos pueden ser suprimidos y/o recreados, haciendo la tarea de descubrimiento excesivamente difícil.

Esta eventualidad es grave: la posible legitimación de la fabricación de pruebas que ahora se crean. En el caso que las partes no pueden estar seguras de la autenticidad de lo que ven o escuchan, la búsqueda de justicia se ha hecho más fácil, ya no es tal la búsqueda de la justicia, ha pasado a ser importante lo que ven o escuchan las partes. Por este motivo, el profesional del derecho deberá adquirir la competencia de informática forense, adquirirá materiales que sean utilizados para la verificación de los datos y creará protocolos rigurosos en la admisión de documentos que hayan sido elaborados por IA o que hayan sido alterados a consecuencia de su parte. En conclusión, a pesar de que la IA ha llegado, como ya se dijo, para quedarse —y que tiene un papel de real importancia que desempeñará en el futuro de la justicia—, este aspecto no es uno que debe traerse a colación y la comprobación del tema se halla ligada al de la responsabilidad que la propia IA exige. Los profesionales del derecho, sobre todo los litigantes, deben prepararse para este cambio adoptando el conocimiento y las habilidades que se requieren para convivir en este nuevo entorno. La inteligencia artificial puede automatizar ciertas funciones y ser un potente soporte en el análisis, pero no puede (ni debe) asumir el papel de autoridad judicial. La responsabilidad última de decisiones, estrategias y de la ética en el juicio tiene que seguir en manos humanas. La creación de un marco jurídico y ético determinado —que fije las fronteras del uso de la IA, la asigne responsabilidades, y proteja la sacralidad de la justicia— no es sólo deseable, sino plenamente necesaria. Entonces y sólo entonces, puede ser la IA una fuerza de progreso, en lugar de una fuente de peligro, en la búsqueda de un sistema justo y equitativo de leyes. (Islant, 2025).

Desarrollos Jurisprudenciales y Legislación sobre Inteligencia Artificial en el Derecho Penal

El avance acelerado e imparable de la tecnología ha introducido la inteligencia artificial en el corazón del campo jurídico, con un potencial transformador y a la vez retos profundos. No es sólo un hecho técnico, sino una experiencia que exige una concepción profundamente integrada y multidisciplinaria, que se afine con el paso del derecho con el paso acelerado de la innovación tecnológica. Sólo con esta concepción sinérgica, puede la sociedad aspirar a obtener resultados dentro de los que se den paso a la justicia, la equidad y el bien social que debe estar en el centro de todo Estado de Derecho. A medida que la IA continúe imprimiendo su influencia a la actividad judicial y a la toma de decisiones, resulta indispensable que los operadores jurídicos no sólo se adapten a este proceso, sino que busquen activamente su relación con estos nuevos sistemas. Este proceso exige un esfuerzo en forma continuada por la educación de los propios operadores, el conocimiento de los avances de la tecnología, y la formación de un conocimiento pluralista de cómo funciona efectivamente la IA, particularmente en el sentido que tiene en defensa de un conjunto de derechos fundamentales, como la privacidad, la transparencia y la defensa contra la discriminación. En el nuevo panorama que se va dibujando, la administración de justicia no es ya sólo responsabilidad del criterio humano, sino que parte de ella es intermediada, determinada, o formateada, incluso, por los sistemas algorítmicos. Este proceso pone en evidencia la urgentísima conveniencia de una revisión crítica de los marcos jurídicos existentes y la introducción de un profundo sentido ético en el diseño e implantación de las herramientas de IA en la actividad judicial (Farfán Intriago, 2023). La relación de la inteligencia artificial con el ejercicio de la actividad jurídica no es sólo una actualización del sistema, sino que es una oportunidad para mejorar el ejercicio de la actividad jurídica con toda la ciencia y dignidad que el Estado debe prestar en esta materia. Cuando se utilice la IA con sentido probable, aparecerá un conjunto de posibilidades que crecerá apreciablemente la capacidad del ejercicio del derecho, constituyéndose en el fondo una actividad mucho más ágil y resiliente. Uno de los primeros efectos benéficos se hallará en el terreno de la eficacia operativa. Los sistemas de innovación de tipo IA puede haber de por sí, una carga de tareas rutinarias y muy absorbentes en cuanto tiempo (revisión de documentos, investigaciones jurídicas, redacción de algunos contratos, clasificación de expedientes, etc.) quedando así los operarios del derecho, liberados de la sobrecarga que el trabajo administrativo produce. Así, la digestión que se puede obtener en el ejercicio ordinario del trabajo jurídico, es por sí, ya una esperada mejora, pero el individuo que utiliza la IA automáticamente se dedicara a temas de un nivel que necesitan una inteligencia superior: el análisis estratégico, los litigios complejos, la formulación de políticas y la

defensa de los clientes. Esta transferencia de energías productivas no sólo repercute en la eficacia en el desarrollo ordinario de la ocupación profesional, sino arrastrará la calidad de los juicios y del razonamiento jurídico, con unos resultados que mejorarán los resultados que se obtienen en la práctica del derecho (Farfán Intriago, 2023). (...) Si bien en el ámbito administrativo, la IA muestra posibilidades muy digeridos, se encuentra por sí mismo, en el ejercicio como asistente inteligente en el desarrollo de las soluciones de conflictos y en la administración de justicia. Los sistemas de IA pueden, por medio de algoritmos de incuestionable eficacia, estudiar todo un conjunto de fuentes que versen sobre este tema, desde los precedentes hasta las resoluciones anteriores, a la vez que se recogen las tendencias de la jurisprudencia, en esos nuevos sistemas, incorporando jurisprudencia, que con anterioridad no era analizable en su contexto. De este modo, el profesional del derecho puede recurrir a resoluciones que se produjeran en tiempos pasados de un modo mucho más eficaz y efectivo, asegurando la congruencia de sus decisiones y como consecuencia la creación de coherencia de su contenido, en cuanto al derecho penal. De manera que, el aprendizaje por la legislación de resoluciones anteriores permitirá predecir sus consecuencias jurídicas, sus comportamientos del magistrado, y aún dar recomendaciones de su actuación conducidas por datos, instrumentos que, sin duda, si se pone en práctica en una forma responsable, redundará en la integridad y previsibilidad del derecho.

Quizás la contribución más convincente de la IA se da en el ámbito del principio de igualdad ante la ley. Los tomadores de decisiones, a pesar de sus mejores intenciones, son indefectiblemente vulnerables a sesgos implícitos, ya sean culturales, cognitivos o institucionales. La IA, siempre que se la diseñe debidamente y se realicen auditorías rigurosas, ofrece un camino para que se mitiguen tales para introducir mecanismos de evaluación más objetivos a los procesos legales. Cuando es entrenada por data diversas y representativas y es manejada por protocolos transparentes, la IA reduce las disparidades en las sentencias, mejora el acceso a los recursos judiciales y asegura que los sujetos sean tratados con justicia, sin importar su raza, género, condición socioeconómica u origen (Calo, 2017). De este modo, la inteligencia artificial es no solo un instrumento de conveniencia, sino un guardián de la equidad, un mecanismo por el cual el sistema judicial puede acercarse a su ideal de imparcialidad o justicia universal. Finalmente, la convergencia del legal y la inteligencia artificial tiene un sentido de evento histórico definitivo en el ámbito del derecho. Este desarrollo conlleva un nuevo tipo de profesionalismo, o de actitud profesional, por parte de los jurídicos, un profesionalismo que admite la fluidez tecnológica, pero no debe sacrificar la ética y que contempla la innovación no por sí misma sino en términos de justicia, y rendición de cuentas, y de la dignidad humana.

Conclusiones

La inteligencia artificial, IA, se define aquí como un mecanismo que puede alentar un cambio importante en el acceso y en la ejecución de las leyes penales, así como de las instituciones judiciales, al permitir un número importante de mejoras en cuanto a eficiencia, precisión, análisis informático, así como automatización de procedimientos complejos. Si es introducido debidamente, esto puede resultar en un cambio en la duración de los procesos, el fortalecimiento de las decisiones, como así también aliviar las cargas de las fiscalías y los tribunales, especialmente en aquellos casos que, fundamentalmente, son repetitivos o que requieren una gran cantidad de actividad documentaria. Sin embargo, este mismo potencial tiene un costo y nos introduce a nuevos problemas que requieren ser analizados desde el punto de vista no solo jurídico sino ético y constitucional. Son problemas de bastante relevancia los que provienen de la opacidad de los propios sistemas algorítmicos destinados para los diferentes tipos de IA que funcionan, en donde hay poco margen de cuestionamiento o de auditoría o de ninguna manera de fiscalización de su lógica interna limitada que brinda la oportunidad de defensa y la garantía del derecho a una justicia integral. También existe el peligro de que se perpetúen o de que se amplifiquen las falencias discriminatorias inherentes a los estándares de IA mediante la carga de data, que da lugar a vulneraciones de varios principios de igualdad y de justicia. Finalmente, por la cantidad de data y la forma en que se presenta la información en tipos de sistemas como el SATJE, el cual es permanente y visible también, da lugar a la cuestión de la pertinencia y a la cuestión de las leyes de protección de la data y en forma general del derecho a la información no ya solo del tipo de data que lleva, sino de toda la información con que se pueda acceder, lo que enfrenta a contraposición al acceso a la justicia y en particular de los derechos de defensa.

Así, en este contexto, se vuelve indispensable establecer un marco normativo que garantice principios, criterios tecnológicos y limitaciones que permitan el adecuado uso de la IA, así como auditorías o supervisiones humanas de las decisiones que adoptan estos sistemas por la vía automatizada. La IA debe ser un instrumento de ayuda y soporte de la decisión de los jueces, no su reemplazo o exclusión. La figura del juez como garante de los derechos fundamentales y de la legalidad y justicia sustantivas no puede ser sustituida por algoritmos, ya que la naturaleza social y política del derecho excede el auto computo. Así mismo, la introducción de esta tecnología debe hacerse desde una perspectiva interdisciplinaria que permita la exploración cuidadosa de su potencial, mediante la consideración de las diversas áreas del derecho, de la tecnología, de la ética, de la gestión de registros, de la informática forense y de las políticas públicas. Esto permitirá construir sistemas confiables que cumplan con los estándares internacionales de derechos humanos y que contribuyan a consolidar el Estado de derecho en general y el sistema de justicia ecuatoriano

en especial. Finalmente, resulta imprescindible fomentar planes de capacitación para los jueces con el fin de garantizar que no se vean lesionados de desigualdades en el uso de las tecnologías. La replicabilidad y auditabilidad son características que hay que garantizar para dar satisfacción a las exigencias de que la IA sirva para consolidar y no para debilitar la justicia. A través de estas será posible garantizar la transparencia, la lucha contra la discriminación, la prevención de la arbitrariedad y la garantía del derecho a la explicación y participación en las decisiones que toman estos sistemas. Simultáneamente, deben llevarse a cabo investigaciones con el fin de hallar buenas prácticas, experiencias, desafíos y debilidades derivados de la aplicación de la IA en el derecho penal a nivel internacional, que sean susceptibles de ser adaptadas al contexto ecuatoriano. De igual modo, se vuelve vital consolidar la digitalización de los procesos y expedientes por medio de sistemas de gestión de causas electrónicos que faciliten la interoperabilidad entre los tribunales, para garantizar que la automatización de procesos no agrave los problemas existentes. En conclusión, la modernización del sistema judicial ecuatoriano requiere de una planificación estratégica y de un fortalecimiento estructural. Por otro lado, la aplicación de la IA exige cautela para la satisfacción de los principios probatorios y la garantía de los derechos fundamentales. Así las cosas, resulta de toda necesidad enfatizar que el uso de esta tecnología debe darse conforme a los principios de proporcionalidad, rendición de cuentas, igualdad y transparencia para garantizar la justicia sustantiva.

GLOSARIO JURÍDICO A-Z

*(Diccionario técnico del procedimiento
coactivo y derecho administrativo)*



A

Acto administrativo

Declaración unilateral de voluntad emitida por una autoridad de la administración pública en ejercicio de una potestad legal, destinada a producir efectos jurídicos individuales o generales. Se presume legítimo y ejecutable mientras no sea declarado inválido por autoridad competente.

Administración pública

Conjunto de órganos, instituciones y entidades del Estado encargados de ejecutar las políticas públicas y aplicar el ordenamiento jurídico mediante actos administrativos orientados a la satisfacción del interés general.

Administrado

Persona natural o jurídica que se encuentra sometida a la actuación de la administración pública y que puede resultar destinataria de derechos u obligaciones derivadas de un acto administrativo.

Autotutela administrativa

Prerrogativa jurídica que permite a la administración pública declarar y ejecutar sus propios actos sin necesidad de obtener previamente una sentencia judicial, siempre que exista habilitación legal y respeto a las garantías del debido proceso.

Autotutela ejecutiva

Manifestación específica de la autotutela administrativa que faculta a la administración a ejecutar directamente sus decisiones mediante mecanismos coercitivos para asegurar el cumplimiento de obligaciones frente al Estado.

B

Bien embargado

Elemento patrimonial del deudor que es afectado mediante una medida cautelar dentro del procedimiento de ejecución coactiva para garantizar el pago de una obligación exigible.

Bien mueble

Objeto susceptible de traslado físico que puede ser objeto de embargo, retención o remate dentro de un procedimiento de ejecución.

Bien inmueble

Propiedad raíz, como terrenos o edificaciones, que puede ser objeto de medidas cautelares o ejecución dentro de un proceso coactivo.

Buena fe administrativa

Principio jurídico que exige que tanto la administración como los administrados actúen con honestidad, lealtad y confianza en las relaciones jurídicas administrativas.

C

Coactiva

Procedimiento administrativo especial mediante el cual una entidad pública ejecuta el cobro forzoso de obligaciones líquidas, determinadas y exigibles a favor del Estado.

Cobro coactivo

Actividad administrativa dirigida a obtener el pago de obligaciones frente al Estado mediante la utilización de mecanismos de apremio como embargo, retención o remate.

Competencia administrativa

Facultad legal otorgada a un órgano de la administración pública para ejercer determinadas funciones dentro de los límites establecidos por la Constitución y la ley.

Control jurisdiccional

Facultad de los tribunales para revisar la legalidad de los actos administrativos y garantizar la protección de los derechos fundamentales de los administrados.

Citación

Acto procesal mediante el cual se comunica formalmente a una persona la existencia de un procedimiento administrativo o judicial que le afecta.

D

Debido proceso

Principio constitucional que garantiza a toda persona el derecho a ser oída, defenderse y obtener una decisión motivada dentro de cualquier procedimiento administrativo o judicial.

Deudor

Persona natural o jurídica obligada al cumplimiento de una obligación frente a la administración pública.

Delegación administrativa

Acto mediante el cual una autoridad administrativa transfiere temporalmente el ejercicio de una competencia a otro funcionario, manteniendo la titularidad de la potestad.

Determinación administrativa

Acto mediante el cual la administración establece la existencia de una obligación a cargo de un administrado.

E

Ejecución coactiva

Procedimiento administrativo de ejecución forzosa que permite a la administración pública cobrar obligaciones exigibles mediante mecanismos coercitivos.

Ejecutor coactivo

Funcionario administrativo encargado de dirigir y tramitar el procedimiento de ejecución coactiva dentro de una entidad pública.

Embargo

Medida cautelar que recae sobre bienes del deudor con el fin de garantizar el pago de una obligación.

Excepción procesal

Mecanismo de defensa que permite al deudor oponerse a la ejecución coactiva cuando se configura una causa legal que impide el cobro.

F

Fase de apremio

Etapas del procedimiento coactivo en la cual la administración utiliza medidas coercitivas para obtener el cumplimiento de una obligación.

Funcionario ejecutor

Servidor público responsable de impulsar el procedimiento coactivo y dictar las providencias necesarias para la ejecución de la deuda.

Fisco

Conjunto de recursos financieros pertenecientes al Estado destinados a la financiación de las actividades públicas.

G

Garantías constitucionales

Conjunto de mecanismos jurídicos destinados a proteger los derechos fundamentales frente a actuaciones arbitrarias del poder público.

Gestión administrativa

Actividad desarrollada por los órganos del Estado para cumplir con las funciones públicas asignadas por el ordenamiento jurídico.

H

Habilitación legal

Autorización expresa otorgada por la ley que permite a una autoridad administrativa ejercer determinadas competencias.

Hetero tutela judicial

Sistema mediante el cual la resolución de conflictos se encomienda a un órgano jurisdiccional independiente.

I

Impugnación administrativa

Acción mediante la cual un administrado solicita la revisión o anulación de un acto administrativo que considera ilegal o lesivo.

Imperium estatal

Poder coercitivo del Estado que le permite imponer el cumplimiento de obligaciones mediante el uso legítimo de la fuerza pública.

J

Juez de coactiva

Funcionario administrativo que ejerce la potestad de ejecución coactiva dentro de una entidad pública.

Jurisdicción contencioso-administrativa

Rama de la jurisdicción encargada de resolver los conflictos entre la administración pública y los particulares.

L

Legalidad administrativa

Principio según el cual toda actuación de la administración debe estar fundada en una norma jurídica que la autorice.

Liquidez de la obligación

Condición jurídica que implica que la cuantía de una deuda está determinada de manera exacta.

M

Medida cautelar

Actuación provisional destinada a asegurar la eficacia de una futura decisión administrativa o judicial.

Motivación del acto administrativo

Exposición clara de las razones jurídicas y fácticas que justifican la emisión de un acto administrativo.

N

Notificación

Acto procesal mediante el cual se comunica formalmente a una persona la existencia de un acto administrativo o providencia.

Nulidad administrativa

Sanción jurídica que priva de efectos a un acto administrativo cuando ha sido emitido con violación del ordenamiento jurídico.

O

Obligación exigible

Deuda que ha vencido y puede ser legalmente exigida por el acreedor.

Oficiosidad administrativa

Principio según el cual la administración debe impulsar de oficio los procedimientos de su competencia.

P

Potestad coactiva

Facultad de la administración pública para ejecutar el cobro de obligaciones sin intervención judicial previa.

Presunción de legalidad

Principio según el cual los actos administrativos se consideran válidos y eficaces mientras no sean anulados por autoridad competente.

Procedimiento administrativo

Conjunto ordenado de actos destinados a producir una decisión administrativa.

R

Remate

Venta pública de bienes embargados con el fin de satisfacer una obligación.

Retención de valores

Medida cautelar mediante la cual se inmovilizan fondos del deudor para garantizar el pago de una deuda.

S

Secretario de coactiva

Funcionario encargado de certificar las actuaciones dentro del procedimiento coactivo y garantizar la legalidad documental del proceso.

Seguridad jurídica

Principio que garantiza estabilidad y previsibilidad en la aplicación del derecho.

T

Título de crédito

Documento administrativo que acredita la existencia de una obligación líquida, determinada y exigible a favor de una entidad pública y que sirve de base para iniciar la ejecución coactiva.

Tutela judicial efectiva

Derecho fundamental que garantiza el acceso a los tribunales para la protección de los derechos e intereses legítimos.

V

Validez del acto administrativo

Condición jurídica que determina que un acto administrativo cumple con los requisitos legales de competencia, forma y finalidad.

Vía de apremio

Procedimiento mediante el cual la administración ejecuta forzosamente una obligación.

Z

Zona de jurisdicción administrativa

Ámbito territorial dentro del cual una autoridad administrativa puede ejercer válidamente sus competencias.

AUTORES



AB. DIANA ELIZABETH CORREA MANZANO. MG.

Biografía

Abogada de los Tribunales y Juzgados de la República del Ecuador, graduada en la Universidad Central del Ecuador. Maestría en Derecho Penal y Criminología por la Universidad Regional Autónoma de Los Andes (UNIANDES) y actualmente cursa una Maestría en Derecho Procesal y Litigación Oral en la Universidad Indoamérica; Litigante y docente universitaria.



AB. JOSÉ FABIÁN MOLINA MORA. MG.

Biografía

Abogado de los Tribunales de la República (UNIANDES)
Diplomado en Arbitraje y Mediación (UTEQ)
Diplomado en Compras Públicas (Formativa)
Especialista en Derecho Administrativo (UASB)
Magister en Derecho Procesal y Litigación Oral (UISEK)
Candidato a PhD en Derecho con mención en
Derecho Constitucional (UCAB)
Docente a tiempo completo en la Universidad Regional
Autónoma de Los Andes "UNIANDES Quevedo"
Docente investigador de la Universidad Regional
Autónoma de Los Andes "UNIANDES Quevedo"
Miembro de la Red Koinonia Revista Arbitrada.

AB. CÉSAR ELÍAS PAUCAR PAUCAR. MG.

Biografía

Abogado, Magister en Derecho Penal y Criminología, Magister en Derecho Constitucional, Especialista en Derecho Penal y Justicia Indígena, Diploma Superior en Contratación Laboral, Juez de Garantías Penales, Juez del Tribunal de Garantías Penales de Quevedo, docente de pregrado en Universidad Regional Autónoma de Los Andes Uniandes, candidato a Doctor en Derecho por la U.N. de Mar del Plata – Argentina, Magister en Derecho Penal (c).



AB. CINTHIA MARIELA CAJAS PÁRRAGA MG.

Biografía

Abogada, Magister en derecho constitucional, Jueza Civil, Multicompetente y actualmente de Adolescentes Infractores, docente de la Universidad Regional Autónoma de Los Andes Uniandes, candidata a Doctora en Derecho por la U.N. de Mar del Plata-Argentina, Especialista en DDHH y Justicia Juvenil Restaurativa (c) y Magister en Derecho Penal (c).

Referencias

- Aguilera García, E. R. (2020). *Inteligencia artificial aplicada al derecho*. Universidad Nacional Autónoma de México.
- Albán, E. (2015). *Manual de Derecho Penal Ecuatoriano* (Vol. I). Quito: Ediciones Legales EDLE S.A.
- Ashley, K. D. (2017). *Artificial intelligence and legal analytics: New tools for law practice in the digital age*. Cambridge University Press.
- Asamblea Nacional Constituyente del Ecuador. (2008). *Constitución de la República del Ecuador*. Registro Oficial 449.
https://www.defensa.gob.ec/wp-content/uploads/downloads/2021/02/Constitucion-de-la-Republica-del-Ecuador_act_cne-2021.pdf
- Asamblea Nacional del Ecuador. (2002). *Ley de Comercio Electrónico, Firmas y Mensajes de Datos*. Registro Oficial Suplemento 557.
<https://www.telecomunicaciones.gob.ec/ley-de-comercio-electronico-firmas-y-mensajes-de-datos>
- Asamblea Nacional del Ecuador. (2009). *Ley Orgánica de Garantías Jurisdiccionales y Control Constitucional*.
<https://vlex.ec/vid/ley-organica-garantias-jurisdiccionales-643461681>
- Asamblea Nacional del Ecuador. (2010). *Ley del Sistema Nacional de Registro de Datos Públicos*.
<https://vlex.ec/vid/ley-sistema-nacional-registro-643461673>
- Asamblea Nacional del Ecuador. (2014). *Código Orgánico Integral Penal (COIP)*. Registro Oficial Suplemento 180.
<https://www.defensa.gob.ec/wp-content/uploads/downloads/2024/05/COIP.pdf>
- Asamblea Nacional del Ecuador. (2021). *Ley Orgánica de Protección de Datos Personales*.
<https://vlex.ec/vid/ley-organica-proteccion-datos-868545422>
- Asamblea Nacional. (10 de febrero de 2014). *Código Orgánico Integral Penal*. Registro Oficial Suplemento 180. Quito, Ecuador.
- Asamblea Nacional. (17 de febrero de 2021). *Ley Orgánica Reformatoria al Código Orgánico Integral Penal en materia Anticorrupción*. Registro Oficial Suplemento 392. Quito, Ecuador.
- Asamblea Nacional. (24 de junio de 2005). *Código Civil*. Registro Oficial Suplemento 46. Quito, Ecuador.
- Barocas, S., Hardt, M., & Narayanan, A. (2019). *Fairness and machine learning: Limitations and opportunities*. MIT Press.
- Basco, A. I., Beliz, G., Coatz, D., & Garner, P. (2018). *Industria 4.0: Fabricando el futuro* (Vol. 647). Inter-American Development Bank.
<https://doi.org/10.18235/0001229>
- Binder, A. (2016). *Introducción al derecho procesal penal*. Ad-Hoc.

- Cárdenas, E. R., & Molano, V. M. (2021). Un estudio sobre la posibilidad de aplicar la inteligencia artificial en las decisiones judiciales. *Revista Direito*, 17.
<https://doi.org/10.1590/2317-6172202101>
- Casanovas, P. (2020). Inteligencia artificial y derecho: A vuelapluma. *Teoría & Derecho*.
<https://ojs.tirant.com/index.php/teoria-y-derecho/article/view/248>
- Congreso Nacional [Senado y Cámara de Diputados]. (1971). *Código Penal*. Registro Oficial Suplemento 22. Quito, Ecuador.
- Congreso Nacional. (2005). *Ley No. 2*. Registro Oficial 45. Quito, Ecuador.
- Consejo de la Judicatura. (2014). *Plan Estratégico de la Función Judicial 2013–2019*. Quito, Ecuador.
- Constitución de la República del Ecuador. (2008). Registro Oficial No. 449.
- Convención de las Naciones Unidas contra la Corrupción. (2004). Nueva York, Estados Unidos.
- Donna, E. (1996). *Teoría del delito y de la pena* (2.^a ed.). Buenos Aires: Astrea.
- Escobar-Escobar, G. A., Arteaga-Jaramillo, H. R., & Jiménez-Lizarazo, F. A. (2024). La inteligencia artificial generativa y su impacto en la administración de justicia. *Revista Con-Justicia*, 7(13), 259–278.
<https://doi.org/10.62574/mr9wjn56>
- Farfán Intriago, J. L., Farfán Largacha, J. A., Farfán Largacha, B., & Núñez Vera, J. P. (2023). Inteligencia artificial y Derecho. *Frónesis*, 30(2), 173–197.
- Ferrajoli, L. (2011). *Derecho y razón: Teoría del garantismo penal*. Trotta.
- Gamba Cifuentes, G. (2021). *La inteligencia artificial (IA) y su implementación en la prueba*. Universidad Libre.
- Garland, D. (2001). *The culture of control: Crime and social order in contemporary society*. Oxford University Press.
- Gogolin, G. (2021). The challenge of artificial intelligence for criminal law. *Artificial Intelligence and Law*, 29(3), 295–314.
<https://doi.org/10.1007/s10506-021-09296-5>
- Hernández Martínez, D. F. (2021). Inteligencia artificial, Derecho Penal y compliance. *Revista Mexicana de Ciencias Penales*, 4(14), 63–70.
<https://doi.org/10.57042/rmcp.v4i14.434>
- Katz, D. M., Bommarito, M., & Blackman, J. (2017). A general approach for predicting the behavior of the Supreme Court of the United States. *PLOS ONE*, 12(4), e0174698.
<https://doi.org/10.1371/journal.pone.0174698>
- Larrea Holguín, J. (2010). *Enciclopedia Jurídica Ecuatoriana*. Quito: Fundación Latinoamericana Andrés Bello.
- López, F. O. (2024). *Fundamentos para un derecho de la inteligencia artificial*. Tirant lo Blanch.
- Martín Esquivel, S. (2021). *Corrupción en la administración pública y formas de prevenirla*.

- Meythaler, J. (2021). *La corrupción privada y la responsabilidad penal de las personas jurídicas*. Quito, Ecuador.
- Mila, F. (2020). La responsabilidad penal de las personas jurídicas en el derecho ecuatoriano. *Ius et Praxis*, 149–170.
http://www.scielo.cl/scielo.php?script=sci_arttext&pid=S0718-00122020000100149
- Ministerio de Telecomunicaciones y Sociedad de la Información. (2022). *Estrategia Nacional de Ciberseguridad*.
<https://asobanca.org.ec/wp-content/uploads/2022/08/ESTRATEGIA-NACIONAL-DE-CIBERSEGURIDAD-DEL-ECUADOR-2022.pdf>
- Mir, S. (2016). *Derecho Penal Parte General* (10.a ed.). Barcelona: Reppertor.
- Mora Bernal, A. E., Sánchez Sarmiento, M. P., Cajamarca Torres, A. E., & Idrovo Torres, D. (2022). El sistema automático de trámite judicial. *Revista Chilena de Derecho y Tecnología*, 11(1), 203–228.
- Muñoz, F., & García, M. (2010). *Derecho Penal Parte General* (8.a ed.). Valencia: Tirant lo Blanch.
- Muñoz, R. (2020). *Las TICs en la administración pública*. Universidad de Friburgo.
- Olivares, L. E. (2024). Por primera vez, la ONU adopta resolución para regular la IA. *Agenda Estado de Derecho*.
- Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura (UNESCO). (2022). *La IA y el Estado de derecho*.
<https://www.unesco.org/es/artificial-intelligence/rule-law/mooc-judges>
- O’Neil, C. (2016). *Weapons of math destruction: How big data increases inequality and threatens democracy*. Crown Publishing.
- Ossorio, M. (s.f.). *Diccionario de ciencias jurídicas, políticas y sociales* (Ed. electrónica). Ciudad de Guatemala: Datascan.
- Quintero, M. E. (2012). *Persona jurídica y Derecho penal*. UNAM.
<https://archivos.juridicas.unam.mx/www/bjv/libros/7/3169/4.pdf>
- Real Academia Española. (s. f.). *Diccionario de la lengua española*. <https://dle.rae.es>
- Riestra Gaytán, E. (1995). *Informática jurídica aplicada a la enseñanza del Derecho*. UNAM.
- Russell, S., & Norvig, P. (2021). *Artificial intelligence: A modern approach* (4th ed.). Pearson.
- Solar Cayón, J. I. (2020). La inteligencia artificial jurídica. *Revus*, 41.
<https://doi.org/10.4000/revus.6547>
- Susskind, R. (2019). *Online courts and the future of justice*. Oxford University Press.
- Tamayo y Salmorán, R. (1984). La persona jurídica. En J. Barrera (Ed.), *Estudios de derecho en memoria a Roberto Mantilla* (pp. 733–745). México: Porrúa.
- Tique-Onatra, L. Á. (2018). *La responsabilidad del Estado colombiano como consecuencia de la mora judicial*. Universidad Católica de Colombia.
- Tonry, M. (2011). *Punishing race: A continuing American dilemma*. Oxford University Press.

- Valdés Téllez, J. (2020). *Derecho informático* (4.a ed.). UNAM.
- Valenzuela, D. (2020). La protección de datos personales en contextos de pandemia y la constitucionalización del derecho a la autodeterminación informativa. *Revista Chilena de Derecho y Tecnología*, 9(1), 11–41.
<https://doi.org/10.5354/0719-2584.2020.57777>
- Van Weezel, A. (2010). Contra la responsabilidad de las personas jurídicas. *Política Criminal*, 5(9), 114–142.
- Vera, A., Calderón, L., & Vera, M. (2017). Dogmática penal y responsabilidad civil. *Revista Penal México*, (13), 207–219.
- Wachter, S., Mittelstadt, B., & Floridi, L. (2017). Why a right to explanation of automated decision-making does not exist in the General Data Protection Regulation. *International Data Privacy Law*, 7(2), 76–99.
- Wilson, A. (2018). *El ascenso de la automatización*. Babelcube Inc.
- Zaffaroni, E., Alagia, A., & Slokar, A. (2002). *Derecho penal: Parte general*. Ediar.



DERECHO PENAL EN LA ERA DE LA INTELIGENCIA ARTIFICIAL

