

OPUS MAGNA

CONSTITUCIONAL

CORTE DE CONSTITUCIONALIDAD – INSTITUTO DE JUSTICIA CONSTITUCIONAL
REPÚBLICA DE GUATEMALA

TOMO XXII – OCTUBRE, 2025

ISSN: 2707-9857

opusmagna.cc.gob.gt

A vueltas con la IA ¿Un Derecho inteligente o una inteligencia artificial para el Derecho?

Back to AI: Smart law or artificial intelligence for law?

DOI: <https://doi.org/10.37346/opusmagna.v22i1.162>



Santos Romeo Barrientos Aldana*

Universidad de San Carlos de Guatemala, Guatemala

<https://orcid.org/0000-0002-7213-1304>

santosbarrientos3@gmail.com

Recibido: 15/07/2025

Aceptado: 07/10/2025

Publicado: 15/10/2025

Resumen: Este ensayo examina los desafíos jurídicos que plantea la incorporación de la inteligencia artificial (IA) en el ámbito jurídico guatemalteco, con especial énfasis en la administración de justicia. Se parte de la hipótesis de que la adopción de IA solo será constitucionalmente legítima si se implementa dentro de un marco garantista, adaptado a la realidad institucional del país. La investigación emplea un enfoque cualitativo jurídico-analítico y comparado, que incluye el estudio de marcos normativos internacionales —como el Reglamento Europeo de inteligencia artificial (Reglamento UE 2024/1689) y el análisis de jurisprudencia relevante, como la Sentencia T-323/2024 de la Corte Constitucional de Colombia (uso de ChatGPT en decisiones judiciales), el fallo Denegri c. Google de la Corte Suprema Argentina (derecho al olvido digital), el Recurso 27/2021 de la Suprema Corte mexicana (caso Pegasus) y el expediente 3552-2014 de la Corte de Constitucionalidad de Guatemala, que reconoce incipientemente la autodeterminación informativa. Los resultados identifican cuatro brechas regulatorias principales:

* Licenciado en Ciencias Jurídicas y Sociales, Abogado y Notario y magister en Derecho Constitucional por la Universidad de San Carlos de Guatemala. Doctorando en derecho por la Universidad Rafael Landívar y la Universidad del País Vasco. Coordinador de Vocalía V de la Corte Suprema de Justicia y docente de postgrado en la Universidad de San Carlos de Guatemala.

rezago en la protección de datos personales, ausencia de políticas públicas que introduzcan marcos éticos sobre IA, debilidad institucional en ciberseguridad y un marco insuficiente para la ciberdelincuencia. Se propone la creación de una Ley de Inteligencia Artificial y Protección de Derechos, basada en principios de transparencia, explicabilidad y rendición de cuentas, junto con una Estrategia Nacional de IA para la Justicia que incluya capacitación especializada, proyectos piloto controlados y mecanismos de control democrático. Se concluye que modernizar la justicia guatemalteca requiere un enfoque que equilibre innovación tecnológica y protección efectiva de los derechos fundamentales.

Palabras clave: Inteligencia artificial, protección de datos personales, administración de justicia, derechos fundamentales, regulación algorítmica.

Abstract: *This essay examines the legal challenges posed by the incorporation of artificial intelligence (AI) in the Guatemalan legal sphere, with particular emphasis on the administration of justice. It is based on the hypothesis that the adoption of AI will only be constitutionally legitimate if implemented within a rights-based framework adapted to the country's institutional reality. The research employs a qualitative, legal-analytical, and comparative approach, which includes the study of international regulatory frameworks—such as the European Union Artificial Intelligence Regulation (Regulation EU 2024/1689)—and the analysis of relevant case law, such as Judgment T-323/2024 of the Colombian Constitutional Court (use of ChatGPT in judicial decisions), the Denegri v. Google ruling of the Argentine Supreme Court (right to digital oblivion), Appeal 27/2021 of the Mexican Supreme Court (Pegasus case), and Case File 3552-2014 of the Guatemalan Constitutional Court, which incipiently recognizes informational self-determination. The findings identify four main regulatory gaps: delay in personal data protection, absence of public policies introducing ethical frameworks on AI, institutional weakness in cybersecurity, and an insufficient framework for addressing cybercrime. It proposes the creation of an Artificial Intelligence and Rights Protection Act, grounded in principles of transparency, explainability, and accountability, together with a National AI Strategy for Justice that includes specialized training, controlled pilot projects, and mechanisms for democratic oversight. The conclusion is that modernizing Guatemalan justice requires an approach that balances technological innovation with the effective protection of fundamental rights.*

Keywords: *Artificial intelligence, personal data protection, administration of justice, fundamental rights, algorithmic regulation.*

Sumario:

Introducción: el reto de la inteligencia artificial en el derecho guatemalteco – La inteligencia artificial en el contexto global: implicaciones jurídicas – El marco normativo en Guatemala: brechas y desafío legales con relación a la integración de la IA en decisiones judiciales – Marco jurídico de la digitalización de la justicia en Guatemala – Análisis de la legislación guatemalteca obre derechos fundamentales, privacidad y protección de datos – Propuesta normativa y de

política pública para la regulación de la inteligencia artificial en el ámbito jurídico guatemalteco
– A manera de conclusión - Referencias

Introducción

A vueltas con la IA. ¿Un derecho inteligente o una inteligencia artificial para el derecho? Esta pregunta sintetiza el dilema central de la investigación, ya que se buscó determinar si el derecho debe adaptarse a las lógicas tecnológicas para volverse “inteligente” o si, por el contrario, la inteligencia artificial debe subordinarse a los principios garantistas y constitucionales que históricamente han regulado el ejercicio del poder. La creciente incorporación de herramientas algorítmicas en la administración pública y, en particular, en el ámbito judicial, plantea desafíos inéditos para los derechos fundamentales, especialmente en materia de privacidad, autodeterminación informativa, debido proceso e igualdad ante la ley.

La irrupción de la inteligencia artificial -IA- en el ámbito jurídico representa una de las transformaciones más disruptivas de los últimos tiempos. Su capacidad para procesar grandes volúmenes de información, generar predicciones y asistir en la toma de decisiones plantea oportunidades inéditas para mejorar la eficiencia de la administración de justicia, pero también riesgos significativos para los derechos fundamentales, en particular para la privacidad, la autodeterminación informativa, el debido proceso y la igualdad ante la ley. En este escenario, la cuestión central no es únicamente tecnológica, sino profundamente jurídica y constitucional. Por ello, conviene preguntarse, ¿cómo integrar la IA al sistema de justicia garantizando la supremacía de los derechos humanos y el control democrático de la tecnología?

En el contexto guatemalteco, este debate adquiere especial relevancia debido a un doble fenómeno. Por un lado, existe un rezago normativo estructural, pues el país carece de una legislación sólida y específica sobre protección de datos personales en materia de tecnología, no dispone de un marco integral sobre ciberdelincuencia y no ha desarrollado políticas públicas que orienten la digitalización judicial con criterios éticos y constitucionales. Por otro lado, el Poder Judicial aún funciona bajo esquemas predominantemente manuales y burocráticos, con decisiones “cajoneras” que podrían beneficiarse de sistemas inteligentes de asistencia, pero cuya adopción desregulada podría amplificar sesgos, opacidad y violaciones a derechos fundamentales.

La presente investigación parte de la hipótesis de que la incorporación de IA en el ámbito jurídico guatemalteco solo será legítima y constitucionalmente sostenible si se construye un marco regulatorio garantista, adaptado a la realidad institucional del país y fundamentado en principios de transparencia, rendición de cuentas y respeto a la dignidad humana. Para desarrollar esta investigación se recurrió a una metodología cualitativa jurídico-analítica y comparada, que incluyó el análisis de instrumentos internacionales como el Reglamento Europeo de inteligencia artificial (Reglamento UE 2024/1689); el estudio de jurisprudencia comparada, destacando la Sentencia T-323/2024 de la Corte Constitucional de Colombia sobre el uso de ChatGPT en decisiones judiciales, el fallo “Denegri, Natalia Ruth c/ Google Inc. s/ derechos personalísimos” de la Corte Suprema de

Justicia de la Nación de Argentina relativo al derecho al olvido digital y el Recurso 27/2021 de la Suprema Corte de Justicia de México en el caso Pegasus; así como la revisión crítica del *corpus iuris* guatemalteco, incluyendo la Constitución Política de la República, el Decreto 57-2008, Ley de Acceso a la Información Pública, y el expediente 3552-2014 de la Corte de Constitucionalidad de Guatemala, que reconoce de forma incipiente la autodeterminación informativa como parte del derecho a la intimidad.

Este estudio se estructura en tres grandes ejes. En primer lugar, se presenta un marco conceptual sobre la relación entre IA y derecho, diferenciando sus principales modelos de interacción. Posteriormente, se realiza un análisis crítico de la legislación guatemalteca en materia de privacidad y protección de datos, complementado con un estudio de las brechas regulatorias que dificultan la implementación legítima de IA en el ámbito jurídico. Finalmente, se formula una propuesta normativa y de política pública orientada a garantizar un uso ético y controlado de la IA en la administración de justicia guatemalteca. En un mundo donde la tecnología avanza a un ritmo mucho más rápido que el derecho, Guatemala se enfrenta al reto de evitar que la IA reproduzca o amplifique desigualdades estructurales y de asegurar que la modernización judicial no erosione garantías constitucionales. De ahí que se busca aportar, desde una perspectiva crítica y garantista, a la construcción de un modelo regulatorio que equilibre innovación y protección de los derechos fundamentales.

La inteligencia artificial en el contexto global: implicaciones jurídicas

La inteligencia artificial se ha vuelto un tema de moda que sigue desarrollándose a pasos agigantados. Sus desarrollos y desafíos comprenden, además, el fortalecimiento de los marcos normativos. No obstante, resulta importante señalar que los predicamentos de esta construcción automatizada provienen desde concepciones de la matemática para dar lugar a los algoritmos y su formulación en el ciberespacio.

De esta cuenta, desde que Aristóteles imaginó los silogismos, como una forma de comprensión humana, para dar lugar a premisas y conclusiones válidas, se han desarrollado estas comprensiones que siguen la lógica de combinaciones numéricas. Así también, se comenzó hablando que el razonamiento se produce de construcciones artificiales. Es decir, la lógica y la matemática han sido los principales motores que dieron origen al razonamiento artificial, para dar lugar al mundo del ciberespacio y formas automatizadas de dirigir el pensamiento algorítmico. Por ello, fue con Alan Turing con que se inicia a hablar de manera oficial de la informática teórica, generando el pensamiento algorítmico y matemático para dar paso al conocimiento digital, para ejecutar tareas mediante un ordenador o computador.

En contraste con Rebollo Delgado (2023):

En 1943 Warren McCulloch y Walter Pitts presentaron su modelo de neuronas artificiales, el cual se considera el primer trabajo en el campo de la Inteligencia artificial, y ya en 1950 Turing lo consolidó con su artículo *Computing Machinery and Intelligence*, en el que propuso una prueba

concreta para determinar si una máquina era inteligente o no, su famosa Prueba o test de Turing, por lo que se le considera el padre de la Inteligencia artificial. Años después Turing se convirtió en el adalid de quienes defendían la posibilidad de emular el pensamiento humano a través de la computación y fue coautor del primer programa para jugar al ajedrez. (p. 20)

Como se observa Turing representó el pensador fundamental de la IA en entornos digitales; es decir, de comprender las formas algorítmicas y transformar los computadores en piezas claves que emulan el pensamiento humano. Sin embargo, es con John McCarthy con quien se acuña de manera formal el término inteligencia artificial para expresar máquinas inteligentes capaces de resolver enigmas humanos. Bajo estos parámetros: “Los trabajos de George Boole y Alan Turing ... constituyen las primeras contribuciones teóricas en IA” (Kong, 1993, p. 18). Más adelante, Kong (1993), señaló que:

Oficialmente se reconoce que la IA se originó en la conferencia organizada por John McCarthy y Marvin Minsky en el Dartmouth College ... durante el verano de 1956, en la cual se aceptó como una conjetura básica la posibilidad de describir en forma precisa las distintas características y aspecto de la inteligencia de manera que una máquina pueda simularlos. (p. 18)

De esta cuenta, si bien es con Turing con quien inicia a desarrollarse el concepto de inteligencia artificial, sus desarrollos y postulados se intensifican con McCarthy y Minsky, quienes comenzaron haciéndolo con programas sobre juegos de razonamiento. Como puede advertirse los antecedentes se remontan a mediados del siglo XX, pero es en la segunda mitad del siglo XX en que comienza a hablarse con mayor detenimiento de IA y derecho.

Los estudios contemporáneos sobre la relación entre IA y derecho se han diversificado, abordando desde enfoques centrados en la protección de datos personales hasta la exploración de la IA como herramienta para la toma de decisiones judiciales. Este abanico de perspectivas ha dado lugar a distintas formas de conceptualizar la interacción entre ambas disciplinas, que pueden sintetizarse en cuatro grandes modelos: IA y Derecho, IA *para el* Derecho, IA *con* Derecho y Derecho *con* IA.

El primer modelo, IA y Derecho, asume un rol protagónico de ambas dimensiones, concebidas como sistemas complementarios que interactúan para la protección y generación de información automatizada. Se trata de un enfoque amplio que no se limita a funciones estrictamente judiciales, sino que comprende la IA como parte de un ecosistema de gobernanza de datos donde el derecho actúa tanto como garante de derechos fundamentales como usuario de la tecnología.

El segundo modelo, IA *para el* Derecho, se centra en la utilización de la IA como herramienta para generar conocimientos jurídicos. Aquí, la IA se pone al servicio de la función judicial o normativa, asistiendo en la elaboración de decisiones, la interpretación de normas o la producción de jurisprudencia. Ejemplos de este enfoque son los sistemas de búsqueda predictiva de jurisprudencia, los algoritmos de análisis o los sistemas de apoyo a la redacción de resoluciones.

El tercer modelo, IA *con* Derecho, desplaza el foco hacia la regulación jurídica de la IA y su uso ético. Este enfoque se preocupa por establecer marcos normativos, principios y estándares que limiten los riesgos de sesgos, opacidad o afectación de derechos fundamentales. Es el modelo

actualmente predominante en la doctrina internacional, ejemplificado en instrumentos como el Reglamento Europeo de Inteligencia Artificial (Reglamento UE 2024/1689).

Finalmente, el cuarto modelo, Derecho *con* IA, amplía la concepción de la IA *para el* Derecho, proponiendo la transformación del propio derecho en un sistema dotado de inteligencia automatizada. Aquí, la IA no se limita a asistir a jueces o legisladores, sino que asume un rol protagónico en la toma de decisiones. Se trata de una evolución hacia el uso de IA generativa en modelos de lenguaje jurídico, capaces no solo de producir decisiones o normas, sino de convertirse en actores decisorios autónomos: jueces robot, algoritmos que deciden, sistemas robóticos con capacidad deliberativa programada. Bajo esta concepción, el derecho podría dotarse de una “inteligencia automatizada”, capaz de operar con relativa independencia humana.

Si bien los tres primeros modelos responden a lógicas de complementariedad y control, el cuarto modelo plantea desafíos éticos y constitucionales profundos, pues supone delegar funciones tradicionalmente humanas a sistemas algorítmicos cuya legitimidad y rendición de cuentas resultan, al menos por ahora, insuficientemente garantizadas. Por ello, este estudio, inscrito en la pregunta central ¿un derecho inteligente o una inteligencia artificial para el derecho?, parte precisamente de esta tensión: ¿debe el derecho aspirar a convertirse en un sistema “inteligente” mediante algoritmos autónomos, o debe la IA permanecer subordinada a los principios del Estado constitucional de Derecho?

Breve panorama de la regulación global de la IA en el derecho. En una perspectiva global, comúnmente se ha utilizado la IA para la creación de modelos computacionales de razonamiento jurídico (lo que hemos denominado como IA *para el* Derecho). Estos modelos constituyen:

un programa informático que implementa un proceso destinado a evidenciar las propiedades del razonamiento jurídico practicado por los seres humanos. El proceso puede implicar el análisis de una situación y la respuesta a una pregunta jurídica, la predicción de un resultado o incluso la formulación de un argumento jurídico. (Ashley, 2023, p. 19)

De esta cuenta, se observa que los usos de la IA contribuyen al fortalecimiento de los marcos normativos. Sin embargo, su utilización requiere, además, una aplicación ética y moderada, con el objeto de evitar que sus usos trasciendan las posibilidades prácticas, que solo los seres humanos pueden manejar.

Existen países como Colombia que han tenido un desarrollo considerable en el uso de las tecnologías de la información, aunque dicho avance se ha enfocado principalmente en la digitalización de las decisiones judiciales y, en menor medida, en el desarrollo de herramientas orientadas al manejo de la inteligencia artificial. En igual sentido, Quintero Londoño (2025), ha señalado que:

Colombia ha tenido un desarrollo considerable respecto de las tecnologías de la información y sus aplicaciones, pero también incierto a la hora de regular la inteligencia artificial en torno a un modelo ético-moral que al mismo tiempo privilegie el uso responsable de la información y los datos de los administrados desde una visión constitucional. (p. 90)

Bajo esta perspectiva, la regulación jurídica de la IA ha encontrado poco desarrollo en algunos países, tal es el caso de los países centroamericanos, en especial el caso de Guatemala que no cuenta con una Ley que, además de proteger datos personales, tenga un enfoque basado en el uso de la IA de manera ética y respetuosa de los derechos humanos. Más aún no existe una regulación en torno a los ciberdelitos y la ciberseguridad en el país.

Por su parte, es importante mencionar que, además de la necesidad de una regulación que logre un adecuado equilibrio entre la protección de datos personales (*habeas data*) y el derecho de acceso a la información pública, se plantea también el dilema relativo al uso responsable de la inteligencia artificial. Ello obedece a que esta tecnología, en su vertiente más avanzada, permite desarrollos generativos de alto alcance que, si bien ofrecen oportunidades para optimizar procesos y ampliar capacidades en el ámbito judicial, al mismo tiempo pueden propiciar nuevos modos de actuación para la delincuencia organizada, incrementando los riesgos en materia de seguridad jurídica y ciudadana.

Comparación de experiencias internacionales con el sistema jurídico guatemalteco. La experiencia internacional, producto de la globalización, revela importantes avances tecnológicos. Sin embargo, a la par de estos avances la regulación jurídica ha mostrado pocos desarrollos. Para efectos de la presente investigación, tomaremos únicamente la comparación de países como España, Colombia, Argentina y México.

España. En España, la regulación jurídica de la IA comenzó a regirse por el Reglamento de Inteligencia Artificial para Europa. El Reglamento (UE) 2024/1689 (2024), conocido como el Reglamento de Inteligencia Artificial, es un marco normativo pionero adoptado por la Unión Europea para regular el uso de sistemas de IA. Este reglamento tiene como objetivo garantizar que la IA se desarrolle y utilice de manera segura, ética y respetuosa con los derechos fundamentales, al tiempo que promueve la innovación y la competitividad en el mercado único europeo. Dada la creciente influencia de la IA en diferentes sectores, incluido el ámbito jurídico, este reglamento es un paso significativo hacia la creación de un entorno regulador más coherente y responsable para los sistemas automatizados en Europa.

Una de las características fundamentales del Reglamento es la clasificación de los sistemas de IA según su nivel de riesgo. Esta clasificación permite una regulación proporcional, adaptada a las implicaciones que cada tipo de IA puede tener sobre la sociedad y los derechos humanos. En primer lugar, los sistemas de IA que representan un riesgo inaceptable son completamente prohibidos. Esto incluye sistemas que podrían manipular el comportamiento humano, como los utilizados para realizar vigilancia masiva sin control o autorización. En segundo lugar, se identifican los sistemas de alto riesgo, que son aquellos utilizados en sectores clave como la justicia, la salud o la educación. Estos sistemas están sujetos a estrictos requisitos regulatorios, que incluyen evaluaciones de conformidad, medidas para mitigar los riesgos y la obligación de garantizar una supervisión humana de las decisiones automatizadas. Para los sistemas de riesgo limitado, se exige transparencia, ya que los usuarios deben ser informados de que están interactuando con una IA, pero no se imponen obligaciones regulatorias tan estrictas. Finalmente,

los sistemas de riesgo mínimo, como los filtros de *spam* o los videojuegos, no están sujetos a las regulaciones del Reglamento, debido a su bajo impacto en los derechos fundamentales.

Sin embargo, es importante apuntar que si bien se considera el *spam* o los videojuegos de bajo riesgo, con la evolución de la sociedad de riesgos, la imperativa navegación entre riesgos permitidos proveniente del sistema funcionalista del derecho penal y los crecientes desarrollos de la IA generativa, abona a que se establezcan estándares mínimos a efecto de evitar los abusos en el ciberespacio y respetar los derechos fundamentales.

El Reglamento también establece obligaciones claras para los proveedores y usuarios de IA. Los proveedores deben realizar evaluaciones de conformidad para garantizar que sus sistemas cumplan con los requisitos de seguridad, transparencia y gestión de riesgos. Asimismo, deben mantener registros detallados de las actividades realizadas por los sistemas de IA para facilitar la supervisión. Por su parte, los usuarios de IA tienen la responsabilidad de asegurar que las decisiones automatizadas sean supervisadas por seres humanos, evitando así que los sistemas operen de manera autónoma y sin intervención.

Una característica notable del Reglamento es su alcance extraterritorial. Es decir, se aplica no solo a los proveedores de IA establecidos dentro de la UE, sino también a aquellos proveedores que, aunque ubicados fuera de la Unión Europea, ofrezcan productos o servicios que utilicen IA y afecten a los usuarios dentro del territorio europeo.

Colombia. Colombia, se puede considerar pionera en la aplicación de la IA en decisiones judiciales de Tribunales Constitucionales de Latinoamérica. Ya que es la sentencia T 323/2024 (*Sentencia sobre el uso de herramientas de inteligencia artificial generativas en procesos judiciales de tutela*, 2024) la que estructura y desarrolla lo concerniente a la aplicación de la IA en decisiones judiciales, particularmente en el uso de ChatGPT para la aplicación y fundamentación de sus decisiones. Sin embargo, también es importante resaltar que, además de ser referente, constituye un avance en el derecho de manera pretoriana, ya que no existe normativa que regule, al momento, temas referentes a la IA en el Estado de Colombia.

En la sentencia T 323/2024 (2024), el Tribunal Constitucional, entre otras consideraciones, manifestó:

los avances tecnológicos en materia de IA han tenido un impacto global complejo que ha irradiado cada ámbito de la vida humana, sin que la práctica jurídica sea una excepción y, dentro de ella, el sistema judicial. En efecto, la proliferación de sistemas de IA y su aplicación en escenarios judiciales, tanto en el trámite como en lo sustancial, dan paso progresivo a un nuevo paradigma en el servicio público de administración de justicia. De allí la necesidad de evaluar las condiciones para que la implementación de estas nuevas tecnologías en la Rama Judicial pueda llevarse a cabo con respeto de los derechos fundamentales, entre ellos el debido proceso. (párr. 79)

De lo establecido en dicha decisión dentro de la justicia constitucional colombiana, se desprenden tres aspectos que engloban el uso de la IA generativa: i) las decisiones judiciales deben resguardar siempre el debido proceso, ii) la IA generativa constituye un avance, pero es necesario

su estricta regulación y iii) la rama judicial puede valerse del uso de IA generativa responsable y respetuosa de derechos fundamentales.

Estas consideraciones nutren la perspectiva global sobre el uso de la IA, ya que ahora se habla de un uso indiscriminado de la tecnología, a tal punto que se hace tan urgente como necesario una regulación sobre las responsabilidades que puedan derivarse del mal manejo. Como en todo, los avances traen aparejadas consecuencias que colisionan con derechos fundamentales. Es decir, pasamos de un paradigma garantista constitucional a un paradigma de riesgos y desafíos por el uso de la IA generativa. La gobernanza de la IA contribuye a generar un sistema de protección de datos y de datos abiertos. Por ello, Quintero Londoño (2025), considera que

todas las formas de violación de garantías a la información son actuaciones ilegítimas, requisito además inicial de la falla del servicio, no obstante, también hay que atender a que hay condiciones propias de cada caso que hacen que sea más fácil intentar la reparación directa. (p. 146)

Ahora bien, continuando con la resolución T 323/2024, se debe destacar que esta no solo se limita a resolver un caso concreto relacionado con la salud de un menor diagnosticado con TEA, sino que introduce criterios orientadores que podrían considerarse paradigmáticos para otros sistemas jurídicos latinoamericanos, entre ellos el guatemalteco, donde aún no existe una regulación específica en esta materia.

En dicha sentencia, la Corte analizó si el uso de ChatGPT 3.5 por parte de un juez vulneraba el derecho al debido proceso, y concluyó que, aunque no hubo una sustitución de la racionalidad humana ni una delegación en la IA de la decisión judicial, sí se identificaron deficiencias en el cumplimiento de los principios de transparencia y responsabilidad. Esta distinción es crucial: el uso de IA como herramienta auxiliar puede ser admisible, siempre que no sustituya la función jurisdiccional esencial, y que su utilización se realice de forma controlada, informada y ética.

La Corte propuso un conjunto de doce principios orientadores para el uso de IA en la administración de justicia: transparencia, responsabilidad, privacidad, no sustitución de la racionalidad humana, seriedad y verificación, prevención de riesgos, igualdad y equidad, control humano, regulación ética, adecuación a buenas prácticas, seguimiento y adaptación, e idoneidad. Estos principios configuran un marco ético-normativo que supera la mera técnica regulatoria, al integrar estándares propios del constitucionalismo contemporáneo, como la protección reforzada de los derechos fundamentales en entornos digitales. Lo que daría paso a un constitucionalismo digital (Sánchez Barrilao, 2022).

Este enfoque es especialmente relevante para Guatemala, donde la adopción de tecnologías en la administración de justicia se encuentra aún en etapas iniciales y carece de una política pública coherente sobre IA. En este contexto, la experiencia colombiana ofrece una referencia útil para avanzar hacia una regulación anticipada, preventiva y garantista. Por ejemplo, la exigencia de motivación racional humana y la prohibición de sustituir el juicio judicial por algoritmos opacos deben ser principios rectores en cualquier intento de implementación tecnológica en tribunales guatemaltecos.

Además, la sentencia destaca la necesidad de emitir guías institucionales por parte del órgano rector de la judicatura (en Colombia, el Consejo Superior de la Judicatura), algo que bien podría inspirar a la Corte Suprema de Justicia de Guatemala a asumir una función proactiva en la definición de estándares éticos y operativos. Esta iniciativa permitiría, entre otras cosas, mitigar los riesgos de sesgos algorítmicos, alucinaciones de lenguaje o afectaciones a derechos fundamentales que podrían derivarse de un uso irreflexivo de tecnologías generativas.

Argentina. En el marco del debate sobre el impacto de la tecnología en los derechos fundamentales, la Corte Suprema de Justicia de la Nación de Argentina resolvió un caso paradigmático en materia de protección de datos personales y derecho al olvido digital, es el expediente “Denegri, Natalia Ruth c/ Google Inc. s/ derechos personalísimos”, sentencia del 28 de junio de 2022. Aunque este fallo no aborda explícitamente el uso de inteligencia artificial, sí ofrece claves importantes sobre el control judicial de las tecnologías algorítmicas, particularmente en lo que se refiere al rol de los motores de búsqueda y su capacidad de perpetuar contenidos lesivos, irrelevantes o descontextualizados a lo largo del tiempo.

Natalia Denegri promovió una acción contra Google Inc. solicitando la eliminación de enlaces a sitios web que mostraban videos y noticias de hace más de veinte años, en los que aparecía involucrada en hechos de alto impacto mediático relacionados con una causa penal. La actora alegó que dicha información, aunque verídica en su momento, había perdido interés público con el paso del tiempo y afectaba gravemente su honor, privacidad, vida familiar y desarrollo profesional. Su pretensión no fue la eliminación del contenido original en los sitios que lo alojaban, sino el bloqueo del acceso desde el buscador mediante su nombre.

Este conflicto obligó al tribunal a ponderar entre el derecho a la información y los derechos personalísimos, en particular el derecho a la intimidad y la reputación. La Corte Suprema resolvió en favor del interés público, revocando las decisiones de instancias inferiores que habían ordenado el bloqueo de resultados. Consideró que la difusión de los contenidos, por tratarse de hechos verídicos vinculados a causas judiciales y de gran impacto social, seguía teniendo relevancia histórica, incluso si resultaban dolorosos para la actora. Además, enfatizó que el derecho al olvido no podía utilizarse como instrumento para reescribir la historia o eliminar del debate público cuestiones que alguna vez fueron objeto de atención general.

Este fallo es relevante para el derecho porque pone en evidencia el problema de la persistencia digital de los algoritmos, especialmente los de los motores de búsqueda, y la dificultad de controlar su impacto en la vida de las personas. En este sentido, el fallo plantea interrogantes sobre hasta qué punto las decisiones tomadas por sistemas automatizados (como los algoritmos de búsqueda) deben someterse a revisión desde la perspectiva de los derechos fundamentales.

Desde la óptica del constitucionalismo latinoamericano, esta decisión argentina contrasta con la doctrina europea del Tribunal de Justicia de la Unión Europea (caso *Google Spain*), que ha admitido el derecho al olvido frente a resultados de búsqueda que afectan la dignidad de la persona cuando la información ha perdido relevancia pública (*Google v. España*, 2014). Para el contexto guatemalteco, donde aún no existe una legislación robusta sobre protección de datos personales ni

una jurisprudencia consolidada sobre el derecho al olvido, este tipo de fallos regionales ofrece insumos fundamentales para reflexionar sobre la necesidad de regular no solo la inteligencia artificial, sino también los efectos de los algoritmos en el espacio digital.

El caso Denegri, en suma, no discute la IA de manera explícita, pero subraya la importancia de que el derecho desarrolle herramientas críticas frente a las tecnologías de automatización de la información. La justicia no puede ser indiferente a los efectos prolongados, muchas veces invisibles, que los sistemas digitales generan sobre los derechos humanos. En este sentido, toda arquitectura regulatoria sobre inteligencia artificial en el ámbito jurídico guatemalteco debe incluir —como parte de su horizonte ético— el examen de las tecnologías de búsqueda, indexación, perfilamiento y almacenamiento digital.

México. En México ha suscitado controversia el uso de software espía para controlar la información de políticos y servir como un medio de ataque (Comisión Interamericana de Derechos Humanos (CIDH), 2023). La sentencia del Recurso de Revisión 27/2021 resuelta por la Suprema Corte de Justicia de la Nación (SCJN) de México constituye un hito en la relación entre tecnología, seguridad nacional y acceso a la información pública, especialmente en el contexto del escándalo internacional vinculado al software espía Pegasus (*Recurso de revisión en materia de seguridad nacional previsto en la Ley General de Transparencia y Acceso a la Información Pública*, 2024). Aunque la Corte no se refiere explícitamente a la inteligencia artificial (IA), el análisis del caso aporta elementos fundamentales para abordar la gobernanza constitucional de tecnologías de vigilancia automatizada y su compatibilidad con el derecho a la información y la protección de datos personales.

El origen del litigio está en la solicitud ciudadana de información relacionada con las contrataciones gubernamentales del software Pegasus, mencionadas públicamente por el titular de la Unidad de Inteligencia Financiera (UIF). La información fue clasificada como reservada por motivos de seguridad nacional. Sin embargo, el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) ordenó su entrega en versión pública, considerando que existía un interés público prevalente, en tanto el propio Ejecutivo había divulgado su existencia.

La Consejería Jurídica del Ejecutivo Federal interpuso el recurso de revisión ante la SCJN, invocando como base la reserva automática de toda información generada por instituciones vinculadas con la seguridad nacional. No obstante, la Corte desestimó este argumento por considerar que la clasificación no puede derivarse de una mera relación funcional o institucional, sino que debe probarse que la divulgación de la información ocasionaría un daño presente, probable y específico a la seguridad nacional (SCJN, 2024).

Desde la perspectiva del derecho y la inteligencia artificial, este caso pone de relieve una dimensión crítica que supone la opacidad algorítmica del Estado en contextos de vigilancia masiva. Pegasus no es una herramienta de IA general, pero sí opera con algoritmos de recolección y procesamiento automatizado de datos, facilitando el monitoreo integral de dispositivos móviles sin conocimiento del usuario. Su despliegue, oculto bajo el velo de la “seguridad nacional”, representa

un riesgo estructural para los derechos fundamentales, incluyendo el derecho a la intimidad, la privacidad informática y el acceso a la información pública.

El fallo mexicano es relevante para Guatemala en tanto revela la necesidad de establecer límites constitucionales y democráticos al uso de tecnologías de vigilancia, especialmente cuando estas operan con alto grado de automatización y sin control judicial previo. El razonamiento de la SCJN puede extrapolarse a herramientas más complejas de IA, como sistemas de reconocimiento facial, análisis predictivo o rastreo digital, cuyo uso está en expansión en América Latina.

Asimismo, el fallo subraya el principio fundamental de que no toda tecnología utilizada en nombre de la seguridad nacional puede estar exenta de control ciudadano. La Corte exige que las autoridades demuestren con evidencia concreta y proporcional por qué la divulgación afectaría intereses esenciales, desarmando así la presunción de reserva automática. En otras palabras, se impone una lógica de rendición de cuentas incluso sobre tecnologías sofisticadas y sensibles.

Para el caso guatemalteco, el precedente mexicano destaca la urgencia de regular el uso de sistemas automatizados de vigilancia (basados o no en IA), incluyendo la exigencia de marcos legales claros, evaluaciones de impacto en derechos humanos y garantías de transparencia pública. La importación acrítica de tecnologías de ciberinteligencia sin mecanismos de control judicial o social podría derivar en una erosión sistemática de las libertades fundamentales.

El caso Pegasus en México obliga a repensar la relación entre secrecía algorítmica, razón de Estado y control constitucional, lo cual es indispensable para la construcción de una política de IA centrada en los derechos en países como Guatemala, ya que actualmente en el país no existe un sistema jurídico robusto en cuanto a la protección de datos, principalmente aquellos que se derivan del uso de IA.

De ahí que sea preciso establecer parámetros equilibrados que busquen priorizar los principios fundamentales y defensa e intereses de los particulares con un enfoque estructurado en la protección de derechos humanos. El caso de vigilancia a través de un software espía requiere de un estricto cumplimiento ético por parte del Estado, ya que a la par de que es el mismo Estado quien adquiere estos servicios de ciberinteligencia bajo la bandera de mantener la seguridad, es también el mismo Estado quien avanza en desarrollos garantistas del derecho. Por ello, en palabras de Quintero Londoño (2025):

en el ... espionaje estatal ... para la desaparición o manipulación fraudulenta de la información, donde valga la redundancia, es el Estado mismo quien vulnera el principio de confianza y garante, y además lo hace de forma maliciosa, salta a la vista que además de ser un evento incluso político-penal, atenta contra toda el alma de la constitución, el fundamento directo es la falla del servicio sujeto a las condiciones de tipo de información y forma de extracción y constituye un ataque sistematizado por parte del Estado a sus administrados. (pp. 150-151)

De esta cuenta, es importante establecer que existen riesgos versus amenazas. Pero esto no es nada novedoso, en la multicitada novela distópica de George Orwell, *1984*, se preveía un mundo destinado a la vigilancia constante por parte del gobierno, el llamado *big brother* -el hermano

mayor-, quien, a través de los ojos constantes y dominio de intimidades logra controlar sin parpadear o dejar un velo delgado de sombras que no puedan ser descubiertas, porque este, el hermano mayor, vigila sin un minúsculo tiempo de descanso. Si bien, esta advertencia de un narrador futurista advertía los grandes problemas que ahora nos enfrentamos, corresponde en esta era de las garantías y de la constitucionalización de derechos prever los abusos y usos de la IA en constante evolución.

Sin embargo, desde el punto de vista de Queralt (2024):

los derechos fundamentales no son ilimitados y, en determinados supuestos y bajo determinadas condiciones, pueden ser objeto de afectación, siempre respetando su contenido esencial. Estas restricciones y los procedimientos para llevarlas a cabo deben venir, tal como establece la Constitución, de la mano de normativa específica con el formato de ley orgánica. (p. 1358)

Bajo estos paisaje que se dibuja, se tiene que, si bien el Estado tiene cierta injerencia en la información de las personas, también es cierto que debe existir un tipo de control gubernamental a efecto de evitar vulneraciones sistemáticas a la seguridad del Estado. En consecuencia, existen amenazas y riesgos versus garantías constitucionales que deben respetarse. Por lo que se debe crear una construcción de sistemas de vigilancia basados en el respeto a la dignidad humana.

El marco normativo en Guatemala: brechas y desafíos legales con relación a la integración de la IA en decisiones judiciales

En Guatemala a la fecha del presente artículo no existe una política pública del manejo de la IA de manera ética, como si la hay en Europa. Tampoco existe dentro del Organismo Judicial una política de uso de la IA en resoluciones judiciales, pese a que, sin duda, muchos operadores jurídicos, con cierta cautela, han implementado el uso de, por ejemplo, ChatGPT. Asimismo, se han brindado algunas capacitaciones aisladas en esta materia, pero no se ha concretado un uso de la IA de manera ética y respaldada de la ciberseguridad.

No obstante, se ha tratado de avanzar dentro del Poder Judicial guatemalteco en torno a la regulación de medios electrónicos para facilitar el acceso a la justicia. Pero ello no significa que constituya un avance en la incorporación de la IA al ámbito judicial, sino más bien constituye la incorporación de medios electrónicos para facilitar el acceso a la justicia. Ejemplo de normativa sobre este propósito tenemos:

Marco jurídico de la digitalización de la justicia en Guatemala

Relacionadas con el comercio y la firma electrónica, están:

- i) Ley para el Reconocimiento de las Comunicaciones y Firmas Electrónicas, Decreto Número 47-2008 del Congreso de la República de Guatemala (2008).

- ii) Reglamento de la Ley para el Reconocimiento de las Comunicaciones y Firmas Electrónicas, Acuerdo Gubernativo Número 135-2009 del Presidente de la República de Guatemala (2009).

Relacionadas con el expediente judicial electrónico, comunicaciones y notificaciones electrónicas, están:

- i) Ley Reguladora de las Notificaciones por Medios Electrónicos en el Organismo Judicial, Decreto Número 15-2011 del Congreso de la República de Guatemala (2011).
- ii) Reglamento del Sistema de Gestión de Tribunales, Acuerdo Número 20-2011 de la Corte Suprema de Justicia de Guatemala (2011).
- iii) Reglamento de la Ley Reguladora de las Notificaciones por Medios Electrónicos en el Organismo Judicial, Acuerdo Número 11-2012 de la Corte Suprema de Justicia de Guatemala (2012).
- iv) Los Juzgados de lo Económico Coactivo, podrán remitir vía correo electrónico las órdenes de embargo de las cuentas de depósitos bancarios, que deben proporcionar las instituciones bancarias del país, Acuerdo Número 2-2012 de la Corte Suprema de Justicia de Guatemala (2012).
- v) Los Jueces podrán tener comunicaciones vía electrónica a la entidad que corresponda al Registro General de la Propiedad, a los bancos del sistema, Dirección General de Migración, a la Policía Nacional Civil y al Registro Fiscal de Vehículo, Acuerdo Número 55-2012 de la Corte Suprema de Justicia de Guatemala (2012).
- vi) Implementación de la “Carpeta Judicial Electrónica” como parte integral de la Política Cero Papel del Organismo Judicial, Acuerdo Número 53-2012 de la Corte Suprema de Justicia de Guatemala (2012).
- vii) Instructivo para realizar notificaciones electrónicas en el área administrativa del Organismo Judicial, Acuerdo Número 1/2013 de la Presidencia del Organismo Judicial y Corte Suprema de Justicia de Guatemala (2013).
- viii) Utilización del sistema de diligencias judiciales electrónicas para la optimización de oficios, Acuerdo Número 16-2015 de la Corte Suprema de Justicia de Guatemala (2015).
- ix) Acuerdo de Cooperación entre el Organismo Judicial y la Superintendencia de Administración Tributaria, el cual implementa la figura del Embargo Electrónico en los Tribunales Económico Coactivo, Acuerdo Número 2-2016 de la Corte Suprema de Justicia de Guatemala (2016).
- x) Acuerdo Número 8-2017 de la Corte Suprema de Justicia de Guatemala (Se autoriza a todos los órganos jurisdiccionales del ramo penal, notificar de forma electrónica, las resoluciones emitidas dentro de los expedientes en los cuales las partes y demás sujetos procesales, se adhieran al sistema de notificación, 2017).

- xi) Implementación de la Firma Electrónica Interna Jurisdiccional del Organismo Judicial y Firma Electrónica Avanzada Institucional en las Actuaciones Judiciales de los Órganos Jurisdiccionales y las Unidades Administrativas, Acuerdo Número 75-2017 de la Corte Suprema de Justicia de Guatemala (2017).
- xii) Se autoriza a los órganos jurisdiccionales que conocen en materia de Trabajo y Previsión Social y a los órganos jurisdiccionales que tramiten procesos en materia constitucional, de todo el territorio notificar en forma electrónica las resoluciones, Acuerdo Número 46-2017 de la Corte Suprema de Justicia de Guatemala (2017).
- xiii) Ley de Avisos Electrónicos, Decreto Número 24-2018 del Congreso de la República de Guatemala (2018).
- xiv) Implementación de la Firma Electrónica Interna De La Unidad De Antecedentes Penales Del Organismo Judicial y Firma Electrónica Avanzada Institucional, Acuerdo Número 27-2018 de la Corte Suprema de Justicia de Guatemala (2018).
- xv) Reglamento De Servicios Electrónicos Prestados Por La Cámara De Amparo Y Antejuicio De La Corte Suprema De Justicia, Acuerdo Número 49-2019 de la Corte Suprema de Justicia de Guatemala (2019).
- xvi) Firma Electrónica Para La Unidad De Información Pública Del Organismo Judicial, Acuerdo Número 038/019 de la Presidencia del Organismo Judicial y Corte Suprema de Justicia de Guatemala (2019).
- xvii) Creación e implementación del Sistema Informático del Archivo General de Tribunales y de la Delegación del Archivo General de Tribunales de Quetzaltenango -SIAT- e implementación de la firma electrónica interna y avanzada institucional, Acuerdo Número 68-2018 de la Corte Suprema de Justicia de Guatemala (2020).
- xviii) Ley de tramitación electrónica de expedientes judiciales, Decreto Número 13-2022 del Congreso de la República de Guatemala (2022).
- xix) Reglamento General de la Ley de Tramitación Electrónica de Expedientes Judiciales, Acuerdo Número 8-2023 de la Corte Suprema de Justicia de Guatemala (2023).
- xx) Reglamento de Notificaciones Electrónicas en los Procedimientos Administrativos Internos del Organismo Judicial, Acuerdo Número 189-2023 de la Presidencia del Organismo Judicial y Corte Suprema de Justicia de Guatemala (2023).

Relacionadas con la celebración de audiencias por medios electrónicos, están:

- i) Reglamento para el desarrollo de las Declaraciones por videoconferencia reguladas en las reformas al Código Procesal Penal, Decreto 51-92, Acuerdo Número 31-2009 de la Corte Suprema de Justicia de Guatemala (2009).

- ii) Adquisición por compra del equipo audiovisual a través de videoconferencia e instalación a fin de resguardar la integridad de los jueces, como de los sujetos procesales, Acuerdo Número 57-2010 de la Corte Suprema de Justicia de Guatemala (2010).
- iii) Reglamento para el uso del Sistema Informático de Expedientes de la Corte de Constitucionalidad (SIECC), Acuerdo Número 03-2016 de la Corte de Constitucionalidad de Guatemala (2016).
- iv) Reglamento para el desarrollo de las declaraciones por videoconferencia en materia disciplinaria dentro del organismo judicial, Acuerdo Número 6-2016 de la Corte Suprema de Justicia de Guatemala (2016).
- v) Reglamento de audiencias por medios electrónicos de comunicación audiovisual en tiempo real, Acuerdo Número 35-2020 de la Corte Suprema de Justicia de Guatemala (2020).
- vi) Creación de los juzgados primero y segundo de paz penal móvil con competencia exclusiva para primeras declaraciones y exhibiciones personales bajo el sistema de audiencias por medios electrónicos, Acuerdo Número 25-2020 de la Corte Suprema de Justicia de Guatemala (2020).
- vii) Disposiciones reglamentarias para la celebración de Vistas Públicas por Videoconferencia, Acuerdo Número 3-2020 de la Corte de Constitucionalidad de Guatemala (2020).

A pesar de este marco jurídico, es importante subrayar que ninguno de estos cuerpos normativos regula el uso de IA en la función jurisdiccional ni establece lineamientos éticos o técnicos para su eventual implementación. Las reformas se han limitado a la digitalización de procesos y comunicaciones, lo que evidencia que Guatemala se encuentra aún en una etapa inicial de modernización tecnológica. La incorporación de IA en el ámbito judicial requiere un marco normativo distinto, centrado no solo en la validez procesal de actos electrónicos, sino en garantías específicas frente a los riesgos de decisiones automatizadas, sesgos algorítmicos y afectación de derechos fundamentales.

Análisis de la legislación guatemalteca sobre derechos fundamentales, privacidad y protección de datos

El desarrollo normativo guatemalteco en materia de privacidad y protección de datos personales presenta avances limitados y dispersos, lo que contrasta notablemente con las tendencias de digitalización y automatización judicial que se observan en países como Argentina, donde ya se exploran usos experimentales de inteligencia artificial generativa -como el caso del programa piloto de IA judicial- o se implementan sistemas como PROMETEA en tareas fiscales (Estevez et al., 2020; Ministerio de Justicia, 2025; Sistema Argentino de Información Jurídica -SAIJ-, 2025). En Guatemala, en cambio, los desafíos para introducir IA en la administración de justicia son múltiples, entre ellos, la débil protección jurídica de los datos personales.

El principal cuerpo normativo en la materia es el Decreto 57-2008, Ley de Acceso a la Información Pública (2008). Esta norma reconoce expresamente el derecho al *hábeas data* como la garantía de toda persona para conocer, corregir o suprimir los datos que de ella consten en archivos públicos (art. 9, numeral 4). Asimismo, define los datos personales como toda información concerniente a personas naturales identificadas o identificables, y distingue los datos sensibles, incluyendo aquellos relativos a la salud, vida sexual, creencias religiosas o ideología política, entre otros aspectos íntimos (art. 9, numerales 1 y 2).

Sin embargo, esta ley no establece una autoridad especializada de control en materia de uso de IA¹, carece de un régimen sancionatorio adecuado y omite fijar obligaciones específicas para los desarrolladores, procesadores o usuarios de tecnologías automatizadas o algorítmicas. Si bien garantiza el principio de máxima publicidad (arts. 3 y 9.8), también prevé excepciones que permiten declarar información como reservada o confidencial, sin delimitar con criterios técnicos suficientes su aplicación frente a tecnologías de vigilancia o de procesamiento masivo de datos.

Del mismo modo, aunque la norma regula el acceso a la información y a los actos de la administración pública, no contempla disposiciones aplicables a los desarrolladores de IA ni a las empresas privadas. Tampoco existe en el ordenamiento jurídico guatemalteco una legislación específica en materia de protección de datos personales que, de manera integral, aborde los desafíos derivados del uso de IA. Asimismo, no se ha creado una autoridad independiente encargada de supervisar el tratamiento y empleo de sistemas algorítmicos tanto en el ámbito público como en el privado.

Este vacío estructural genera importantes riesgos frente a la implementación de la IA en el ámbito judicial, donde resultan esenciales principios como el consentimiento informado, la minimización de datos, la transparencia algorítmica y la garantía de que ninguna persona sea objeto de decisiones completamente automatizadas sin la debida intervención humana significativa.

Desde una perspectiva constitucional, si bien los artículos 28 y 31 de la Constitución Política de la República de Guatemala (Asamblea Nacional Constituyente, 1985) garantizan el derecho de petición y el acceso a expedientes administrativos, no existe una consagración expresa del derecho a la protección de datos personales ni al *hábeas data*. Este vacío limita la posibilidad de establecer estándares jurídicos robustos frente a prácticas tecnológicas que impliquen tratamiento masivo de información personal, como ocurre en los sistemas de IA empleados para decisiones judiciales, análisis de reincidencia o predicción de riesgo.

Así, mientras otras jurisdicciones avanzan hacia una justicia digital inteligente, Guatemala permanece rezagada, sin una política pública articulada que acompañe la introducción de herramientas algorítmicas con criterios éticos, constitucionales y de derechos humanos. Este escenario exige con urgencia una reforma normativa integral que garantice la protección de los

¹ Si bien se establecen las Unidades de Acceso a la Información Pública en cada órgano estatal, no existe una sola entidad que, de manera general, optimice y controle sobre la protección de datos personales que involucren el uso de la IA.

datos personales, la rendición de cuentas tecnológica y la legitimidad democrática de la digitalización judicial, especialmente cuando se trata de decisiones de fondo -automatizadas o estandarizadas- que impactan derechos fundamentales.

Por otro lado, en cuanto al tema de autodeterminación informativa, ha sido la Corte de Constitucionalidad la que ha abordado desde el control constitucional esta temática. En este sentido, un ejemplo notable lo constituye el expediente 3552-2014 (*Apelación de sentencia de Amparo*, 2015) que versa sobre una acción de amparo promovida por el Procurador de los Derechos Humanos contra diversas entidades privadas -entre ellas INFORNET, DIGIDATA, INFILE y otras-, por la presunta violación de derechos fundamentales derivados de la captación, almacenamiento y difusión ilegítima de datos personales de personas particulares sin su consentimiento. El caso constituye uno de las sentencias más relevantes en el ámbito guatemalteco en materia de protección de datos personales, privacidad y autodeterminación informativa.

El acto reclamado consistía en la actividad sistemática y comercial de procesamiento y divulgación de información personal, crediticia, judicial, mercantil y de prensa, recopilada sin autorización de los titulares y difundida por medios informáticos, lo cual -según el amparista- vulneraba los derechos fundamentales a la intimidad, al trabajo, a una vida digna, a la defensa y a la autodeterminación informativa. Esta última se conceptualizó como una manifestación autónoma del derecho a la intimidad.

La Corte de Constitucionalidad, al resolver el recurso, confirmó la sentencia de amparo dictada por el Juzgado Décimo Primero de Primera Instancia Civil del departamento de Guatemala, constituido en Tribunal de Amparo, reconociendo que la actividad de las entidades reprochadas violaba derechos fundamentales de las personas afectadas. En particular, se hizo énfasis en el carácter lesivo del tratamiento de datos sin consentimiento expreso, señalando que el uso indiscriminado y comercial de datos personales, especialmente aquellos de naturaleza sensible o con potencial de generar discriminación social o económica, constituye una vulneración directa de la dignidad humana.

Este fallo es fundamental en el reconocimiento del derecho a la autodeterminación informativa en el orden constitucional guatemalteco, a pesar de que este derecho no está consagrado expresamente en la Constitución Política. La Corte lo vinculó al contenido protegido del derecho a la intimidad (los primeros cinco artículos de la Constitución Política de la República de Guatemala). Se trata, en esencia, de un reconocimiento implícito del derecho al *habeas data*, que aún no ha sido desarrollado de manera robusta a nivel legislativo, pero que se ha estado consolidando jurisprudencialmente [de manera pretoriana].

En el contexto de la inteligencia artificial, esta sentencia adquiere relevancia sustantiva, ya que establece criterios de legitimidad en el tratamiento de datos personales -como la necesidad del consentimiento, la finalidad específica del tratamiento y la prohibición de usos lesivos o discriminatorios- que deben ser considerados ante el despliegue de sistemas automatizados de análisis y decisión. Los sistemas de IA, especialmente los entrenados con bases de datos públicas

o privadas, pueden incurrir en las mismas prácticas que la Corte ha considerado inconstitucionales si no se someten a principios de legalidad, consentimiento y transparencia.

Identificación de las brechas regulatorias en la legislación actual para regular el uso de IA en el ámbito jurídico. La incorporación de herramientas de inteligencia artificial en la administración pública, y en particular en el sistema de justicia, demanda un *corpus iuris* sólido y ético que garantice la protección de los derechos fundamentales. En el contexto guatemalteco, dicho ecosistema está aún en formación y enfrenta múltiples deficiencias estructurales. Se pueden identificar -sin caer en reduccionismos teóricos o técnicos- al menos cuatro brechas regulatorias centrales que obstaculizan una implementación legítima y segura de la IA en el ámbito jurídico:

- i) Rezago normativo en la protección de datos personales en materia de tecnología;
- ii) Falta de implementación de políticas públicas que incluyan el manejo ético de la IA generativa;
- iii) Ausencia de capacidades en ciberseguridad y gestión de riesgos tecnológicos en la administración pública; e,
- iv) Inexistencia de un marco regulatorio integral sobre la ciberdelincuencia.

En el primer aspecto, es importante señalar que pesar de que Guatemala cuenta con la Ley de Acceso a la Información Pública (Decreto Número 57-2008, Congreso de la República de Guatemala), esta norma se encuentra desfasada frente a los estándares actuales en materia de tratamiento de datos personales, en especial en lo que respecta a tecnologías automatizadas. No existe una ley específica sobre protección de datos que contemple principios como la minimización de datos, el consentimiento informado, el derecho a la portabilidad, ni obligaciones claras para responsables y encargados del tratamiento. Esta carencia resulta especialmente grave ante la eventual utilización de IA generativa en la justicia, pues estos sistemas requieren grandes volúmenes de datos para su entrenamiento, procesamiento y toma de decisiones. La ausencia de garantías normativas pone en riesgo el derecho a la autodeterminación informativa, especialmente en contextos de vulnerabilidad procesal.

Ahora bien, en cuanto a la segunda brecha, la modernización tecnológica del Estado guatemalteco no ha venido acompañada de una reflexión estratégica sobre los impactos éticos, sociales y jurídicos del uso de la IA en las decisiones públicas. No se han adoptado marcos éticos institucionales ni protocolos específicos que regulen el diseño, implementación y fiscalización de algoritmos en el ámbito judicial, administrativo o policial. Además, el país carece de una estrategia nacional de IA que articule principios como la explicabilidad, la transparencia algorítmica, la intervención humana significativa y la prohibición de discriminación automatizada (León Pulido & Cañas Sánchez, 2025). Esto contrasta con otras jurisdicciones -como la Unión Europea- donde el enfoque basado en el riesgo y la regulación *ex ante* permiten identificar y controlar los efectos adversos de estos sistemas sobre los derechos humanos.

En cuanto a la tercera brecha, es importante mencionar que la infraestructura institucional en Guatemala no se encuentra preparada para enfrentar los riesgos de seguridad que conlleva la digitalización de procesos judiciales mediante herramientas inteligentes. Las políticas de ciberseguridad son fragmentarias, escasamente actualizadas y carecen de una arquitectura de gobernanza tecnológica transversal que permita identificar, prevenir y responder a vulnerabilidades en los sistemas judiciales. Esta situación no solo compromete la integridad de la información y los procesos, sino que genera incertidumbre jurídica sobre la autenticidad y fiabilidad de las decisiones automatizadas. El riesgo de ataques cibernéticos, manipulación de datos o uso indebido de sistemas predictivos exige protocolos claros de trazabilidad, auditoría y supervisión humana, los cuales aún no se encuentran institucionalizados en el país. Ejemplo de la falta de política pública en ciberseguridad lo representa el hackeo que sufrió el 27 de noviembre de 2023 el Ministerio de Finanzas Públicas en el país, vulnerando sistemas informáticos financieros (Gamarro, 2023).

Por último, Guatemala aún no cuenta con una legislación especializada y moderna en materia de ciberdelincuencia que aborde fenómenos como la manipulación algorítmica, el robo de identidad digital, el acceso indebido a sistemas informáticos, o la utilización de IA para fines delictivos (por ejemplo, *deepfakes* judiciales, perfiles falsos automatizados o suplantación de identidad). Este vacío se traduce en una limitada capacidad de las autoridades para investigar y sancionar delitos informáticos complejos, así como para proteger adecuadamente los derechos de las víctimas en el entorno digital. La falta de tipificación penal específica y de mecanismos procesales adecuados debilita el aparato de justicia frente a un fenómeno criminal que evoluciona con velocidad y sofisticación.

Habría que decir también que los delitos cometidos mediante sistemas informáticos han evolucionado constantemente. Es importante distinguir entre las formas tradicionales de delitos informáticos y las nuevas modalidades delictivas dirigidas contra sistemas informáticos, las cuales utilizan métodos de intrusión cada vez más sofisticados. Esta evolución ha sido impulsada, en gran medida, por los efectos de la globalización.

La pandemia de COVID-19 marcó un punto de inflexión en la expansión de estas nuevas formas de criminalidad. Durante este período, se popularizaron métodos delictivos que van desde acciones de Jáquers que ven la intrusión como un desafío técnico o deportivo, hasta ataques ejecutados por ciberdelincuentes altamente especializados que afectan negativamente a sistemas informáticos tanto del sector empresarial como del sector público.

En este contexto, la IA, si bien ha traído avances positivos en diversos campos, también ha sido utilizada como medio para facilitar nuevas formas de ciberdelincuencia. Ejemplos de esto incluyen el *phishing* automatizado, los *deepfakes* y el *malware* adaptativo, entre otros.

Uno de los principales desafíos que enfrenta Guatemala respecto a la ciberdelincuencia es la ausencia de un marco normativo robusto que regule esta forma de criminalidad organizada, la cual vulnera bienes fundamentales y, por ende, los derechos humanos. A la fecha, Guatemala no se ha adherido al Convenio de Budapest sobre la Ciberdelincuencia (2001), uno de los instrumentos internacionales clave en esta materia. Desde 2020, el país participa únicamente como observador.

A pesar de haberse presentado varias iniciativas legislativas en el Congreso de la República para abordar esta problemática (Iniciativa que dispone aprobar ley contra el cibercrimen, 2009; Iniciativa que dispone aprobar Ley contra la Ciberdelincuencia, 2017; Iniciativa que dispone aprobar Ley de Ciberseguridad, 2024; Iniciativa que dispone aprobar Ley de Prevención y Protección contra la Ciberdelincuencia, 2019), ninguna ha prosperado.

Entre 2020 y 2024, el Ministerio Público registró un total de 2,111 denuncias por delitos informáticos contemplados en el Título IV, capítulo VII del Código Penal, relativos a la libertad y seguridad de las personas (Unidad de Información Pública, Ministerio Público, 2024). Aunque estos delitos se cometen mediante el uso de tecnología, no abarcan adecuadamente las complejas formas de criminalidad organizada contemporánea.

Es útil clasificar la evolución de la ciberdelincuencia en tres generaciones (Vega Aguilar & Arévalo Minchola, 2022):

- i) Primera generación: delitos centrados en el riesgo informático, donde el daño se produce manipulando sistemas o datos informáticos (por ejemplo, acceso no autorizado a computadoras).
- ii) Segunda generación: delitos que implican redes telemáticas vulneradas mediante actividades criminales en el ciberespacio.
- iii) Tercera generación: delitos que requieren el uso del internet y de tecnologías avanzadas como la inteligencia artificial (Castaldo, 2024).

En el caso de Guatemala, puede decirse que el país enfrenta una fusión de la primera y segunda generación de ciberdelitos, pero aún se encuentra rezagado frente a las amenazas propias de la tercera generación. Por ello, es fundamental que el Estado impulse el desarrollo de un marco legal específico que aborde adecuadamente estos delitos, sin descuidar los principios y garantías establecidos en materia de derechos humanos.

Además, diversos grupos en situación de vulnerabilidad se ven particularmente afectados por estas nuevas formas de criminalidad, ya que el uso indebido de la inteligencia artificial también facilita delitos como la trata de personas y el abuso sexual infantil en línea (Martínez Cantón, 2024).

En consecuencia, el Estado de Guatemala debe avanzar en la elaboración de políticas públicas y marcos normativos que salvaguarden los bienes jurídicos fundamentales amenazados por la ciberdelincuencia y garantizar que su regulación esté alineada con los estándares internacionales de derechos humanos.

Propuesta normativa y de política pública para la regulación de la inteligencia artificial en el ámbito jurídico guatemalteco

Frente al panorama de rezago y dispersión normativa que caracteriza al ordenamiento jurídico guatemalteco en relación con la IA, es urgente avanzar hacia la construcción de un marco

legal específico, complementado con una política pública integral, que permita una implementación ética, segura y eficaz de la IA en el ámbito judicial. Esta propuesta se articula en dos niveles: normativo y estratégico.

Hacia una ley de inteligencia artificial y protección de derechos en la administración pública y la justicia. Se propone la formulación de una ley especial sobre inteligencia artificial, enfocada en su uso dentro del sector público, especialmente en órganos jurisdiccionales, administrativos y fiscales. Esta ley debería incluir, como mínimo, los siguientes ejes estructurales:

- i) Principios rectores: legalidad, transparencia algorítmica, explicabilidad, responsabilidad, intervención humana significativa, no discriminación, justicia tecnológica, trazabilidad y protección reforzada de grupos en situación de vulnerabilidad.
- ii) Clasificación de sistemas de IA por niveles de riesgo, tomando como referencia el enfoque europeo (Reglamento UE 2024/1689), estableciendo prohibiciones para usos inaceptables, requisitos estrictos para usos de alto riesgo (como decisiones judiciales automatizadas), y obligaciones más flexibles para sistemas de bajo impacto.
- iii) Regulación de decisiones automatizadas en el ámbito judicial y administrativo, exigiendo trazabilidad, explicabilidad y posibilidad de impugnación. La ley debería prohibir la emisión de resoluciones jurisdiccionales vinculantes exclusivamente fundadas en IA sin validación humana previa.
- iv) Protección de datos personales: incorporación expresa del principio de minimización de datos, evaluación de impacto en derechos fundamentales antes del despliegue de sistemas, y prohibición del uso de datos sensibles sin consentimiento informado.
- v) Supervisión institucional: creación de una autoridad nacional de supervisión de sistemas algorítmicos en el sector público, autónoma, con funciones de auditoría, fiscalización, registro y control.
- vi) Mecanismos de rendición de cuentas y auditoría algorítmica, incluyendo la obligación de evaluar sesgos, asegurar la equidad en los resultados, y publicar informes técnicos periódicos.

Estrategia nacional de IA para la justicia y la administración pública. Complementariamente, se propone la formulación de una Estrategia Nacional de Inteligencia Artificial para la justicia y la administración pública, con los siguientes ejes estratégicos:

- i) Diagnóstico institucional y evaluación de capacidades tecnológicas y jurídicas en el Organismo Judicial, Ministerio Público, Instituto de la Defensa Pública Penal y Ministerio de Gobernación.

- ii) Capacitación especializada y formación judicial en ética digital, derechos humanos y funcionamiento técnico de sistemas de IA, destinada a jueces, fiscales, defensores y operadores del sistema.
- iii) Diseño y prueba de sistemas piloto de IA explicables y de bajo riesgo, como herramientas de gestión judicial (asignación de casos, búsqueda de jurisprudencia, redacción asistida, generador de decisiones en casos similares), evitando por el momento su uso en decisiones sustantivas o de fondo.
- iv) Fortalecimiento de la infraestructura de ciberseguridad y gobernanza digital, incluyendo protocolos de respuesta ante incidentes tecnológicos, integración con sistemas de gestión documental, y protección de información sensible.
- v) Participación ciudadana y control democrático, asegurando mecanismos de consulta pública, veeduría civil y auditoría ciudadana sobre el uso de tecnologías en la justicia.
- vi) Armonización regional y cooperación internacional, a través de convenios con países latinoamericanos y europeos que ya han iniciado procesos regulatorios en IA y justicia digital, para recibir asistencia técnica, compartir estándares y generar un ecosistema latinoamericano de gobernanza algorítmica.

A manera de conclusión

El análisis realizado evidencia que Guatemala se encuentra en una etapa incipiente respecto a la regulación de la inteligencia artificial en el ámbito jurídico, lo cual genera riesgos significativos para los derechos fundamentales, especialmente en materia de protección de datos personales, transparencia y debido proceso. A diferencia de otras jurisdicciones latinoamericanas, como Colombia y México, el país carece de estándares normativos claros para regular el uso de tecnologías automatizadas en procesos judiciales o administrativos. La pregunta planteada en el título, ¿un derecho inteligente o una inteligencia artificial para el derecho?, se responde desde una perspectiva garantista, ya que no es el derecho el que debe adaptarse de manera acrítica a la tecnología, sino que la IA debe ser regulada de modo que se subordine a los valores y principios fundamentales del Estado de constitucional de Derecho.

Entre los resultados más relevantes, se identificaron cuatro brechas estructurales: i) un rezago normativo en la protección de datos personales, con ausencia de una ley específica y de una autoridad supervisora independiente; ii) la falta de políticas públicas que introduzcan marcos éticos que orienten el manejo de la IA en el sector público; iii) la debilidad de las capacidades institucionales en ciberseguridad y gestión de riesgos; y, iv) la inexistencia de un marco integral de ciberdelincuencia acorde con las amenazas derivadas de tecnologías inteligentes.

A partir de estas constataciones, se propone la creación de una Ley de inteligencia artificial y Protección de Derechos, centrada en principios como la legalidad, transparencia algorítmica, explicabilidad y rendición de cuentas, así como el desarrollo de una Estrategia Nacional de IA para

la Justicia, que incluya capacitación judicial, plan piloto controlado de IA explicable, fortalecimiento de la ciberseguridad y mecanismos de control democrático. Solo mediante un enfoque garantista y adaptado a la realidad nacional será posible avanzar hacia una modernización judicial que respete la dignidad humana y los principios constitucionales.

Referencias

- Asamblea Nacional Constituyente (1985). Constitución Política de la República de Guatemala.
- Ashley, K. D. (2023). Inteligencia Artificial y analítica jurídica. Nuevas herramientas para la práctica del Derecho en la era digital (M. Parmigiani, Trad.). Yachay legal y Facultad de Derecho de la Pontificia Universidad Católica del Perú.
- Castaldo, A. R. (2024). IA y metaverso: Nuevos peligros y oportunidades. En Libro Homenaje al Profesor Javier de Vicente Remesal por su 70º aniversario (Primera edición, pp. 1225-1231). Agencia Estatal Boletín Oficial del Estado, Fundación Internacional de Ciencias Penales.
- Comisión Interamericana de Derechos Humanos (CIDH). (2023, junio 2). CIDH manifiesta su preocupación por el aumento de casos sobre uso de Pegasus en México [Comunicado de Prensa No. 109/23]. Comisión Interamericana de Derechos Humanos (CIDH). <https://www.oas.org/es/cidh/jsForm/?File=/es/cidh/prensa/comunicados/2023/109.as>
- Congreso de la República de Guatemala (2009). Iniciativa que dispone aprobar ley contra el cibercrimen, No. 4054. https://www.congreso.gob.gt/detalle_pdf/iniciativas/2227#gsc.tab=0
- Congreso de la República de Guatemala (2017). Iniciativa que dispone aprobar Ley contra la Ciberdelincuencia, No. 5254. https://www.congreso.gob.gt/detalle_pdf/iniciativas/4266#gsc.tab=0
- Congreso de la República de Guatemala (2024). Iniciativa que dispone aprobar Ley de Ciberseguridad, No. 6347. https://www.congreso.gob.gt/detalle_pdf/iniciativas/6074
- Congreso de la República de Guatemala (2019). Iniciativa que dispone aprobar Ley de Prevención y Protección contra la Ciberdelincuencia, No. 5601. https://www.congreso.gob.gt/detalle_pdf/iniciativas/5614
- Congreso de la República de Guatemala (2008). Ley de Acceso a la Información Pública, Decreto Número 57-2008.
- Congreso de la República de Guatemala (2018). Ley de Avisos Electrónicos, Decreto Número 24-2018.

- Congreso de la República de Guatemala (2022). Ley de Tramitación Electrónica de Expedientes Judiciales, Decreto Número 13-2022.
<https://leyes.infile.com/visualizador2/index.php?id=84690#0>
- Congreso de la República de Guatemala (2008). Ley para el Reconocimiento de las Comunicaciones y Firmas Electrónicas, Decreto Número 47-2008.
<https://leyes.infile.com/visualizador2/index.php?id=59637#0>
- Congreso de la República de Guatemala (2011). Ley Reguladora de las Notificaciones por Medios Electrónicos en el Organismo Judicial, Decreto Número 15-2011.
<https://leyes.infile.com/visualizador2/index.php?id=64897#0>
- Consejo de Europa (2001). Convenio sobre la Ciberdelincuencia (Convenio de Budapest).
https://www.oas.org/juridico/english/cyb_pry_convenio.pdf
- Corte Constitucional de Colombia (2024). Sentencia sobre el uso de herramientas de inteligencia artificial generativas en procesos judiciales de tutela, expediente No. T-323 de 2024.
- Corte de Constitucionalidad de Guatemala (2015). Apelación de sentencia de Amparo, expediente No. 3552-2014 de 10 de febrero de 2015.
- Corte de Constitucionalidad de Guatemala (2020). Disposiciones reglamentarias para la celebración de Vistas Públicas por Videoconferencia. Acuerdo Número 3-2020,
<https://leyes.infile.com/visualizador2/index.php?id=81275#0>
- Corte de Constitucionalidad de Guatemala (2016). Reglamento para el uso del Sistema Informático de Expedientes de la Corte de Constitucionalidad (SIECC), Acuerdo Número 03-2016, <https://leyes.infile.com/visualizador2/index.php?id=74112#0>
- Corte Europea de Justicia (2014). Google v. España, expediente No. C-131/12 de 13 de mayo de 2014. <https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:62012CJ0131>
- Corte Suprema de Justicia de Guatemala (2016). Acuerdo de Cooperación entre el Organismo Judicial y la Superintendencia de Administración Tributaria, el cual implementa la figura del Embargo Electrónico en los Tribunales Económico Coactivo, Acuerdo Número 2-2016.
<https://leyes.infile.com/visualizador2/index.php?id=74048#0>
- Corte Suprema de Justicia de Guatemala (2010). Adquisición por compra del equipo audiovisual a través de videoconferencia e instalación a fin de resguardar la integridad de los jueces, como de los sujetos procesales. Acuerdo Número 57-2010.
<https://leyes.infile.com/visualizador2/index.php?id=63411#0>
- Corte Suprema de Justicia de Guatemala (2020). Creación de los juzgados primero y segundo de paz penal móvil con competencia exclusiva para primeras declaraciones y exhibiciones

- personales bajo el sistema de audiencias por medios electrónicos. Acuerdo Número 25-2020, <https://leyes.infile.com/visualizador2/index.php?id=81350#0>
- Corte Suprema de Justicia de Guatemala (2020). Creación e implementación del Sistema Informático del Archivo General de Tribunales y de la Delegación del Archivo General de Tribunales de Quetzaltenango -SIAT- e implementación de la firma electrónica interna y avanzada institucional. Acuerdo Número 68-2018. <https://leyes.infile.com/visualizador2/index.php?id=81259#0>
- Corte Suprema de Justicia de Guatemala (2012). Implementación de la «Carpeta Judicial Electrónica» como parte integral de la Política Cero Papel del Organismo Judicial. Acuerdo Número 53-2012, <https://leyes.infile.com/visualizador2/index.php?id=66646#0>
- Corte Suprema de Justicia de Guatemala (2018). Implementación de la Firma Electrónica Interna De La Unidad De Antecedentes Penales Del Organismo Judicial y Firma Electrónica Avanzada Institucional. Acuerdo Número 27-2018. <https://leyes.infile.com/visualizador2/index.php?id=78304#0>
- Corte Suprema de Justicia de Guatemala (2017). Implementación de la Firma Electrónica Interna Jurisdiccional del Organismo Judicial y Firma Electrónica Avanzada Institucional en las Actuaciones Judiciales de los Órganos Jurisdiccionales y las Unidades Administrativas. Acuerdo Número 75-2017. <https://leyes.infile.com/visualizador2/index.php?id=76714#0>
- Corte Suprema de Justicia de Guatemala (2012). Los Jueces podrán tener comunicaciones vía electrónica a la entidad que corresponda al Registro General de la Propiedad, a los bancos del sistema, Dirección General de Migración, a la Policía Nacional Civil y al Registro Fiscal de Vehículo. Acuerdo Número 55-2012. <https://leyes.infile.com/visualizador2/index.php?id=66848#0>
- Corte Suprema de Justicia de Guatemala (2012). Los Juzgados de lo Económico Coactivo, podrán remitir vía correo electrónico las órdenes de embargo de las cuentas de depósitos bancarios, que deben proporcionar las instituciones bancarias del país. Acuerdo Número 2-2012, <https://leyes.infile.com/visualizador2/index.php?id=65511#0>
- Corte Suprema de Justicia de Guatemala (2020). Reglamento de audiencias por medios electrónicos de comunicación audiovisual en tiempo real, Acuerdo Número 35-2020. <https://leyes.infile.com/visualizador2/index.php?id=81680#0>
- Corte Suprema de Justicia de Guatemala (2012). Reglamento de la Ley Reguladora de las Notificaciones por Medios Electrónicos en el Organismo Judicial, Acuerdo Número 11-2012. <https://leyes.infile.com/visualizador2/index.php?id=65874#0>
- Corte Suprema de Justicia de Guatemala (2019). Reglamento De Servicios Electrónicos Prestados por la Cámara De Amparo y Antejuicio de la Corte Suprema De Justicia, Acuerdo Número 49-2019. <https://leyes.infile.com/visualizador2/index.php?id=80105#0>

- Corte Suprema de Justicia de Guatemala (2011). Reglamento del Sistema de Gestión de Tribunales, No. Acuerdo Número 20-2011.
<https://leyes.infile.com/visualizador2/index.php?id=64422#0>
- Corte Suprema de Justicia de Guatemala (2023). Reglamento General de la Ley de Tramitación Electrónica de Expedientes Judiciales, Acuerdo Número 8-2023.
<https://leyes.infile.com/visualizador2/index.php?id=86649#0>
- Corte Suprema de Justicia de Guatemala (2016). Reglamento para el desarrollo de las declaraciones por videoconferencia en materia disciplinaria dentro del organismo judicial, Acuerdo Número 6-2016.
<https://leyes.infile.com/visualizador2/index.php?id=74121#0>
- Corte Suprema de Justicia de Guatemala (2009). Reglamento para el desarrollo de las Declaraciones por videoconferencia reguladas en las reformas al Código Procesal Penal, Decreto 51-92, Acuerdo Número 31-2009,
<https://leyes.infile.com/visualizador2/index.php?id=61772#0>
- Corte Suprema de Justicia de Guatemala (2017). Se autoriza a los órganos jurisdiccionales que conocen en materia de Trabajo y Previsión Social y a los órganos jurisdiccionales que tramiten procesos en materia constitucional, de todo el territorio notificar en forma electrónica las resoluciones, Acuerdo Número 46-2017.
<https://leyes.infile.com/visualizador2/index.php?id=76282#0>
- Corte Suprema de Justicia de Guatemala (2017). Se autoriza a todos los órganos jurisdiccionales del ramo penal, notificar de forma electrónica, las resoluciones emitidas dentro de los expedientes en los cuales las partes y demás sujetos procesales, se adhieran al sistema de notificación, Acuerdo Número 8-2017.
<https://leyes.infile.com/visualizador2/index.php?id=75780#0>
- Corte Suprema de Justicia de Guatemala (2015). Utilización del sistema de diligencias judiciales electrónicas para la optimización de oficios. Acuerdo Número 16-2015.
<https://leyes.infile.com/visualizador2/index.php?id=72785#0>
- Corte Suprema de Justicia de la Nación de Argentina (2022). Denegri, Natalia Ruth c/ Google Inc. s/ derechos personalísimos, expediente No. 50016/2016 de 28 de junio de 2022.
- Estevez, E., Linares Lejarraga, S., & Fillottrani, P. (2020). PROMETEA. Transformando la administración de justicia con herramientas de Inteligencia Artificial. Banco Interamericano de Desarrollo. <http://hdl.handle.net/11336/183777>
- Gamarro, U. (2023, noviembre 28). Ataque cibernético impide las operaciones del Ministerio de Finanzas por segundo día consecutivo [Prensa]. Prensa Libre. <https://www.prensalibre.com/economia/ataque-cibernetico-impide-las-operaciones-informaticas-del-ministerio-de-finanzas-por-segundo-dia-consecutivo/>

- Kong, M. (1993). *Inteligencia Artificial* (Primera edición). Pontificia Universidad Católica del Perú-Fondo Editorial.
- León Pulido, M. M., & Cañas Sánchez, E. A. (2025). El futuro de los derechos humanos en la era posthumana: Un análisis desde el derecho y la Inteligencia Artificial. En E. A. Velandia Canosa (Ed.), *Derecho Procesal Constitucional. Inteligencia Artificial y neuroderechos* (pp. 134-159). Ediciones Nueva Jurídica.
- Martínez Cantón, S. (2024). La cibercaptación de víctimas de trata de personas. En M. García Mosquera, V. Rodríguez Vásquez, M. Díaz y García Conlledo, & D.-M. Luzón Peña (Eds.), *Libro Homenaje al Profesor Javier de Vicente Remesal por su 70.o aniversario* (Primera edición, pp. 1045-1054). Agencia Estatal Boletín Oficial del Estado, Fundación Internacional de Ciencias Penales.
- Ministerio de Justicia. (2025, mayo 8). El programa piloto de IA Generativa en la Justicia arrojó resultados positivos. Argentina.gob.ar. <https://www.argentina.gob.ar/noticias/el-programa-piloto-de-ia-generativa-en-la-justicia-arrojo-resultados-positivos>
- Parlamento Europeo y del Consejo (2024). Reglamento de Inteligencia Artificial, No. 2024/1689.
- Presidencia del Organismo Judicial y Corte Suprema de Justicia de Guatemala (2019). Firma Electrónica Para La Unidad De Información Pública Del Organismo Judicial. Acuerdo Número 038/019. <https://leyes.infile.com/visualizador2/index.php?id=79659#0>
- Presidencia del Organismo Judicial y Corte Suprema de Justicia de Guatemala (2023). Reglamento de Notificaciones Electrónicas en los Procedimientos Administrativos Internos del Organismo Judicial, Acuerdo Número 189-2023. <https://leyes.infile.com/visualizador2/index.php?id=87462#0>
- Presidencia del Organismo Judicial y Corte Suprema de Justicia de Guatemala (2013). Instructivo para realizar notificaciones electrónicas en el área administrativa del Organismo Judicial. Acuerdo Número 1/2013. <https://leyes.infile.com/visualizador2/index.php?id=67323#0>
- Presidente de la República de Guatemala (2009). Reglamento de la Ley para el Reconocimiento de las Comunicaciones y Firmas Electrónicas, Acuerdo Gubernativo Número 135-2009. <https://leyes.infile.com/visualizador2/index.php?id=60881#0>
- Queralt, J. J. (2024). Caso Pegasus: Un haz de vulneración de derechos. En M. García Mosquera, V. Rodríguez Vásquez, M. Díaz y García Conlledo, & D.-M. Luzón Peña (Eds.), *Libro Homenaje al Profesor Javier de Vicente Remesal por su 70.o aniversario* (Primera edición, pp. 1357-1369). Agencia Estatal Boletín Oficial del Estado, Fundación Internacional de Ciencias Penales.
- Quintero Londoño, D. (2025). Responsabilidad del estado por daños causados por medios tecnológicos. Propuesta inicial para la creación y declaración de principios para el

uso, manejo y desarrollo de inteligencias artificiales en Colombia. Grupo Editorial Ibáñez.

Rebollo Delgado, L. (2023). Inteligencia Artificial y derechos fundamentales. Editorial DYKINSON.

Sánchez Barrilao, J. F. (2022). Constitucionalismo digital: Entre realidad digital, prospectiva tecnológica y mera distopía constitucional. Revista da AJURIS-Qualis A2, 49(152), 395-418.

Sistema Argentino de Información Jurídica -SAIJ-. (2025, marzo 25). El Programa Piloto de Uso de la IA Generativa en la Justicia Argentina arrojó resultados positivos. SAIJ. <https://www.saij.gob.ar/NV46008>

Suprema Corte de Justicia de la Nación de México (2024). Recurso de revisión en materia de seguridad nacional previsto en la Ley General de Transparencia y Acceso a la Información Pública, expediente No. 27/2021 de 6 de febrero de 2024. <file:///D:/Users/Sbarrientos/Downloads/content.pdf>

Unidad de Información Pública, Ministerio Público. (2024). Reporte estadístico a nivel nacional, denuncias por delitos informáticos, registrados en el período comprendido del 01/01/2020 al 29/08/2024 (No. Resolución UDIP/G 2024-005136 /komg; pp. 1-3).

Vega Aguilar, J. A., & Arévalo Minchola, M. (2022). Ciberdelitos. Análisis en el sistema penal (Primera edición). Iustitia.

Derechos de Autor (c) 2025 Santos Romeo Barrientos Aldana

El autor declara que realizó la investigación con fondos propios y que no tiene conflicto de interés.



Este texto está protegido por una licencia [Creative Commons 4.0](https://creativecommons.org/licenses/by/4.0/).

Usted es libre para Compartir —copiar y redistribuir el material en cualquier medio o formato— y Adaptar el documento —remezclar, transformar y crear a partir del material— para cualquier propósito, incluso para fines comerciales, siempre que cumpla la condición de:

Atribución: Usted debe dar crédito a la obra original de manera adecuada, proporcionar un enlace a la licencia, e indicar si se han realizado cambios. Puede hacerlo en cualquier forma razonable, pero no de forma tal que sugiera que tiene el apoyo del licenciante o lo recibe por el uso que hace de la obra.

[Resumendelicencia](#) - [Textocompletodelalicencia](#)

