



**UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL**

**FACULTAD DE JURISPRUDENCIA, CIENCIAS SOCIALES Y
POLITICAS**

CARRERA DE DERECHO

TEMA:

**Garantías procesales para la protección de datos personales frente a
tecnologías automatizadas**

AUTORES

Pinargote Mendoza, María José

Villegas Melgarejo, Carlos José

Trabajo de titulación previo a la obtención del título de

ABOGADO

TUTOR:

Ab. Mendoza Colamarco, Elker Pavlova, Mgts

Guayaquil, Ecuador

25 agosto del 2026



UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

**FACULTAD DE JURISPRUDENCIA, CIENCIAS SOCIALES Y
POLITICAS**

CARRERA DE DERECHO

CERTIFICACIÓN

Certificamos que el presente trabajo de titulación fue realizado en su totalidad por **Pinargote Mendoza, María José; Villegas Melgarejo, Carlos José**, como requerimiento para la obtención del título de **Abogado**.

TUTOR (A)

f. _____

Ab. Elker Pavlova Mendoza Colamarco Mgts

DIRECTOR DE LA CARRERA

f. _____

Dra. Nuria Pérez Puig-Mir, PhD.

Guayaquil, a los 25 días del mes de agosto del año 2026



UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

**FACULTAD DE JURISPRUDENCIA, CIENCIAS SOCIALES Y
POLITICAS**

CARRERA DE DERECHO

DECLARACIÓN DE RESPONSABILIDAD

Nosotros, **Pinargote Mendoza, María José; Villegas Melgarejo, Carlos José**

DECLARAMOS QUE:

El Trabajo de Titulación, **Garantías procesales para la protección de datos personales frente a tecnologías automatizadas** previo a la obtención del título de **Abogado** ha sido desarrollado respetando derechos intelectuales de terceros conforme las citas que constan en el documento, cuyas fuentes se incorporan en las referencias o bibliografías. Consecuentemente este trabajo es de nuestra total autoría.

En virtud de esta declaración, nos responsabilizamos del contenido, veracidad y alcance del Trabajo de Titulación referido.

Guayaquil, a los 25 días del mes de agosto del año 2026

AUTORES

f.  Validar Únicamente en FirmaEC.
Firmado electrónicamente por:
**MARIA JOSE
PINARGOTE MENDOZA**

Pinargote Mendoza, María José

f.  Validar Únicamente en FirmaEC.
Firmado electrónicamente por:
**CARLOS JOSE
VILLEGAS MELGAREJO**

Villegas Melgarejo, Carlos José



UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

FACULTAD DE JURISPRUDENCIA, CIENCIAS SOCIALES Y POLITICAS

CARRERA DE DERECHO

AUTORIZACIÓN

Nosotros, **Pinargote Mendoza, María José; Villegas Melgarejo, Carlos José**

Autorizamos a la Universidad Católica de Santiago de Guayaquil a la **publicación** en la biblioteca de la institución del Trabajo de Titulación, **Garantías procesales para la protección de datos personales frente a tecnologías automatizadas**, cuyo contenido, ideas y criterios son de nuestra exclusiva responsabilidad y total autoría.

Guayaquil, a los 25 días del mes de agosto del año 2025

AUTORES

f.  Validar únicamente en FirmaEC.
Firmado electrónicamente por:
**MARIA JOSE
PINARGOTE MENDOZA**

Pinargote Mendoza, María José

f.  Validar únicamente en FirmaEC.
Firmado electrónicamente por:
**CARLOS JOSE
VILLEGAS MELGAREJO**

Villegas Melgarejo, Carlos José



UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

FACULTAD DE JURISPRUDENCIA, CIENCIAS SOCIALES Y POLITICAS

CARRERA DE DERECHO



Certificado de análisis

Compilatio Magister+ | UCSG-EC- Universidad Católica de Santiago de Guayaquil

Tesis Carlos Villegas- María José Pinargote (1)

ID : adbcfcf86fff9ecef2a78bac60b70136ee556d0d



4%

Textos sospechosos

Nombre del fichero : Tesis Carlos Villegas- María José Pinargote (1).txt
Tamaño del archivo original : 981,17 kB
Número de palabras : 7259

Depositante : Elker Pavlova Mendoza Colamarco
Fecha de depósito : 21 de agosto de 2026
Tipo de carga : interface
fecha de fin de análisis : 21 de agosto de 2026

TUTOR

ELKER PAVLOVA
MENDOZA
COLAMARCO

Firmado digitalmente
por ELKER PAVLOVA
MENDOZA COLAMARCO
Fecha: 2026.08.21
16:29:45 -05'00'

Dra. Elker Pavlova Mendoza Colamarco

AUTORES



Validez documente en FirmadU:
Firmado digitalmente por:
MARIA JOSE
PINARGOTE MENDOZA

María José Pinargote



Validez documente en FirmadU:
Firmado digitalmente por:
CARLOS JOSE
VILLEGAS MELGAREJO

Carlos José Villegas

Guayaquil, a los 25 días del mes de agosto del año 2025

AGRADECIMIENTO

Con infinita gratitud a Dios por ser mi Guía en cada paso de este camino, llegar a concluir esta etapa representa reconocimiento de todas las personas que me han acompañado e hicieron posible la culminación de este proceso, a lo largo de mi desarrollo académico fueron muchas las personas que aportaron de manera e indirecta con su apoyo, conocimiento y motivación, demostrando así que este logro no es únicamente individual sino también el resultado de todo el apoyo brindado.

A mis padres y mis hermanos, por los sacrificios silenciosos, el apoyo y amor incondicional que me han brindado desde pequeña, por nunca soltar mi mano. Gracias por acompañarme en cada etapa de mi vida y sobre todo por ser el hogar al que siempre puedo regresar.

A la Abogada Elker Mendoza, expreso mi sincero agradecimiento por su orientación académica, compromiso profesional y acompañamiento constante durante el desarrollo de este trabajo de Titulación.

Al Abogado Gonzalo Burgassi, por las lecciones valiosas que aprendí a lo largo de la carrera, por el apoyo y experiencia como Abogado y estudiante en su momento.

A Carlos Villegas, mi compañero de tesis y gran amigo, gracias por tu apoyo y motivación durante esta etapa, por los aprendizajes compartidos y sobre todo por los momentos que hicieron que este proceso fuese más llevadero.

A mi pareja, Ronny, por estar a mi lado durante este proceso, por su amor, paciencia y apoyo incondicional. Gracias por creer en mí y motivarme en los momentos difíciles.

A mis amigas de la vida, Jessica, Nicole, Carla, Anisse y Angie, por acompañarme en este recorrido académico y personal, por su apoyo sincero y por estar presentes tanto en los momentos difíciles como en las victorias.

Finalmente, expreso mi sincero agradecimiento a todas aquellas personas que, de una u otra manera, formaron parte de este proceso académico

María José Pinargote Mendoza,

AGRADECIMIENTO

En el marco del presente trabajo de titulación, previo a la obtención del título de tercer nivel de Abogado, expreso mi más profundo agradecimiento en primer lugar a Dios. Agradezco la fortaleza, el discernimiento, la resiliencia y la capacidad que me brindó para llegar a este momento y culminar con éxito mi etapa académica. Reconozco que cada paso en este camino ha sido guiado y sostenido por su presencia; confié plenamente en su voluntad y en su intercesión para mi futuro personal y profesional, Gracias Padre.

Agradezco profundamente a mis padres, quienes han estado a mi lado en cada etapa de mi trayectoria académica. Gracias por su respaldo incondicional, no solo a través de su esfuerzo económico, sino sobre todo por su constante apoyo emocional. Sus consejos oportunos, su guía, y su presencia inquebrantable ante cualquier circunstancia han sido mi mayor fortaleza, Este logro también les pertenece. Los amo queridos padres. Asimismo, agradezco a mis hermanos, quienes, con su presencia diaria, cariño y complicidad se han convertido en un soporte indispensable y constante en mi vida.

Expreso mi gratitud a mis grandes amigos, con quienes compartí inolvidables experiencias en las aulas y en los pasillos de la universidad; gracias por su respaldo sincero y por hacer más ameno este trayecto formativo. Asimismo, agradezco a mi pareja por su compañía constante, su entrega y su amor incondicional, los cuales fueron un motor indispensable para alcanzar esta meta.

A mi compañera de tesis, por compartir este reto y estar a lo largo de mi vida universitaria. Gracias porque hemos consolidado una amistad genuina que trascienden aulas. A mi tutora, Mgs. Elker Mendoza, por su invaluable guía en la elaboración de este trabajo de titulación y en las materias que tuve el honor de cursar bajo su cátedra.

Carlos José Villegas Melgarejo.

DEDICATORIA

A Dios, por guiar mis pasos y permitir alcanzar mis sueños

A mi papá, Antonio Pinargote, hoy quiero dedicarte uno de los logros más importantes de mi vida, no existen palabras para agradecer y demostrar toda mi admiración por ti. Desde pequeña te vi como un héroe, y con el pasar del tiempo esa imagen jamás cambio, desde ahí comprendí la fortaleza con la que has enfrentado cada desafío que la vida nos ha puesto. Espero muy pronto poder devolverte un pedacito de todo lo que has hecho por mí.

A mi mamá, Mayra Mendoza, siempre he admirado la mujer tan fuerte y valiente que eres, de ti aprendí que rendirse nunca ha sido una opción. Tu confianza y admiración fueron impulso para nunca desistir y seguir adelante. Este logro también te pertenece, porque sin ti, jamás habría llegado hasta aquí.

A mis hermanos, José, Alex y Amaya, el regalo más grande que mis papas me han dado, su alegría ilumina mi vida y me recuerda siempre la razón para seguir, jamás hubiese podido sin su amor y su apoyo.

A mi novio y compañero de vida, Ronny Recalde, por tu motivación constante, por tu apoyo incondicional, tu presencia en mi vida es un regalo invaluable.

A mi abuelito Pedro Pinargote, aunque hoy no este físicamente en nuestras vidas, estoy segura de lo orgulloso que estaría de mí en este momento, esto lo hago en honor a tu memoria y al amor que siempre me brindaste.

A María José, aquella niña de 5 años que soñaba sin imaginar todo lo que algún día sería capaz de lograr, Hoy, con orgullo, puedo decirle; lo estamos logrando, pequeña.

María José Pinargote Mendoza,

DEDICATORIA

El presente trabajo de titulación se lo dedico, en primer lugar a mi Padre Celestial, Dios, quien ha sido mi principal pilar de fortaleza y guía en cada paso del camino. A él le entrego este esfuerzo, pues en los días de mayor angustia e incertidumbre siempre estuvo presente para brindarme paz y resiliencia. Este éxito y todos los que estén por venir son para Él.

A mis amados padres, les dedico este logro por su presencia y entrega incondicional, por brindarme el consejo oportuno, su guía constante, su amor, comprensión y complicidad, tanto dentro como fuera de mi vida académica. Soy plenamente consciente de los innumerables esfuerzos y sacrificios que han realizado para que hoy pueda alcanzar este sueño compartido; desde siempre conocieron mi anhelo de ser abogado e hicieron hasta lo imposible por verlo hecho realidad. Este triunfo les pertenece. Dedico también a mis hermanos, testigos de mis jornadas de estudio, noches de esfuerzo y momentos de tensión académica. Gracias por su respaldo incondicional, su comprensión y por ser un pilar diario en mi vida.

A mi abuela, por su cariño y compañía constante, y a la memoria de mis abuelos, quienes desde el cielo celebran conmigo este y todos los logros que he cosechado. Desde pequeño sabían de mi sueño de convertirme en Abogado, y hoy culmino esta etapa con la certeza de que me han cuidado en cada paso. Sé que les hubiera encantado estar físicamente conmigo, pero hoy lo están en espíritu y en el corazón. Gracias por haber creído siempre en mi desde que era un niño.

A mi pareja por su amor incondicional, su paciencia infinita y por convertirse en mi principal refugio y sostén en cada desafío que se presentó. Gracias por creer en mí y celebrar cada meta a mi lado. Asimismo, dedico este logro a mis amigos más cercanos, cómplices de extensas jornadas de estudio, risas en los pasillos, y experiencias compartidas dentro y fuera las aulas. Su lealtad y compañía sincera hicieron de esta etapa universitaria in camino inolvidable.

Carlos José Villegas Melgarejo.



UNIVERSIDAD CATÓLICA DE SANTIAGO DE GUAYAQUIL

**FACULTAD DE JURISPRUDENCIA, CIENCIAS SOCIALES Y
POLITICAS**

CARRERA DE DERECHO

TRIBUNAL DE SUSTENTACIÓN

f. _____

Dr. LEOPOLDO XAVIER ZAVALA EGAS

DECANO DE CARRERA

f. _____

Ab. MARITZA GINETTE REYNOSO GAUTE, Mgs.

COORDINADOR DEL ÁREA

f. _____

Dr. MARCO ANTONIO ELIZALDE JALIL

OPONENTE

INDICE

INTRODUCCIÓN.....	2
Antecedentes Históricos	3
Definiciones.....	4
Naturaleza Jurídica.....	6
Pregunta de Investigación.....	8
El Rol De La Superintendencia De Protección De Datos Personales Frente A Los Fallos Algorítmicos.....	10
La Imputación Corporativa Por Inobservancia De La Reserva De Humanidad	12
CONCLUSIONES.....	13
RECOMENDACIONES	14
REFERENCIAS	15

RESUMEN

La proliferación de sistemas de inteligencia artificial para el tratamiento masivo de datos personales plantea una severa encrucijada para la tutela judicial efectiva en Ecuador. Los algoritmos operan bajo el fenómeno de la "caja negra", configurando entornos opacos donde resulta inviable reconstruir el nexo causal o identificar la culpa conforme a las reglas clásicas del derecho civil. Esta asimetría técnica genera una barrera probatoria insuperable frente a las corporaciones bajo el régimen dispositivo ordinario del COGEP.

Mediante un análisis dogmático y normativo, se confronta el principio de autodeterminación informativa y el derecho a no ser sometido a decisiones automatizadas exclusivas (LOPDP, Resolución SPDP-SPD-2026-0009-R y estándares comparados). Se concluye que las normas procesales ordinarias resultan ineficaces para tutelar a los afectados, habilitando la evasión de responsabilidad corporativa.

Frente a ello, se propone la aplicación obligatoria de la carga dinámica de la prueba, un régimen de responsabilidad civil objetiva por riesgo creado, la consagración inexcusable de la reserva de humanidad y una regulación técnica basada en niveles de riesgo ante la autoridad de control.

***Palabras Clave:* Carga Dinámica de la Prueba; Inteligencia Artificial; Caja Negra; Reserva de Humanidad; Tutela Judicial Efectiva; Responsabilidad Objetiva; Protección de Datos Personales.**

ABSTRACT

The proliferation of artificial intelligence systems for mass personal data processing poses a severe dilemma for effective judicial protection in Ecuador. Machine learning algorithms operate as "black boxes," creating opaque environments where reconstructing causation or establishing direct human fault under traditional civil law rules becomes virtually impossible. This technical asymmetry creates an insurmountable evidentiary barrier for individuals against corporations under the standard procedural regime of the General Organic Code of Processes (COGEP). Through dogmatic and statutory analysis, this study examines informational self-determination and the right not to be subjected to solely automated decisions under the Organic Law on Personal Data Protection (LOPDP), Resolution SPDP-SPD-2026-0009-R, and comparative legal standards. The findings indicate that ordinary procedural rules fail to address harmful algorithmic outcomes, allowing technological complexity to shield corporate liability. Consequently, this paper proposes the mandatory application of the dynamic burden of proof in judicial proceedings, a strict civil liability framework based on created risk, the mandatory inclusion of the human-in-the-loop safeguard, and risk-based regulatory classifications enforced by the supervisory authority.

Keywords: *Dynamic Burden of Proof; Artificial Intelligence; Black Box; Human-in-the-Loop; Effective Judicial Protection; Strict Liability; Personal Data Protection.*

INTRODUCCIÓN

Este estudio analiza las barreras legales para asegurar el derecho básico de cuidar la información privada de las personas frente a las decisiones tomadas por sistemas automatizados. Evaluamos cómo dejar estas importantes decisiones en manos de sistemas de Inteligencia Artificial (IA) deja a las personas muy desprotegidas ante posibles abusos o injusticias. Esto pasa porque es muy difícil entender cómo toman sus decisiones estos complejos programas informáticos.

La importancia de este trabajo radica en el gran riesgo de que las defensas creadas por la Ley de Protección de Datos no sirvan para nada ante los tribunales. Como resulta casi imposible rastrear paso a paso cómo razona la IA, nuestras normas legales de siempre terminan fallando. Esto pone en claro peligro la defensa real de nuestros derechos tecnológicos, permitiendo que queden sin castigo varios abusos escondidos tras programas complicados o simples secretos de empresa.

La investigación se centrará en el análisis de las garantías procesales de defensa a la ciudadana contra la vulneración de datos procedente de decisiones automatizadas por medio sistemas de IA. Se abordará, de manera concreta, el encuentro jurídico entre el derecho a la motivación o explicación contemplado en la LOPDP y las reglas procesales acerca de la carga de la prueba establecidas en el Código Orgánico General de Procesos (COGEP).

El objetivo fundamental es demostrar cómo la opacidad tecnológica de la IA impide probar la responsabilidad civil por vulneración de datos personales, para consecutivamente estructurar de manera conceptual los mecanismos procesales que exige la tutela de los datos personales con el objeto de equilibrar el desarrollo tecnológico y la defensa de los derechos del titular.

El trabajo se desarrollará mediante un análisis dogmático de la normativa ecuatoriana de protección de datos. Para nutrir esta perspectiva el trabajo analiza las disposiciones de la autoridad de control, apoyándose en la doctrina y la experiencia del derecho comparado en materia de responsabilidad tecnológica. A lo largo de la investigación se demostrará que, frente a los perjuicios ocasionados por resoluciones automatizadas, el problema central no radica en la falta de culpables, sino en las trabas procesales que impiden juzgarlos. Plantear nuevas herramientas procedimentales resulta indispensable; solo así los derechos previstos en la LOPDP tendrán una defensa real y efectiva dentro del sistema de justicia ecuatoriano.

Antecedentes Históricos

El rápido avance de las tecnologías de la información ha transformado profundamente tanto a la sociedad como al derecho. En Ecuador, la protección de los datos personales ha tenido que recorrer un largo camino para intentar alcanzar el ritmo de estos cambios. El primer hito normativo de verdadera importancia en esta materia se dio con la reforma constitucional de 1996, la cual incorporó formalmente la garantía jurisdiccional del hábeas data.

Este mecanismo permitió a los ciudadanos ejercer un nivel inicial de control sobre la información que reposaba en bancos de datos públicos y privados. En esta etapa temprana, el ordenamiento buscaba mitigar los nacientes riesgos digitales, ya que, como afirman Rosas-Lanas y Pila-Cárdenas (2023), las tecnologías de la información y comunicación (TIC) se constituyen como herramientas indispensables para la satisfacción de las necesidades básicas del ser humano (p. 2). Sin embargo, la posterior masificación del internet también multiplicó exponencialmente la vulnerabilidad ciudadana frente al abuso corporativo y estatal, exigiendo marcos más robustos.

El salto cualitativo y el momento histórico en que este derecho adquiere una verdadera relevancia dogmática ocurrió con la promulgación de la norma suprema que rige actualmente al Estado. En el año 2008 por medio del cuerpo constitucional, se reconoció de manera explícita y soberana el derecho fundamental sobre la protección de datos de carácter personal, desvinculándolo definitivamente de la esfera estricta de la privacidad. Se elevó la autodeterminación informativa a la categoría de un bien jurídico superior, estableciendo normativamente que cualquier actividad de recolección o tratamiento requiere la autorización del titular.

En este sentido la Carta Magna consagra taxativamente: El derecho a la protección de datos es de carácter personal, en el cual se incluye el acceso y la decisión sobre información y datos de esta índole, así como su correspondiente protección. De esta manera, se estructuró un escudo formal frente a los poderes públicos y las presiones del mercado. A pesar del rango constitucional otorgado a este derecho, Ecuador se mantuvo en un limbo legislativo durante más de una década. La ausencia de una normativa secundaria que detallara las reglas del juego dejó a los titulares de la información en una clara situación de vulnerabilidad frente a terceros. El legislador se vio obligado a reaccionar y expedir reglas claras como consecuencia directa de uno de los mayores escándalos informáticos a nivel regional.

Aguilar Martínez et al. (2022) detallan la magnitud de esta crisis sistémica de la siguiente manera: Bajo la concepción anteriormente citada, es menester considerar que en el año 2019 de acuerdo con el informe de la empresa israelí VPNMentor especialista en seguridad informática, los datos de 20 millones de ecuatorianos fueron afectados por la violación a los sistemas de seguridad de los equipos de cómputo de la empresa ecuatoriana llamada Novaestrat. (p. 370).

Esta alarmante filtración masiva incluyó historiales laborales e información financiera, evidenciando de manera catastrófica la incapacidad estructural del Estado para tutelar los derechos digitales y exponiendo a millones de ciudadanos a la extorsión y la suplantación de identidad en la red. La abrumadora presión mediática y el legítimo clamor social desatados por esta masiva vulneración intervinieron como ultimátum definitivo con lo que obligó al poder legislativo a acelerar la creación del marco regulatorio.

Como resultado, se expidió la normativa orgánica con el objetivo de sancionar y proteger el ejercicio de la autodeterminación informativa. La Ley Orgánica de Protección de Datos Personales (2021) constituyó de manera detallada el catálogo de principios rectores, en el cual se definió categorías especiales para el tratamiento de datos sensibles e impuso obligaciones precisas de transparencia para los encargados del manejo de la información. De esta forma, el país logró constituir los principios normativos formales necesarios para proteger al ciudadano, en el que se garantiza legalmente sus derechos de acceso, eliminación, rectificación y oposición, en un esfuerzo gubernamental para reducir la asimetría de poder frente a las grandes corporaciones.

De forma paralela a esta consolidación interna, la comunidad global experimentó una transformación impulsada por la vertiginosa irrupción de la inteligencia artificial y de los sistemas de procesamiento masivo conocidos como Big Data. Estos modelos algorítmicos funcionan gracias a una alta capacidad de cómputo que analiza datos personales a gran velocidad, logrando así perfilar y anticipar el comportamiento de las personas. Al delegar resoluciones de impacto en estos sistemas, se evidencia una nueva forma de vulnerabilidad para los titulares de la información. Esto ocurre porque la complejidad técnica del software impide entender cómo llegó a un resultado concreto, operando como un mecanismo de control invisible.

Entender la relación entre derecho y tecnología exige a los juristas un estudio integral, capaz de anticipar los obstáculos probatorios en los juzgados. Aunque la ley reconoce el

derecho a no someterse a resoluciones totalmente automatizadas, la complejidad de este software hace casi imposible probar sus sesgos discriminatorios. Por esto, resulta urgente diseñar nuevas reglas procesales que garanticen una defensa judicial real frente a estos abusos.

Definiciones

La delimitación conceptual de los actores que intervienen en el ciclo de vida de la información es un pilar fundamental para garantizar la seguridad jurídica dentro del derecho tecnológico. Comprender la diferencia y el uso de cada uno de estos roles es de vital importancia, ya que permite atribuir correctamente los niveles de responsabilidad, determinar quién toma las decisiones sobre la información y establecer ante quién debe acudir el ciudadano para el ejercicio de sus derechos (Red Iberoamericana de Protección de Datos, 2019).

En entornos digitales complejos, confundir la figura de quien decide sobre los datos con la de quien simplemente presta un servicio técnico puede derivar en la inaplicabilidad de sanciones y en la vulneración de las garantías procesales.

En el marco de la Ley Orgánica de Protección de Datos Personales (2021), el ecosistema de protección gira en torno a sujetos claramente definidos, cuyas obligaciones varían según su nivel de control sobre la información:

Titular: Es la persona natural cuyos datos son objeto de tratamiento (Ley Orgánica de Protección de Datos Personales, 2021). Es el eje central del sistema y el único titular de los derechos de acceso, rectificación, eliminación y oposición.

Responsable del tratamiento de datos personales: Persona natural o jurídica, pública o privada, autoridad u otro organismo quien, actúa solo o conjuntamente con otros, decide sobre la finalidad y el tratamiento de los datos personales (Ley Orgánica de Protección de Datos Personales, 2021). Su participación es fundamental porque asume la carga principal de rendir cuentas, justificar la legalidad del tratamiento e implementar las medidas de protección desde el diseño.

Encargado del tratamiento de datos personales: Corresponde a la persona natural o jurídica, autoridad u organismo que trata datos personales a nombre y por cuenta exclusiva de un responsable (Ley Orgánica de Protección de Datos Personales, 2021). Su importancia radica en que no decide qué hacer con la información, sino que ejecuta un servicio bajo las instrucciones documentadas del responsable.

Destinatario: Es toda persona natural o jurídica que ha sido comunicada con datos personales, independientemente de si es un tercero o parte de la relación original (Ley Orgánica de Protección de Datos Personales, 2021).

El importante avance de la Inteligencia Artificial ha disipado las tradicionales barreras del tratamiento de datos, obligando a las legislaciones a adoptar un enfoque más detallado sobre la cadena de suministro tecnológico. La Superintendencia de Protección de Datos Personales de Ecuador, mediante su Resolución No. SPDP-SPD-2026-0009-R, concentró nuevas definiciones con la finalidad de identificar a los sujetos que intervienen de manera específica en los sistemas de IA.

Estos nuevos términos encuentran su asidero y equivalencia conceptual en normativas internacionales de vanguardia, como el reciente Reglamento (UE) 2024/1689 (Ley de IA de la Unión Europea), el cual divide las obligaciones a lo largo de toda la cadena de valor de la inteligencia artificial para evitar vacíos de responsabilidad entre quienes programan el código y quienes lo utilizan (Parlamento Europeo y Consejo de la Unión Europea, 2024).

Para comprender el impacto jurídico de estas herramientas y los nuevos roles que surgen de ellas, es indispensable desmitificar la tecnología para el ciudadano común. La Inteligencia Artificial se percibe como un concepto abstracto o futurista; sin embargo, sus aplicaciones actuales y futuras se basan en elementos lógicos concretos que procesan cantidades masivas de datos personales.

Algoritmo: En términos sencillos, un algoritmo no es más que una serie de instrucciones o reglas lógicas definidas paso a paso para resolver un problema o realizar una tarea (Real Academia Española, 2023).

Inteligencia Artificial (IA): En relación con la Organización para la Cooperación y el Desarrollo Económicos (OCDE, 2019), un sistema de IA es un sistema basado en máquinas diseñado con la finalidad de operar con distintos niveles de autonomía y que puede, para un conjunto dado de objetivos definidos por humanos, generar resultados como predicciones, recomendaciones o decisiones que influyen en entornos reales o virtuales. En la práctica actual, esto significa que las máquinas pueden realizar tareas que normalmente requerirían inteligencia humana, como entender el lenguaje, reconocer rostros o aprobar un crédito bancario.

Aprendizaje Automático (Machine Learning): Es la rama más común de la IA en la actualidad. A diferencia de un algoritmo tradicional donde el programador escribe cada regla

exacta, en el aprendizaje automático el sistema aprende por sí mismo analizando miles o millones de datos históricos (Organización Mundial de la Propiedad Intelectual [OMPI], 2019).

Desarrollador: El responsable y encargado acerca del tratamiento de datos personales que genera o crea un sistema de inteligencia artificial (Superintendencia de Protección de Datos Personales, 2026). En el ámbito internacional, este actor guarda relación con la figura del "proveedor", quien asume el deber de entrenar los algoritmos con datos libres de sesgos antes de introducirlos al mercado (Parlamento Europeo y Consejo de la Unión Europea, 2024).

Desplegador: Es el responsable y encargado que, mediante el uso de un sistema de inteligencia artificial, ejecuta la prestación de un servicio, excepto cuando su uso se limite a actividades personales no profesionales (Superintendencia de Protección de Datos Personales, 2026). En el derecho comparado europeo, el "responsable del despliegue" es quien tiene la mejor posición para vigilar el funcionamiento de la máquina en un entorno real y detectar anomalías que el desarrollador no pudo prever (Parlamento Europeo y Consejo de la Unión Europea, 2024).

Distribuidor: Actúa como el responsable y encargado que forma parte de la cadena de suministro, siendo distinto del desarrollador o del desplegador, y cuya función se centra en comercializar o prestar el sistema de IA en el mercado (Superintendencia de Protección de Datos Personales, 2026).

Implementador: Se conceptualiza como el responsable y encargado del tratamiento que encomienda el desarrollo a un tercero o que implementa un sistema de IA específicamente dentro de sus propios procedimientos o procesos internos (Superintendencia de Protección de Datos Personales, 2026).

Naturaleza Jurídica

En el ordenamiento jurídico ecuatoriano, la naturaleza jurídica de las garantías procesales frente al uso de inteligencia artificial se instituye como un derecho fundamental autónomo de carácter eminentemente defensivo. Su estructura se fundamenta en un sistema normativo jerarquizado que relaciona preceptos constitucionales, legales e infralegales con postulados doctrinales contemporáneos.

Esta naturaleza garantista emana directamente del artículo 66, numeral 19, de la Constitución de la República del Ecuador, disposición que consagra el derecho a la protección de datos personales y materializa el principio de autodeterminación informativa. Este fundamento constitucional establece que todo individuo cuenta con el derecho inalienable al acceso, decisión y control sobre su información personal, erigiéndose como el bien jurídico tutelado principal frente a las asimetrías de poder que genera el procesamiento automatizado.

A nivel legislativo este cuerpo constitucional se operativiza a través de la Ley Orgánica de Protección de Datos Personales y su Reglamento General, normativas que transforman la autodeterminación en herramientas de defensa activa. El núcleo de este blindaje procesal se ubica en el artículo 20 de la referida ley, el cual reconoce de manera explícita el derecho del titular a no ser objeto de decisiones basadas, única o parcialmente, en valoraciones automatizadas que produzcan efectos jurídicos en su contra.

Desde la perspectiva doctrinal, esta disposición confirma que la naturaleza jurídica de la protección de datos actúa como el límite indispensable frente a intromisiones algorítmicas ilegítimas (Mendoza, 2021), operando como una barrera estructural frente a la recolección masiva y desproporcionada de información ciudadana en la era digital (Sánchez, 2023).

Para instrumentalizar estas garantías en el complejo ecosistema tecnológico, el ordenamiento ecuatoriano cuenta con la Resolución No. SPDP-SPD-2026-0009-R, emitida por la Superintendencia de Protección de Datos Personales (2026). Esta norma tiene la finalidad de aterrizar los principios de la ley al desarrollo, entrenamiento e implementación de sistemas de inteligencia artificial. Con ello, se busca que lineamientos éticos globales, como la necesidad de una revisión humana significativa recomendada por la Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura (UNESCO, 2021), se traduzcan en exigencias procesales exigibles. Sin embargo, la naturaleza jurídica y la eficacia material de estas garantías se ven severamente limitadas por profundas fallas conceptuales y metodológicas dentro de esta misma resolución.

En primer lugar, la normativa carece de una categorización de riesgos algorítmicos, aplicando el mismo rigor procedimental y prohibitivo a un sistema inofensivo de recomendación musical que a un software invasivo de evaluación crediticia o de filtrado masivo de currículos laborales. Esta falencia desnaturaliza el principio de proporcionalidad, resultando simultáneamente ineficaz para proteger frente a peligros reales y desproporcionada al asfixiar la competitividad empresarial local.

Como segundo punto la resolución presenta un vacío crítico al no establecer directrices técnicas específicas para la gobernanza y el control de calidad de las bases de datos de entrenamiento. Esta ausencia regulatoria permite que los sistemas algorítmicos hereden y perpetúen sesgos humanos bajo una falsa apariencia de neutralidad matemática y estadística.

El documento de la Superintendencia además incurre en graves distorsiones teóricas en la asignación de la responsabilidad legal al subsumir automáticamente la figura del desarrollador dentro de las categorías de responsable o encargado del tratamiento. En el derecho estricto de protección de datos, ambas figuras poseen obligaciones, funciones y niveles de control diametralmente distintos, por lo que fusionarlas de forma automática genera incertidumbre normativa y severas distorsiones en el régimen de responsabilidad civil.

La metodología de evaluación requerida por la resolución fue diseñada conceptualmente para bases de datos estáticas tradicionales, resultando antiguo frente a las redes neuronales y los sistemas de aprendizaje profundo que transforman y generan inferencias predictivas de forma autónoma a partir de datos históricos. Al no exigir auditorías algorítmicas de carácter continuo y limitar el cumplimiento a la simple elaboración estática de matrices de riesgo documentales, la resolución disminuye la verdadera naturaleza jurídica de la garantía procesal.

Aunque el marco legal ecuatoriano tiene una clara orientación garantista, la falta de parámetros matemáticos estandarizados y la incapacidad técnica institucional para fiscalizar el código fuente terminan dejando al ciudadano en un estado de indefensión práctica frente a la opacidad de la inteligencia artificial.

Pregunta de Investigación

¿Cómo La Opacidad De La Inteligencia Artificial Impide Probar La Responsabilidad Por La Vulneración De Datos Personales, Y Qué Soluciones Exige El Derecho Ecuatoriano?

La inteligencia artificial funciona mediante sistemas que aprenden por sí mismos, lo que hace casi imposible rastrear paso a paso cómo procesan la información. Este fenómeno, conocido comúnmente como el efecto de caja negra, provoca que ni siquiera los propios creadores del programa puedan explicar siempre el camino lógico que tomó la máquina para

llegar a un resultado, levantando un muro para cualquier ciudadano que intente descubrir cómo se manejaron sus datos personales (Ferreiro, 2024).

Los sistemas basados en estas nuevas tecnologías necesitan consumir cantidades inmensas de información personal para poder funcionar y aprender correctamente. El cruce constante de estos datos para crear perfiles o predicciones ocurre en un entorno invisible para el usuario, lo que vuelve extremadamente difícil que una persona afectada pueda señalar el momento exacto en el que su privacidad fue vulnerada o su información fue expuesta sin su permiso (Ferreiro, 2024).

Exigir a una víctima que demuestre el error específico de un ser humano, tal como lo pide la ley civil tradicional, es un callejón sin salida cuando el daño proviene de una máquina que actúa de forma autónoma. Intentar aplicar conceptos diseñados para las personas, como la negligencia o la mala intención, a un programa informático es inútil y engañoso, porque rompe la cadena lógica que los jueces exigen normalmente para obligar a alguien a pagar por un daño (Finocchiaro, 2025).

Otorgar derechos o personalidad jurídica a la propia inteligencia artificial para hacerla responsable directa de sus actos solo empeora el problema para el ciudadano afectado. Tratar a un algoritmo como si fuera una persona o una empresa es un invento teórico que enreda más las leyes y deja a la víctima sin una reparación real, ya que los programas informáticos no tienen dinero ni bienes propios con los cuales indemnizar a quienes han perjudicado (Finocchiaro, 2025).

El sistema jurídico debe dejar de buscar a un culpable humano específico dentro del código de programación y avanzar hacia un modelo donde se asuma la responsabilidad simplemente por crear el riesgo. La ley debe asegurar que quien diseña, vende o se beneficia económicamente de la inteligencia artificial sea quien asuma los costos por los daños causados a los datos personales, sin necesidad de que la víctima deba probar que la empresa actuó con mala fe (Finocchiaro, 2025).

Las empresas que manejan información personal mediante estas herramientas deben actuar bajo el principio de responsabilidad proactiva, cambiando las reglas del juego a favor del ciudadano. Este principio exige que la organización que está más cerca del riesgo y que cuenta con la tecnología, sea la que deba demostrar ante un juez que tomó todas las medidas de seguridad posibles para proteger la información, en lugar de obligar a la víctima a descubrir en qué falló la empresa (Finocchiaro, 2025).

La figura de la carga dinámica de la prueba se convierte en la herramienta procesal ideal en el derecho ecuatoriano para equilibrar esta gran desigualdad tecnológica. Al trasladar la obligación de presentar las pruebas hacia la empresa que controla la inteligencia artificial, el derecho libera al ciudadano afectado de la tarea imposible de descifrar un algoritmo complejo para poder defender su derecho a la protección de datos (Finocchiario, 2025).

Exigir reglas claras de transparencia es fundamental para evitar que las personas queden sometidas a decisiones arbitrarias tomadas por máquinas. La ley debe de tener como objeto a obligar a que los datos usados para enseñar a la inteligencia artificial puedan ser rastreados y revisados por personas externas, con la finalidad de garantizar que el ciudadano afectado reciba una explicación y motivación de forma clara, sencilla y oportuna sobre cómo su información íntima fue procesada y evaluada.

Adaptar el derecho a estas nuevas realidades informáticas exige aplicar principios básicos de justicia, como la proporcionalidad, para lograr que la tecnología avance sin aplastar los derechos ciudadanos. Dejar las decisiones en manos de las computadoras nunca puede servir como excusa para que las corporaciones evadan su obligación de dar la cara, explicar sus acciones y reparar económicamente los daños causados a la privacidad de las personas (Rivero Ortega, 2023).

El Rol De La Superintendencia De Protección De Datos Personales Frente A Los Fallos Algorítmicos

La Superintendencia de Protección de Datos Personales asume un papel protagónico como el principal escudo institucional frente a los abusos derivados de la opacidad algorítmica. La creación y el fortalecimiento de esta agencia estatal especializada resulta esencial para vigilar y sancionar los excesos de los programas informáticos en la sociedad, nivelando la balanza de poder entre los ciudadanos y las empresas tecnológicas que controlan el procesamiento masivo de la información (Rivero Ortega, 2023).

Auditar un sistema informático de alta complejidad exige que la autoridad de control desarrolle capacidades que superan el simple conocimiento legal. El Estado requiere incorporar peritos, ingenieros y especialistas en datos que puedan descifrar cómo las máquinas evalúan a los usuarios, garantizando una supervisión continua que venza el efecto de caja negra inherente a las redes neuronales y a los algoritmos de aprendizaje automático (Ferreiro Baamonde, 2024).

La actuación de la Superintendencia debe enfocarse en exigir que detrás de cada decisión automatizada de alto riesgo exista siempre un ser humano capaz de asumir la responsabilidad por los errores cometidos. El control de las decisiones corporativas basadas en inteligencia artificial obliga a establecer una reserva de humanidad, impidiendo que las máquinas realicen juicios que afecten la vida de las personas sin supervisión, ya que esto violaría el derecho ciudadano a una buena administración digital y a recibir una motivación comprensible (Ponce Solé, 2024).

Garantizar el derecho de las personas a recibir una explicación clara depende directamente de la firmeza con la que actúe esta institución reguladora. La intervención de los poderes públicos resulta vital para asegurar que el diseño de las herramientas tecnológicas sea compatible con los derechos fundamentales, obligando a las compañías a utilizar un lenguaje sencillo para justificar las decisiones de sus algoritmos ante los individuos que han sufrido la vulneración de sus datos (Trejo Medina, 2025).

El control centralizado en una única Superintendencia evita que las empresas tecnológicas aprovechen la fragmentación de las leyes para eludir sus responsabilidades civiles. La inteligencia artificial es una tecnología transversal, lo que hace indispensable que un único sujeto estatal coordine eficazmente a todos los actores para liderar una estrategia de supervisión coherente (Finocchiaro, 2025).

La fiscalización preventiva se erige como la herramienta principal de la autoridad para evitar vulneraciones masivas de datos personales antes de que ocurran en el entorno digital. Las compañías deben estar forzadas a presentar evaluaciones de impacto y auditorías algorítmicas ante la Superintendencia antes de lanzar sus programas al mercado, demostrando anticipadamente que sus sistemas son seguros, transparentes y libres de sesgos discriminatorios que afecten a la población (Ponce Solé, 2024).

El poder sancionador de la institución asegura que las corporaciones tomen en serio la protección de la privacidad frente al avance informático. La Superintendencia tiene la facultad de revisar por dentro los sistemas de inteligencia artificial, ordenar la corrección inmediata de los fallos técnicos y aplicar multas severas a quienes no cumplan las reglas básicas de protección y manejo de datos personales (Trejo Medina, 2025).

El equilibrio entre la innovación tecnológica y el respeto a la intimidad se logra únicamente mediante la actuación de un árbitro estatal fuerte y preparado. El papel del derecho y de sus instituciones es buscar puntos de armonía que faciliten la convivencia social frente a

las transformaciones digitales, exigiendo que las empresas asuman la carga dinámica de demostrar su diligencia en la protección de datos en lugar de dejar al usuario en la total indefensión probatoria (Rivero Ortega, 2023).

La Imputación Corporativa Por Inobservancia De La Reserva De Humanidad

Las corporaciones mercantiles y las grandes empresas tecnológicas se posicionan como los actores hegemónicos en el diseño y la utilización de sistemas de inteligencia artificial para el tratamiento masivo de datos personales. El manejo de volúmenes exponenciales de información, fenómeno conocido como big data, exige capacidades de procesamiento computacional y de almacenamiento que resultan técnica y financieramente inalcanzables para las personas naturales en su cotidianidad (Barrio Andrés, 2022).

La concentración del procesamiento de datos en manos de entidades societarias genera un marcado desequilibrio de poder frente a los ciudadanos, incrementando significativamente el riesgo de vulneraciones a la privacidad. El sector privado asume un estándar de responsabilidad civil extraordinariamente riguroso al implementar modelos matemáticos que perfilan, predicen y condicionan el comportamiento humano con fines netamente lucrativos (Corvalán, 2021).

El principio de reserva de humanidad, conceptualizado en la ingeniería informática como human in the loop, se constituye como una barrera jurídica irrenunciable frente a la automatización absoluta de las decisiones empresariales. El derecho fundamental a la protección de datos exige que una persona física mantenga siempre la capacidad real, efectiva e indelegable de supervisar, auditar y revocar cualquier resolución algorítmica que afecte la esfera jurídica de un individuo (Llano Alonso, 2021).

La prudencia, la empatía, el análisis ético y la interpretación del contexto social son atributos intrínsecos de la inteligencia humana que los algoritmos de aprendizaje automático no logran codificar ni reproducir de forma efectiva. Las redes neuronales trabajan por medio de cálculos probabilísticos y patrones estadísticos de naturaleza abstracta que carecen de la capacidad moral para poder ponderar el impacto real de sus predicciones en la vida e incluso en la honra de las personas (Barrio Andrés, 2022).

La inobservancia de esta supervisión humana genera la imputación directa e inmediata de responsabilidad civil al patrimonio de la compañía que despliega la herramienta tecnológica. Delegar el control absoluto de una decisión a un software implica una abdicación deliberada

de la diligencia corporativa, configurando un escenario donde la empresa debe responder de forma objetiva por los daños originados frente a los titulares de la información (Corvalán, 2021).

La carga dinámica de la prueba asume un papel estructurante en la resolución de esta asimetría informativa dentro de la dogmática procesal ecuatoriana, obligando a la corporación a demostrar activamente la intervención del factor humano en sus procesos. El Código Orgánico General de Procesos proporciona la vía adjetiva idónea para exigir que la empresa exhiba las trazas de auditoría y los registros internos que evidencien un análisis humano crítico y posterior sobre la recomendación del algoritmo (Llano Alonso, 2021).

La complejidad técnica y la opacidad inherente a los sistemas algorítmicos no constituyen eximentes válidas para que las corporaciones diluyan sus responsabilidades. El juzgador tiene la potestad de levantar el velo tecnológico para identificar la falla organizativa de la empresa, sancionando la ausencia de mecanismos de gobernanza internos que permitan auditar la actuación del código fuente (Barrio Andrés, 2022).

La responsabilidad proactiva corporativa obliga a las sociedades mercantiles a diseñar desde su origen arquitecturas informáticas que respeten los derechos ciudadanos por defecto y desde el diseño. El cumplimiento estricto de esta obligación impone que los directorios y los oficiales de cumplimiento asuman la carga reparatoria por los sesgos, la discriminación y los errores en el tratamiento de los datos personales que sus sistemas puedan cometer (Corvalán, 2021).

CONCLUSIONES

El volumen de información que se genera en la actualidad hace indispensable recurrir a la inteligencia artificial para poder procesar y gestionar datos a gran escala. Sin embargo, la dependencia hacia estas herramientas tecnológicas trae consigo riesgos profundos para la privacidad ciudadana. Al delegar el tratamiento de nuestra información a sistemas automatizados estos terminan elaborando perfiles que con frecuencia resultan discriminatorios. Esta situación de desventaja tecnológica coloca a distintos grupos de personas en un estado de alta vulnerabilidad frente a la exposición no consentida de su vida privada dejando expuestos detalles íntimos que escapan por completo a su control.

La manera en la que los sistemas algorítmicos aprenden y operan por su cuenta produce un bloqueo informativo que impide por completo seguir la ruta lógica de sus decisiones. Esta

oscuridad técnica vuelve inútil los mecanismos tradicionales del derecho civil que exigen a la víctima comprobar el error humano directo o la negligencia. Tratar de identificar a un culpable individual bajo estas reglas clásicas resulta una tarea materialmente imposible en los juzgados. El ciudadano afectado se enfrenta a una barrera probatoria insalvable al no poder explicar ante un juez cómo la máquina procesó su información o en qué momento exacto ocurrió la falla que causó el daño.

Las grandes empresas son los actores que más utilizan y se benefician del procesamiento masivo de datos mediante algoritmos lo que genera una enorme desigualdad de poder frente a las personas comunes. Al dejar el control total de las operaciones en manos del software sin mantener una vigilancia humana constante las corporaciones incrementan las probabilidades de cometer actos perjudiciales. Esta falta de supervisión real por parte de las compañías sobre las máquinas que ellas mismas implementan y controlan es la principal causa de las vulneraciones a la privacidad. La autonomía de la tecnología funciona en la práctica como un escudo que permite a las empresas distanciarse de los daños ocasionados por sus propios sistemas informáticos.

RECOMENDACIONES

Para solucionar la indefensión del ciudadano frente a la opacidad algorítmica, los operadores de justicia deben aplicar de manera estricta la carga dinámica de la prueba establecida en la legislación procesal ecuatoriana. Esta medida obliga a las empresas tecnológicas a demostrar que sus sistemas funcionaron correctamente y que adoptaron todas las medidas de seguridad necesarias, liberando a la víctima de una exigencia técnica que le resulta imposible de cumplir. Esta obligación debe complementarse con la exigencia de que las compañías realicen y presenten auditorías preventivas que certifiquen la transparencia de sus programas antes de lanzarlos al mercado.

Se debe reformar de manera urgente la resolución emitida por la Superintendencia de Protección de Datos Personales, ya que actualmente presenta errores de fondo que debilitan la defensa ciudadana. La normativa vigente confunde a las personas al mezclar los roles de quienes crean el programa informático con los roles de quienes lo utilizan en el día a día, además de no poseer de una verdadera categorización de riesgos. Es indispensable redactar y definir criterios claros que distingan entre herramientas inofensivas contra sistemas invasivos, para que la autoridad de control tenga un marco real y efectivo al momento de auditar, vigilar y sancionar a las empresas infractoras.

El derecho ecuatoriano debe establecer un modelo de responsabilidad objetiva y directa para las corporaciones, fundamentado en la exigencia ineludible de la reserva de humanidad. La legislación debe prohibir que los sistemas automatizados tomen decisiones importantes de forma solitaria, imponiendo la obligación de mantener siempre una supervisión humana real y significativa que actúe como último filtro. Si una empresa decide delegar el control total a la máquina y esta causa una discriminación o vulneración de datos, la compañía debe responder automáticamente con su patrimonio, evitando que utilicen la complejidad tecnológica como excusa para evadir a la justicia.

REFERENCIAS.

- Aguilar, M., Paredes, J., Gordillo, D., y León, G. (2022). La protección de datos personales en Ecuador. *Estudios del Desarrollo Social: Cuba y América Latina*, 10(Especial 1), 369-382.
- Asamblea Constituyente del Ecuador. (2008). Constitución de la República del Ecuador. Registro Oficial Suplemento 449 de 20 de octubre de 2008.
- Asamblea Nacional del Ecuador. (2021). Ley Orgánica de Protección de Datos Personales. Registro Oficial Suplemento 459 de 26 de mayo de 2021.
- Barrio Andrés, M. (2022). *Manual de Derecho Digital*. Tirant lo Blanch.
- Corvalán, J. G. (2021). *Tratado de Inteligencia Artificial y Derecho*. Thomson Reuters La Ley.
- Ferreiro, X. (2024). La utilización de herramientas de inteligencia artificial en el proceso penal bajo el prisma de la propuesta de reglamento de inteligencia artificial.
- Finocchiaro, G. (2025). *El nuevo derecho de la Inteligencia Artificial* (M. Chumberiza Tupac Yupanqui y H. Rojas Sinche, Trans.). Palestra Europa.
- Llano Alonso, F. H. (2021). *Inteligencia artificial y filosofía del derecho*. Laborum.
- Mendoza, O. (2021). El derecho de protección de datos personales en los sistemas de inteligencia artificial. *Revista IUS*, 15(48).
- Naranjo, L. (2017). El dato personal como presupuesto del derecho a la protección de datos personales y hábeas data en Ecuador. *Foro. Revista de Derecho*, (27), 63-82.
- Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura [UNESCO]. (2021). *Recomendación sobre la ética de la inteligencia artificial*. UNESCO.

Organización Mundial de la Propiedad Intelectual. (2019). Technology Trends 2019: Artificial Intelligence. WIPO.

Organización para la Cooperación y el Desarrollo Económico. (2019). Recommendation of the Council on Artificial Intelligence. OECD Legal Instruments. <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449>

Parlamento Europeo y Consejo de la Unión Europea. (2024). Reglamento (UE) 2024/1689 por el que se establecen normas armonizadas en materia de inteligencia artificial. Diario Oficial de la Unión Europea L 2024/1689. <http://data.europa.eu/eli/reg/2024/1689/oj>

Ponce Solé, J. (2024). El Reglamento de Inteligencia Artificial de la Unión Europea de 2024, el derecho a una buena administración digital y su control judicial en España. Marcial Pons.

Real Academia Española. (2023). Algoritmo. En Diccionario de la lengua española (23.^a ed., actualización 2023). Recuperado de <https://dle.rae.es/algoritmo>

Red Iberoamericana de Protección de Datos. (2019). Recomendaciones Generales para el Tratamiento de Datos en la Inteligencia Artificial. RIPD.

Rivero Ortega, R. (2023). Derecho e Inteligencia Artificial: Cuatro estudios. Ediciones Olejnik.

Rosas-Lanas, G., y Pila-Cárdenas, G. (2023). La protección de datos personales en Ecuador: Una revisión histórica-normativa de este derecho fundamental en el país suramericano. Visual Review, 10(4568), 2-16. <https://doi.org/10.37467/revvisual.v10.4568>

Sánchez, M. (2023). El derecho a la protección de datos personales en la era digital. Revista Euro latinoamericana De Derecho Administrativo, 10(1), e235.

Superintendencia de Protección de Datos Personales. (2026). Resolución No. SPDP-

SPD-2026-0009-R: Norma general para la garantía del derecho de protección de datos personales en el uso de sistemas de inteligencia artificial.

Trejo Medina, D. (2025). Inteligencia Artificial. Fundamentos para abogados y estudiantes de Derecho. Tirant lo Blanch.

DECLARACIÓN Y AUTORIZACIÓN

Nosotros, **Pinargote Mendoza, María José**; con C.C.: 0915874254; **Villegas Melgarejo, Carlos José**, con C.C: # 0927292862; autores del trabajo de titulación: **Garantías procesales para la protección de datos personales frente a tecnologías automatizadas** previo a la obtención del título de **ABOGADO** en la Universidad Católica de Santiago de Guayaquil.

1.- Declaramos tener pleno conocimiento de la obligación que tienen las instituciones de educación superior, de conformidad con el Artículo 144 de la Ley Orgánica de Educación Superior, de entregar a la SENESCYT en formato digital una copia del referido trabajo de titulación para que sea integrado al Sistema Nacional de Información de la Educación Superior del Ecuador para su difusión pública respetando los derechos de autor.

2.- Autorizamos a la SENESCYT a tener una copia del referido trabajo de titulación, con el propósito de generar un repositorio que democratice la información, respetando las políticas de propiedad intelectual vigentes.

Guayaquil, 25 de agosto 2026

f. 

Pinargote Mendoza, María José

C.C: 0915874254

f. 

Villegas Melgarejo, Carlos José

C.C: 0927292862

REPOSITORIO NACIONAL EN CIENCIA Y TECNOLOGÍA

FICHA DE REGISTRO DE TESIS/TRABAJO DE TITULACIÓN

TEMA Y SUBTEMA:	Garantías Procesales Para La Protección De Datos Personales Frente A Tecnologías Automatizadas		
AUTOR(ES)	Villegas Melgarejo, Carlos José; Pinargote Mendoza, María José		
REVISOR(ES)/TUTOR(ES)	Ab. Mendoza Colamarco Elker Pavlova, Mgts		
INSTITUCIÓN:	Universidad Católica de Santiago de Guayaquil		
FACULTAD:	Facultad de Jurisprudencia, Ciencias Sociales y Políticas		
CARRERA:	Carrera de Derecho		
TITULO OBTENIDO:	Abogado		
FECHA DE PUBLICACIÓN:	25 de agosto de 2026	No. DE PÁGINAS:	(17 de páginas)
ÁREAS TEMÁTICAS:	Datos Personales – Derecho Procesal – Derecho Administrativo		
PALABRAS CLAVES/ KEYWORDS:	<i>Carga Dinámica de la Prueba; Caja Negra; Reserva de Humanidad; Responsabilidad Objetiva; Protección de Datos Personales.</i>		

RESUMEN/ABSTRACT:

La proliferación de sistemas de inteligencia artificial para el tratamiento masivo de datos personales desafía la tutela judicial efectiva en Ecuador. La opacidad de la «caja negra» impide reconstruir el nexo causal o probar la culpa bajo las reglas clásicas del derecho civil, generando una barrera probatoria insuperable frente a las corporaciones en el COGEP. Mediante un análisis dogmático y normativo de la LOPDP y la Resolución SPDP-SPD-2026-0009-R, se concluye la ineficacia del régimen ordinario ante decisiones automatizadas lesivas. Se propone implementar la carga dinámica de la prueba, la responsabilidad civil objetiva por riesgo creado, la reserva obligatoria de humanidad y una regulación técnica basada en la clasificación de riesgos ante la autoridad de control. SI N

ADJUNTO PDF:	☒	☐
CONTACTO CON AUTOR/ES:	Teléfono: 0967185575; 0980464516	E-mail: maria.pinargote01@cu.ucsg.edu.ec ; carlos.villegas02@cu.ucsg.edu.ec
CONTACTO CON LA INSTITUCIÓN (COORDINADOR DEL PROCESO UTE):	Nombre: Reynoso Gaute, Maritza Ginette	
	Teléfono: +593-4-3804600	
	E-mail: maritza.reynoso@cu.ucsg.edu.ec	

SECCIÓN PARA USO DE BIBLIOTECA

Nº. DE REGISTRO (en base a datos):	
Nº. DE CLASIFICACIÓN:	
DIRECCIÓN URL (tesis en la web):	