

Tipo de artículo: Artículo original

# Habeas data en era digital, propuestas para fortalecimiento en el marco de protección de datos personales

## *Habeas data in the digital era, proposals to strengthen the personal data protection framework*

Homero Abel Ramírez Cabrera <sup>1\*</sup> , <https://orcid.org/0009-0009-8847-4211>

Andrés Fernando Ramírez Cabrera <sup>2</sup> , <https://orcid.org/0000-0002-0405-7894>

Angélica Viviana Rivas Alvarado <sup>3</sup> , <https://orcid.org/0009-0009-0064-6796>

Andris Nathalye Jama Coello <sup>4</sup> , <https://orcid.org/0009-0002-8967-0475>

María Elisa Cadena Meza <sup>5</sup> , <https://orcid.org/0009-0008-2764-2771>

<sup>1</sup> Universidad de Guayaquil. Ecuador. Correo electrónico: [homero.ramirezca@ug.edu.ec](mailto:homero.ramirezca@ug.edu.ec)

<sup>2</sup> Universidad Laica Eloy Alfaro de Manabí (ULEAM). Ecuador. Correo electrónico: [andres.ramirez@uleam.edu.ec](mailto:andres.ramirez@uleam.edu.ec)

<sup>3</sup> Universidad Metropolitana del Ecuador (UMET). Ecuador. Correo electrónico: [arivas@umet.edu.ec](mailto:arivas@umet.edu.ec)

<sup>4</sup> Estudio jurídico Andris Jama. Ecuador. Correo electrónico: [abg.andrisjama@hotmail.com](mailto:abg.andrisjama@hotmail.com)

<sup>5</sup> Dirección provincial del Consejo de la Judicatura Guayas. Ecuador. Correo electrónico: [maria.cadena@funcionjudicial.gob.ec](mailto:maria.cadena@funcionjudicial.gob.ec)

\* Autor para correspondencia: [homero.ramirezca@ug.edu.ec](mailto:homero.ramirezca@ug.edu.ec)

### Resumen

El concepto de habeas data, derivado como tener datos, representa en la actualidad un área importante en la sociedad del conocimiento. La presente investigación realizó un estudio sobre el impacto de la inteligencia artificial (IA) en el ámbito de la justicia, particularmente en el manejo de Habeas Corpus. Se evidenció que la implementación de IA provocó una revolución cultural, transformando tanto las actitudes de los profesionales del derecho como las estructuras y métodos de investigación. El análisis reveló mejoras significativas en la eficiencia y eficacia de los procesos judiciales, permitiendo una toma de decisiones más rápida. No obstante, se identificaron barreras importantes, como la resistencia al cambio y el temor a que la IA reemplazara empleos en el sector legal. A pesar de estas preocupaciones, los expertos encuestados coincidieron en que la IA no solo genera empleos de alto valor, sino que también actúa como una herramienta fundamental para potenciar la capacidad y la eficiencia de los legalistas comprometidos con su implementación. Se planteó una propuestas para fortalecer el marco de protección de datos personales, evidenciando que, si bien la transición a la digitalización conlleva desafíos, sus beneficios eran indiscutibles para modernizar y optimizar el sistema judicial.

**Palabras clave:** Habeas data; era digital; fortalecimiento; protección de datos personales.

### Abstract

*The concept of habeas data, derived as having data, currently represents an important area in the knowledge society. The present research carried out a study on the impact of artificial intelligence (AI) in the field of justice, particularly in the handling of Habeas Corpus. It was evident that the implementation of AI caused a cultural revolution, transforming both the attitudes of legal professionals and the structures and methods of investigation. The analysis revealed significant improvements in the efficiency and effectiveness of judicial processes, allowing for faster decision-making. However, important barriers were identified, such as resistance to change and fear that AI would replace jobs in the legal sector. Despite these concerns, the experts surveyed agreed that AI not only generates high-value jobs, but also acts as a fundamental tool to enhance the capacity and efficiency of legal*



Esta obra está bajo una licencia *Creative Commons* de tipo Atribución 4.0 Internacional (CC BY 4.0)

*experts committed to its implementation. A proposal was put forward to strengthen the framework for the protection of personal data, showing that, although the transition to digitalisation entails challenges, its benefits were indisputable for modernising and optimising the judicial system.*

**Keywords:** *Habeas data; digital era; strengthening; protection of personal data.*

**Recibido:** 18/05/2024  
**Aceptado:** 04/07/2024  
**En línea:** 01/08/2024

## Introducción

En la era digital, la protección de los datos personales ha emergido como uno de los desafíos significativos para los sistemas jurídicos contemporáneos (Čerka et al., 2017). La globalización de la información, facilitada por el uso extensivo de internet y las tecnologías digitales, ha transformado radicalmente la manera en que se recopilan, almacena, procesan y distribuyen los datos. En este contexto, el habeas data, un mecanismo legal que permite a los individuos acceder, rectificar y eliminar sus datos personales, adquiere una relevancia inédita y se enfrenta a retos y desafíos que requieren un análisis profundo y propuestas concretas para su fortalecimiento (Chen et al., 2022).

El concepto de habeas data, derivado del latín que significa "tener datos", tiene sus raíces en la necesidad de proteger la privacidad y la integridad de los datos personales. Originalmente concebido como una herramienta para contrarrestar el abuso de poder por parte del Estado y garantizar los derechos fundamentales, el habeas data se ha expandido para abarcar también la protección contra las empresas privadas que gestionan grandes volúmenes de información personal (Dal Pont et al., 2021). En muchos países, el derecho al habeas data está consagrado en la legislación, proporcionando a los ciudadanos un medio legal para controlar el uso de sus datos personales. Sin embargo, la rápida evolución tecnológica ha superado muchas veces la capacidad de estas normativas para adaptarse y responder adecuadamente.

La era digital ha traído consigo una serie de transformaciones que han multiplicado las oportunidades para el acceso y uso de los datos personales, pero también ha incrementado los riesgos asociados a la privacidad. Tecnologías emergentes como la inteligencia artificial, el big data y las redes sociales han revolucionado el manejo de la información, permitiendo análisis complejos y detallados de los datos personales (Miraut Martín, 2021). Estas tecnologías ofrecen beneficios significativos, como la personalización de servicios y la mejora de la eficiencia operativa, pero también plantean serias amenazas a la privacidad, incluyendo la vigilancia masiva, el perfilado de individuos y la potencial discriminación algorítmica (Chenou & Valenzuela, 2021).

En este contexto, el habeas data enfrenta múltiples desafíos. Primero, la naturaleza misma de los datos ha cambiado. Ya no se trata solo de información almacenada en archivos físicos, sino de datos digitales que pueden ser copiados,



transferidos y procesados con una facilidad y rapidez sin precedentes. Este cambio requiere una revisión de las normativas existentes para garantizar que sigan siendo efectivas en la protección de la privacidad (Gstrein & Beaulieu, 2022).

Segundo, la globalización de la información ha complicado la jurisdicción de las leyes de protección de datos. Los datos personales pueden ser almacenados en servidores ubicados en diferentes partes del mundo, lo que plantea preguntas sobre la aplicabilidad y el alcance de las leyes nacionales de habeas data. Este desafío se ve exacerbado por la falta de armonización internacional en materia de protección de datos, lo que puede llevar a lagunas legales y a la imposibilidad de hacer cumplir los derechos de los ciudadanos de manera efectiva (Vergari & Preite, 2023).

Tercero, la opacidad y complejidad de las tecnologías utilizadas para procesar los datos personales dificultan la transparencia y la rendición de cuentas. Muchos usuarios no comprenden plenamente cómo se recopilan y utilizan sus datos, lo que limita su capacidad para ejercer sus derechos bajo el habeas data. Las empresas tecnológicas, por su parte, a menudo utilizan términos y condiciones complejos que desincentivan la lectura y comprensión por parte de los usuarios, creando un desequilibrio de poder que favorece a los gestores de datos sobre los titulares de los mismos (Maestri, 2021).

En respuesta a estos desafíos, es esencial fortalecer el mecanismo de habeas data para asegurar una protección robusta y efectiva de los datos personales en la era digital. Esto requiere una serie de acciones y propuestas que aborden las debilidades actuales y adapten el marco legal a las nuevas realidades tecnológicas.

Se hace necesario actualizar las normativas existentes para incluir disposiciones específicas sobre la protección de datos digitales. Esto incluye la definición clara de términos y responsabilidades, así como la incorporación de principios de privacidad por diseño y por defecto, que obliguen a las empresas a considerar la privacidad de los usuarios desde el inicio de sus procesos de desarrollo tecnológico (Basterra, 2022).

Es impostergable promover la cooperación internacional y la armonización de las leyes de protección de datos. Esto puede lograrse a través de acuerdos bilaterales y multilaterales que establezcan estándares comunes y mecanismos de cooperación para la protección de datos transfronterizos. La adopción de marcos regulatorios como el Reglamento General de Protección de Datos (GDPR) de la Unión Europea puede servir como modelo para otros países, ofreciendo un enfoque coherente y riguroso a nivel global.

Es crucial mejorar la transparencia y la educación en materia de protección de datos. Las empresas deben ser obligadas a proporcionar información clara y accesible sobre el uso de los datos personales, y los usuarios deben ser empoderados



a través de campañas educativas que aumenten su comprensión y capacidad para ejercer sus derechos. La implementación de herramientas tecnológicas que faciliten el acceso y control de los datos por parte de los usuarios puede contribuir significativamente a la efectividad del habeas data.

Reforzar los mecanismos de supervisión y cumplimiento constituye una actividad estratégica para el estado el cual debe priorizar políticas que generen seguridad y confianza en el manejo de los datos, esto incluye la creación de autoridades de protección de datos con suficientes recursos y poderes para investigar y sancionar violaciones a los derechos de los ciudadanos, así como el establecimiento de procedimientos judiciales accesibles y eficientes para la defensa de estos derechos.

El habeas data en la era digital enfrenta retos y desafíos significativos que requieren una respuesta integral y adaptativa. Fortalecer este mecanismo es esencial para garantizar la protección de los datos personales y la privacidad de los individuos en un entorno digitalizado y complejo. Las propuestas para su fortalecimiento deben ser amplias y multidimensionales, abarcando desde la actualización de las normativas y la cooperación internacional hasta la mejora de la transparencia, la educación y los mecanismos de supervisión y cumplimiento. Solo así se podrá asegurar una protección efectiva de los datos personales en la era digital, salvaguardando los derechos fundamentales de los ciudadanos frente a los nuevos desafíos tecnológicos.

## **Materiales y métodos**

El enfoque de la investigación fue mixto, que combinó métodos cualitativos y cuantitativos para obtener una comprensión integral de los retos y desafíos del habeas data en la era digital y para proponer estrategias efectivas de fortalecimiento. Se utilizó un alcance exploratorio y descriptivo. Exploratorio, que buscó identificar y analizar nuevas problemáticas y desafíos emergentes en el campo del habeas data en el contexto digital. Descriptivo, porque propicio caracterizar y detallar las actuales prácticas, normativas y percepciones sobre la protección de datos personales. El diseño de investigación fue no experimental, ya que se observarán y analizarán fenómenos sin manipular variables. Además, será transversal, puesto que se recogerán datos en un momento específico en el tiempo.

El Método de Nivel Empírico empleado fue el Análisis Documental: Se analizaron documentos legales, políticas de privacidad, informes de agencias de protección de datos y estudios previos relacionados.

Métodos de Nivel Teórico



**Análisis Jurídico:** Se llevó a cabo un análisis detallado de las normativas nacionales e internacionales relacionadas con el habeas data y la protección de datos personales; **Revisión de Literatura:** Se revisó la literatura académica relevante para contextualizar los hallazgos empíricos y proporcionar un marco teórico sólido para la discusión; **Análisis de derecho Comparado:** Se confrontaron las legislaciones y prácticas de diferentes países para identificar buenas prácticas y áreas de mejora.

#### Métodos para el Procesamiento de Datos

**Análisis Estadístico:** Los datos cuantitativos recolectados a través de encuestas serán analizados utilizando técnicas estadísticas descriptivas e inferenciales para identificar tendencias y patrones; **Análisis Cualitativo:** Las entrevistas en profundidad y los datos de análisis documental serán codificados y analizados utilizando técnicas de análisis temático para identificar categorías y subcategorías relevantes; **Software de Análisis:** Se utilizarán herramientas de software como SPSS para el análisis estadístico y NVivo para el análisis cualitativo.

#### Técnicas e Instrumentos

**Cuestionarios:** Se diseñarán cuestionarios estructurados para las encuestas, que incluirán preguntas cerradas y abiertas para capturar una amplia gama de información. **Guías de Entrevista:** Se desarrollarán guías de entrevista semiestructuradas para orientar las entrevistas en profundidad con expertos. **Matrices de Análisis Documental:** Se utilizarán matrices para organizar y sistematizar la información obtenida a través del análisis documental.

El diagnóstico por criterio de expertos se llevó a cabo a través de un comité conformado por profesionales con experiencia en gestión de la información y derecho. Los diagnosticaron según sus 6 criterios distribuidos en tres dimensiones tal como muestra la tabla 1. Se realiza la evaluación mediante una escala Likert de 5 categorías (1-nada pertinente:5-muy pertinente).

**Tabla 1.** Dimensiones y criterios de para diagnosticar impacto del habeas data en era digital por los expertos.

<b>Dimensión</b>	<b>Criterios de evaluación</b>	<b>Descripción</b>
<b>Dimensión Legal</b>	Cumplimiento Normativo	Evaluar si las legislaciones actuales sobre protección de datos personales y habeas data son adecuadas y se están cumpliendo efectivamente.
	Eficacia Judicial	Analizar la efectividad y eficiencia de los mecanismos judiciales y administrativos disponibles para la protección de datos personales.
<b>Dimensión Tecnológica</b>	Seguridad de la Información	Examinar las medidas de seguridad adoptadas para proteger los datos personales de accesos no autorizados y vulnerabilidades tecnológicas.



	Adaptabilidad a Tecnologías Emergentes	Evaluar la capacidad de las leyes y regulaciones para adaptarse a nuevas tecnologías y prácticas digitales, como la inteligencia artificial y el big data.
<b>Dimensión Social</b>	Conciencia y Educación Ciudadana	Medir el nivel de conocimiento y conciencia de los ciudadanos sobre sus derechos de protección de datos y habeas data.
	Instituciones	Confiar en las Instituciones Evaluar el grado de confianza de la sociedad en las instituciones encargadas de la protección de datos personales y la percepción sobre la efectividad del habeas data en salvaguardar sus derechos.

Esta investigación exploró los retos y desafíos del habeas data en Ecuador, en el contexto de la era digital, con el objetivo de proponer estrategias para fortalecer la protección de datos personales. A través de un enfoque mixto, se analizaron las normativas actuales, la implementación de tecnologías emergentes y las percepciones de los ciudadanos y expertos. Se utilizaron encuestas, entrevistas en profundidad y análisis documental para identificar brechas y áreas de mejora. Los hallazgos permitirán formular recomendaciones para mejorar la eficacia del habeas data, asegurando una protección robusta y adaptativa de los datos personales en Ecuador.

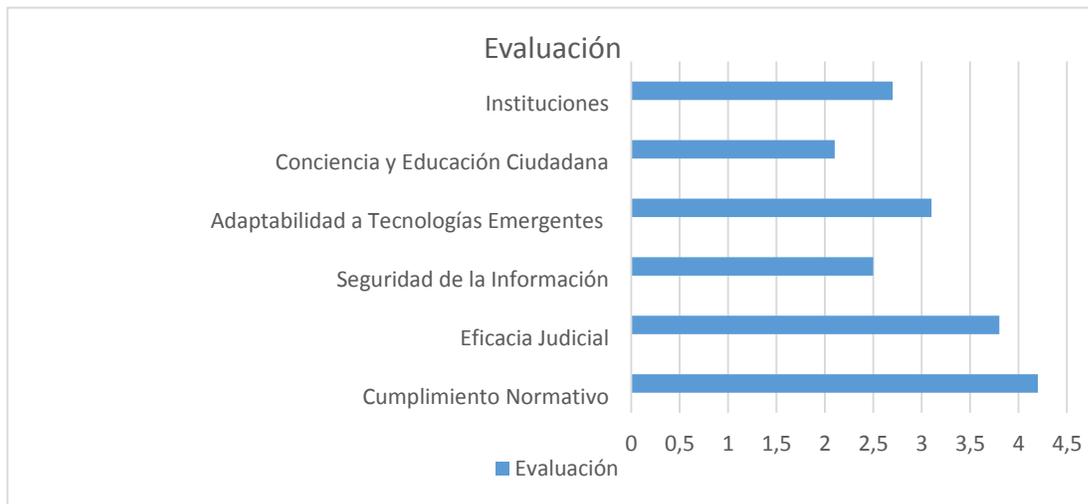
## Resultados y discusión

### Diagnóstico mediante criterio de experto sobre del impacto del habeas data en era digital

Durante el proceso de diagnóstico, los expertos resaltaron diversos aspectos cualitativos sobre el impacto del habeas data en era digital en la actualidad ecuatoriana. La figura 1, presentan los resultados de la evaluación cuantitativa promedio por parte de los expertos, evaluados en las tres dimensiones y sus respectivos criterios.

El diagnóstico sobre el impacto del habeas data en la era digital, realizado como parte de la investigación titulada "Habeas data en la era digital: propuestas para el fortalecimiento en el marco de protección de datos personales", evidenció una serie de hallazgos significativos a través de una evaluación mediante una escala Likert de 5 categorías. Los expertos otorgaron una alta puntuación al cumplimiento normativo con una evaluación de 4.5, indicando que las leyes y regulaciones existentes eran en gran medida pertinentes y adecuadas para abordar la protección de datos personales. Asimismo, la eficacia judicial recibió una evaluación de 3.8, sugiriendo que los mecanismos judiciales y administrativos eran razonablemente efectivos, aunque aún podían mejorarse para garantizar una protección más robusta.





**Figura 1.** Resultados del diagnóstico mediante criterio de experto sobre del impacto del habeas data en era digital.

La evaluación resaltó varias áreas críticas con puntuaciones más bajas. La seguridad de la información obtuvo una evaluación de 2.5, lo que reflejaba una preocupación significativa por las vulnerabilidades tecnológicas y la necesidad de implementar medidas de seguridad más estrictas. La adaptabilidad a tecnologías emergentes fue evaluada con un 3.1, indicando que las leyes actuales no estaban completamente preparadas para enfrentar los desafíos planteados por las nuevas tecnologías. Además, la conciencia y educación ciudadana recibió una baja puntuación de 2.1, destacando una falta de conocimiento y conciencia entre los ciudadanos sobre sus derechos de protección de datos. Por último, la confianza en las instituciones fue evaluada con un 2.7, subrayando la necesidad de fortalecer las capacidades institucionales y aumentar la confianza pública en la protección de datos personales. Estos resultados subrayan la importancia de adoptar medidas integrales para fortalecer el marco de protección de datos personales en la era digital.

### **Propuestas para el fortalecimiento en el marco de protección de datos personales**

Una nueva entidad, la persona digital, ha hecho su aparición en el ecosistema digital como resultado de la reconfiguración del concepto clásico de persona. La privacidad se está erosionando progresivamente debido a la creciente aquiescencia, apatía y despreocupación de las personas, así como a su apoyo explícito a medidas que se presentan como necesarias e inofensivas (Maestri, 2021).

Aunque todavía es prematuro afirmar que la privacidad está casi muerta, las nuevas generaciones, les guste o no, desempeñan un papel protagonista en una praxis cultural y en una socialización primaria alejadas del concepto de privacidad. En este apartado se analizan propuestas efectivas de gobernanza, diseñadas para defender a los ciudadanos



como personas digitales, así como sus derechos a la dignidad, al Habeas Data y a la privacidad de sus datos personales. En la figura 2 se muestran las principales propuestas del marco de protección de datos personales.



**Figura 2.** Propuestas del marco de protección de datos personales.

**Fuente:** Elaboración propia.

Las propuestas representadas en la figura 1 constituyen un robusto marco que no solo enfatiza la importancia de proteger los datos personales, sino que también promueve un entorno de respeto y dignidad en el uso de la información en la sociedad actual.

- Educación digital obligatoria: Implementar programas educativos en escuelas y universidades que enseñen a los estudiantes sobre la importancia de la protección de datos, sus derechos y cómo gestionar su información personal en el entorno digital.
- Consentimiento informado: Establecer directrices más estrictas que garanticen que el consentimiento para el tratamiento de datos personales sea claro, específico, y dado a través de un proceso comprensible. Esto incluiría el uso de lenguaje sencillo y ejemplos prácticos.
- Transparencia en el tratamiento de datos: Obligar a las empresas a publicar informes anuales sobre cómo manejan los datos, incluyendo qué datos se recogen, con qué propósito y cómo se protegen. Esto fomentaría la rendición de cuentas.
- Mecanismos de denuncia: Crear plataformas y líneas directas donde los individuos puedan denunciar violaciones de sus derechos de protección de datos de manera anónima y segura, así como recibir asistencia legal.



- Promoción de la privacidad por diseño: Alentar a las empresas a incorporar principios de protección de datos desde el diseño de sus productos y servicios, asegurando que la privacidad sea un factor central en todas las etapas de desarrollo.
- Colaboraciones internacionales: Fomentar acuerdos internacionales que promuevan la interoperabilidad de normativas de protección de datos, de manera que se facilite la transmisión segura de datos entre países, respetando la privacidad de los individuos.
- Legislación clarificada: Desarrollar leyes claras y específicas que definan el alcance y los derechos relacionados con el habeas data, asegurando que todos los ciudadanos comprendan sus derechos y cómo ejercerlos.
- Protección contra represiones: Implementar mecanismos de protección contra represalias para aquellos que ejercen su derecho de habeas data, garantizando que no enfrenten consecuencias negativas por solicitar el acceso o la corrección de sus datos.
- Mecanismos de revisión judicial: Establecer mecanismos judiciales para que los ciudadanos puedan apelar las decisiones relacionadas con sus solicitudes de habeas data, garantizando un proceso justo y accesible.
- Protección de datos sensibles: Reforzar las medidas de protección para datos sensibles, asegurando que los ciudadanos tengan un acceso especial y derechos adicionales sobre la información que podría afectar su privacidad o dignidad.
- Colaboraciones institucionales: Fomentar la colaboración entre entidades gubernamentales, organizaciones no gubernamentales y sector privado para desarrollar mejores prácticas, políticas y recursos que respalden el ejercicio efectivo del habeas data.

El fortalecimiento de la protección de datos personales es una necesidad imperante en la era digital actual, donde la recolección y procesamiento de información personal son constantes. Para lograr un avance significativo, es fundamental establecer una legislación clara que defina los derechos de los ciudadanos respecto a sus datos y el mecanismo de habeas data. Estas leyes deben ser accesibles y entendibles para todos, asegurando que los derechos de los individuos sean plenamente reconocidos y respetados.

La educación y concientización son pilares esenciales en este marco. Una ciudadanía bien informada sobre sus derechos en materia de protección de datos es menos vulnerable a abusos. Por ello, se deben implementar campañas masivas que permitan a los ciudadanos entender fácilmente sus derechos y el correcto ejercicio del habeas data, facilitando el acceso y la corrección de sus datos personales. Complementando estas iniciativas, es crucial establecer plazos de respuesta riguroso para las solicitudes, lo que garantizará que los ciudadanos no enfrenten demoras innecesarias al ejercer sus derechos.



Además, la transparencia es un elemento clave para fortalecer la confianza en el sistema. Mantener un registro público de las solicitudes de habeas data con estadísticas sobre respuestas y razones de rechazo no solo fomentará la rendición de cuentas de las entidades, sino también el interés de los ciudadanos en estas cuestiones. Asimismo, es importante establecer mecanismos de protección que salvaguarden a quienes ejercen sus derechos, previniendo cualquier forma de represalia.

El entrenamiento de oficiales de protección de datos dentro de las organizaciones es otra estrategia valiosa. Con personal capacitado y responsable del manejo de las solicitudes de habeas data, las instituciones pueden desarrollar una cultura robusta de protección de datos, alineada con las mejores prácticas y regulaciones vigentes. Además, debe existir la posibilidad de apelaciones ante decisiones adversas, brindando a los ciudadanos un camino claro hacia la justicia en caso de disputas.

Asimismo, la creación de coaliciones entre el sector público, privado y organizaciones no gubernamentales permitirá un enfoque colaborativo en la implementación de políticas de protección de datos. Este esfuerzo conjunto puede resultar en la creación de mecanismos efectivos y recursos adicionales, asegurando que la privacidad y la protección de datos personales se conviertan en una prioridad social.

## Discusiones

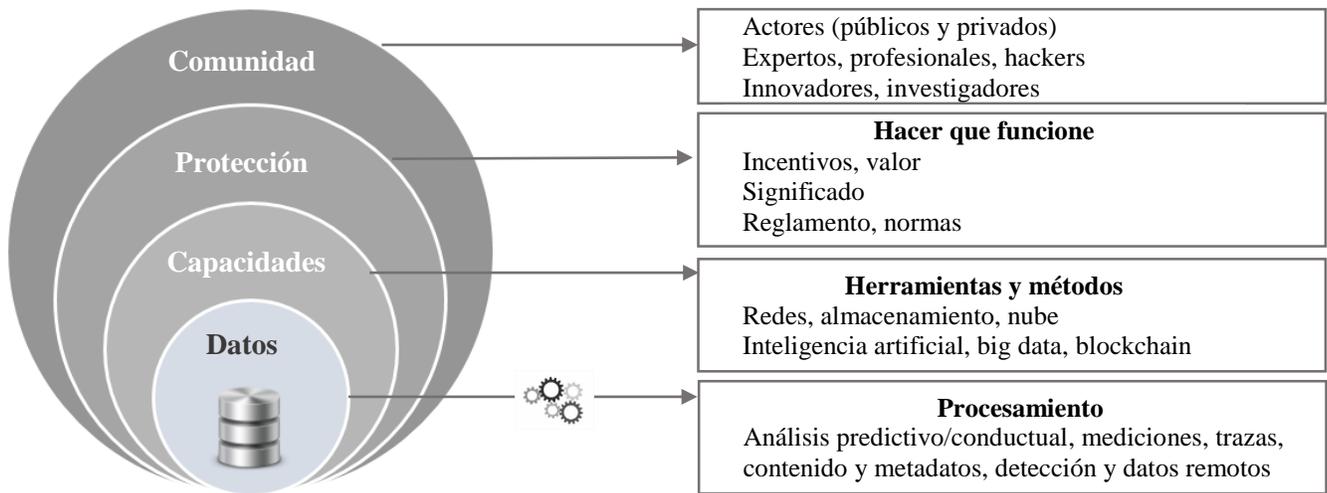
La privacidad no debe entenderse como un concepto aislado, sino más bien como una representación de la relación entre el individuo y la sociedad. Pocos conceptos relacionados con la privacidad y el control de los flujos de información lo demuestran tan claramente como el habeas data, ya que su surgimiento está estrechamente ligado a la historia política de los países de América Latina.

El Habeas Data exige que las autoridades públicas proporcionen todos los datos personales relacionados con un determinado caso o acusación para garantizar que una persona conozca el fundamento de las acusaciones que enfrenta. Este requisito de total transparencia debería permitir al individuo comprender la situación, corregir declaraciones falsas y rectificar datos. Sin embargo, las dimensiones e implementaciones del concepto difieren entre los once países latinoamericanos que lo tienen consagrado en sus constituciones.

En tiempos de uso cada vez mayor de la inteligencia artificial, el aprendizaje automático, el *Big Data* y la toma de decisiones automatizadas, se podría especular si una interpretación progresista centrada en la primacía de la regulación podría transformar el Habeas Data en una respuesta a la amenaza de una "sociedad de caja negra", donde los motivos o datos reales de las decisiones que afectan a los individuos son difícilmente recuperables. Por el contrario, si uno se cree que la inteligencia artificial y el aprendizaje automático explicables no son realistas y que los beneficios de los rápidos



avances tecnológicos superan las posibles preocupaciones en torno a la confiabilidad, tal interpretación del Habeas Data se entendería como equivocada y poco realista. Como tal, una transformación del concepto de Habeas Data potencialmente atraviesa las cuatro capas del modelo de datificación presentado en la figura 3, como un principio totalmente integral.



**Figura 3.** Capas de la datificación.

**Fuente.** Adaptado de (Gstrein & Beaulieu, 2022).

En este sentido, los beneficios de una mayor interconexión se ven limitados por el riesgo de intrusión en la esfera humana (social, personal o privada), que podría suponer una amenaza tanto para el cuerpo físico, biológico, con sus libertades asociadas (Habeas Corpus), como para el cuerpo digital, en sus múltiples formas y representaciones mediáticas (Habeas Data) (Vergari & Preite, 2023).

### Trabajos relacionados

El análisis exhaustivo de cómo la digitalización y la integración de tecnologías avanzadas influenciaban la forma en que se gestionaban las solicitudes de Habeas Corpus. La revisión de documentos normativos, llevó a cabo un estudio que ilustra la aplicación de la IA en la justicia, destacando sus beneficios y desafíos.

Además, se identificaron las actitudes de los actores involucrados en el sistema judicial hacia la implementación de la IA. Se observó que, aunque muchos reconocían las ventajas de la tecnología en términos de eficiencia y rapidez en la toma de decisiones, también existía una considerable resistencia al cambio. Las preocupaciones sobre la posible pérdida de empleos en el sector legal y la desconfianza hacia las máquinas para manejar decisiones tan delicadas fueron temas



recurrentes en las entrevistas realizadas. Los participantes expresaron la necesidad de un enfoque equilibrado que integrara la IA con la supervisión humana para garantizar un uso ético y responsable de la tecnología.

Los resultados obtenidos permiten constatar la novedad y relevancia del tema objeto de estudio. La tabla 2 muestra un resumen de los principales resultados científicos relacionados.

Los resultados obtenidos permitieron elaborar propuestas concretas para el fortalecimiento del marco de protección de datos personales en el contexto digital. Se sugirió la elaboración de directrices claras para regular la aplicación de la IA en el Habeas Corpus, priorizando la transparencia y la rendición de cuentas. Asimismo, se recomendó la capacitación continua de los profesionales del derecho en herramientas digitales y éticas relacionadas con el manejo de datos personales. Se destacó que, a pesar de las barreras existentes, la implementación adecuada de la IA podría enriquecer y modernizar el sistema de justicia, reduciendo los tiempos de respuesta y mejorando la protección de los derechos de los ciudadanos.

**Tabla 2.** Resumen de resultados científicos relacionados.

No	Fuente	Resultado
1	(Muñoz, 2024)	Protección de datos personales en el contexto electoral: análisis de la legislación ecuatoriana
2	(Ordóñez Pineda & Quezada, 2022)	Políticas públicas y protección de datos personales en Ecuador: reflexiones desde la emergencia sanitaria
3	(Rosas-Lanas & Pila-Cárdenas, 2023)	La protección de datos personales en Ecuador: Una revisión histórica-normativa de este derecho fundamental en el país suramericano
4	(Pineda & Ortega, 2023)	El derecho a la educación digital: una oportunidad para afianzar un modelo de cultura digital para la paz

La investigación "Protección de datos personales en el contexto electoral: análisis de la legislación ecuatoriana" propuesta en (Muñoz, 2024). Realiza un análisis crítico de cómo la legislación ecuatoriana protegía los datos personales en el contexto electoral. Se enfocó en la Ley Orgánica de Protección de Datos Personales y la Ley Orgánica Electoral y de Organizaciones Políticas de la República del Ecuador, Código de la Democracia, examinando su impacto en la gestión de datos durante campañas y procesos electorales. Se abordó la aplicación de principios de protección de datos, como la minimización y el consentimiento, y cómo estos afectaban la confianza del electorado y las estrategias de campaña. Además, se realizaron comparaciones con regulaciones internacionales, identificando desafíos y oportunidades para mejorar la transparencia e integridad de los procesos electorales, concluyendo con recomendaciones para fortalecer la democracia en Ecuador.

Para (Ordóñez Pineda & Quezada, 2022) en su investigación "Políticas públicas y protección de datos personales en Ecuador: reflexiones desde la emergencia sanitaria". Evidenció la necesidad de fortalecer la tutela del derecho fundamental de protección de datos personales mediante la formulación y ejecución de políticas públicas en Ecuador.



Para ello, en el contexto nacional, se analizó la política pública "Por una internet segura para niños, niñas y adolescentes" y se estudiaron tres sentencias de la Corte Constitucional al respecto. El estudio consideró importante fortalecer instancias de garantía de protección de datos y subrayar la existencia de información sensible, cuyo tratamiento incidía en el ejercicio de los derechos de las personas afectadas por la emergencia sanitaria. Frente a las intromisiones ilegítimas en la intimidad de las personas, se concluyó que las políticas públicas fortalecían y coadyuvaban a generar programas de prevención y concienciación para el respeto del derecho a la protección de datos personales en Ecuador, similar a lo que acontecía en otros países de la región.

Otro estudio como el propuesto por (Rosas-Lanas & Pila-Cárdenas, 2023) en su investigación "La protección de datos personales en Ecuador: Una revisión histórica-normativa de este derecho fundamental en el país suramericano". Revisó históricamente el proceso de reconocimiento del derecho fundamental a la protección de datos personales en Ecuador hasta la promulgación de la Ley Orgánica de Protección de Datos Personales en 2021. Las TIC se presentaron como herramientas indispensables para la satisfacción de las necesidades básicas del ser humano, aunque la era digital también planteaba múltiples desafíos y riesgos para los ciudadanos. Utilizando una técnica exploratoria y un enfoque descriptivo, el estudio concluyó que el reconocimiento constitucional de este derecho en Ecuador es reciente.

En la investigación: "El derecho a la educación digital: una oportunidad para afianzar un modelo de cultura digital para la paz" propuesta en (Pineda & Ortega, 2023), abordó la necesidad de enfrentar las amenazas que las tecnologías de la información y comunicación pueden ocasionar en los derechos de las personas, conforme a la doctrina y la jurisprudencia. A pesar de que los ordenamientos jurídicos suelen quedarse atrás del desarrollo tecnológico, se destacó la importancia de buscar escenarios que permitan el respeto de las libertades fundamentales, enmarcados en el principio de corresponsabilidad.

Desde la perspectiva del derecho a la protección de datos personales, los objetivos de la investigación se centraron en identificar las oportunidades que ofrece el derecho a la educación digital para consolidar un modelo de cultura digital para la paz, promoviendo el uso responsable de las tecnologías emergentes. A través de una metodología descriptiva, casuística y holística, se enfocaron diversas perspectivas, especialmente en entornos digitales donde la intimidad y la reputación de la niñez y la adolescencia pueden verse comprometidas. El principal resultado enfatizó la importancia de desarrollar el derecho a la educación digital en los menores, tomando como referencia modelos de la Unión Europea y de la Comunidad Andina. Se concluyó que un modelo adecuado de cultura digital es aquel que, mediante el aprendizaje y la formación, construye espacios de paz, competencias y habilidades que promuevan los derechos digitales, rechazando cualquier tipo de violencia.



Las tecnologías en el campo de la automatización de procesos robóticos, la inteligencia artificial y la gestión de casos judiciales están transformando la operacionalización y el control de los procedimientos judiciales, así como la Gestión de Recursos Humanos. Esto se hace mediante la automatización de procesos tediosos y monótonos, lo que se traduce en la producción, evaluación por parte de expertos judiciales, almacenamiento y consulta permanente, haciendo que los procesos judiciales sean más efectivos y altamente productivos, liberando recursos humanos para realizar un trabajo mucho más relevante que involucra organización, planificación y control.

Esto se hace mediante la automatización de procesos tediosos y monótonos, lo que se traduce en la producción, evaluación por parte de expertos judiciales, almacenamiento y consulta permanente, haciendo que los procesos judiciales sean más efectivos y altamente productivos, liberando recursos humanos para realizar un trabajo mucho más relevante que involucra organización, planificación y control.

## Conclusiones

La implementación de IA en Justicia provoca una revolución cultural en las personas, infraestructuras, métodos y metodología de investigación, procesos (eficiencia y eficacia, medios tecnológicos y plazos), tecnologías, toma de decisiones (más rápida), actitudes y percepción de los problemas, productividad. Entre las principales barreras, se encuentra el aumento del nivel de resistencia al cambio y la preocupación de que la IA quitará ocupaciones de recursos humanos, sin embargo, los expertos encuestados coinciden en que la IA genera empleos de alto valor y constituye una herramienta para aumentar la capacidad y la eficiencia de los profesionales de las ciencias jurídicas que apuestan por su implementación dentro del análisis de Habeas Corpus. Sin embargo, estos resultados subrayan la importancia de adoptar medidas integrales para fortalecer el marco de protección de datos personales en la era digital.

## Conflictos de intereses

Los autores no poseen conflictos de intereses.

## Contribución de los autores

1. Conceptualización: Homero Abel Ramírez Cabrera, Andrés Fernando Ramírez Cabrera, Angélica Viviana Rivas Alvarado, Andris Nathalye Jama Coello, María Elisa Cadena Meza.
2. Curación de datos: Homero Abel Ramírez Cabrera, Andrés Fernando Ramírez Cabrera, Angélica Viviana Rivas Alvarado, Andris Nathalye Jama Coello, María Elisa Cadena Meza.



3. Análisis formal: Homero Abel Ramírez Cabrera, Andrés Fernando Ramírez Cabrera.
4. Investigación: Angélica Viviana Rivas Alvarado, Andris Nathalye Jama Coello.
5. Metodología: Andris Nathalye Jama Coello, María Elisa Cadena Meza.
6. Software: Andrés Fernando Ramírez Cabrera, Angélica Viviana Rivas Alvarado.
7. Supervisión: Homero Abel Ramírez Cabrera.
8. Validación: Andrés Fernando Ramírez Cabrera, Angélica Viviana Rivas Alvarado,
9. Visualización: Andris Nathalye Jama Coello, María Elisa Cadena Meza.
10. Redacción – borrador original: Homero Abel Ramírez Cabrera, Andrés Fernando Ramírez Cabrera, Angélica Viviana Rivas Alvarado, Andris Nathalye Jama Coello, María Elisa Cadena Meza.
11. Redacción – revisión y edición: Homero Abel Ramírez Cabrera, Andrés Fernando Ramírez Cabrera, Angélica Viviana Rivas Alvarado, Andris Nathalye Jama Coello, María Elisa Cadena Meza.

## Financiamiento

La investigación no requirió fuente de financiamiento externa.

## Referencias

- Basterra, M. (2022). Hacia una reforma del proceso de protección de datos personales. *Capítulo VI-El Futuro de la Protección de los Datos Personales” en Falke, Ignacio (dir.) Hábeas Data. Estudios en homenaje al Prof. Mario Masciotra, IJ Editores*. <https://marcelabasterra.com.ar/wp-content/uploads/2022/11/Hacia-una-reforma-del-sistema-de-proteccio%CC%81n-de-datos-personales.-Marcela-I.-Basterra.pdf>
- Čerka, P., Grigienė, J., & Širbikytė, G. (2017). Is it possible to grant legal personality to artificial intelligence software systems? *Computer Law & Security Review*, 33(5), 685-699. <https://www.sciencedirect.com/science/article/pii/S0267364916301777>
- Chen, H., Wu, L., Chen, J., Lu, W., & Ding, J. (2022). A comparative study of automated legal text classification using random forests and deep learning. *Information processing & management*, 59(2), 102798. <https://www.sciencedirect.com/science/article/pii/S0306457321002764>
- Chenou, J.-M., & Valenzuela, L. E. R. (2021). Habeas data, habemus algorithms: Algorithmic intervention in public interest decision-making in Colombia. *Law, State and Telecommunications Review*, 13(2), 56-77. <https://periodicos.unb.br/index.php/RDET/article/view/34113>



- Dal Pont, T. R., Sabo, I. C., Wilton, P. E. V., de Menezes, V. A., Copetti, R., Zambrota, L., Martins, P. P., Costa, E. C., Schnitzler, E. L., & Santos, P. M. (2021). Classification and association rules in Brazilian supreme court judgments on pre-trial detention. *International Conference on Electronic Government and the Information Systems Perspective*,
- Gstrein, O. J., & Beaulieu, A. (2022). How to protect privacy in a datafied society? A presentation of multiple legal and conceptual approaches. *Philosophy & Technology*, 35(1), 3. <https://link.springer.com/article/10.1007/s13347-022-00497-4>
- Maestri, E. (2021). Surveillance And Profiling. Online Person's Privacy Between Criminogenic Structures And Legal Paternalism. *Journal of Ethics and Legal Technologies*, 3(2), 55-78. <https://sfera.unife.it/handle/11392/2471663>
- Miraut Martín, L. (2021). New realities, new rights: some reflections on the need to safeguard personal data. *Artificial intelligence and human rights*, 24-47. <https://www.torrossa.com/gs/resourceProxy?an=5109959&publisher=FZ1825>
- Muñoz, D. E. (2024). Protección de datos personales en el contexto electoral: análisis de la legislación ecuatoriana. *Revista Especializada Justicia Electoral y Democracia*, 7(8), 119-155. <http://revista.tce.gob.ec/ojs-3.1.2-4/index.php/revista/article/download/135/175>
- Ordóñez Pineda, L., & Quezada, C. (2022). Políticas públicas y protección de datos personales en Ecuador: reflexiones desde la emergencia sanitaria. *Estado & comunes, revista de políticas y problemas públicos*, 2(15), 77-97. <http://scielo.senescyt.gob.ec/pdf/ecomunes/v2n15/2477-9245-ecomunes-2-15-00077.pdf>
- Pineda, L. O. O., & Ortega, G. J. V. (2023). El derecho a la educación digital: una oportunidad para afianzar un modelo de cultura digital para la paz. *Revista de Cultura de paz*, 7, 123-140. <https://revistadeculturadepaz.com/index.php/culturapaz/article/download/143/134>
- Rosas-Lanas, G., & 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. International Visual Culture Review/Revista Internacional de Cultura Visual*, 13(2), 1-16. <https://visualcompuplications.es/revVISUAL/article/download/4568/2897>



Vergari, U., & Preite, G. (2023). The Ethical Dimension of Artificial Intelligence: Biometric Identity and Human Behaviour. *HUMANA. MENTE Journal of Philosophical Studies*, 16(44), 139-162.  
<https://www.humanamente.eu/index.php/HM/article/view/432>



Esta obra está bajo una licencia *Creative Commons* de tipo **Atribución 4.0 Internacional** (CC BY 4.0)