

<https://doi.org/10.69639/arandu.v11i2.525>

Alcance del Hábeas Data: Protección Jurídica en la Era Digital en Ecuador

Scope of Habeas Data: Legal Protection in the Digital Era in Ecuador

Harold Isaac Agama Apolo

hagama@indoamerica.edu.ec

haroldagama@gmail.com

<https://orcid.org/0009-0007-7095-4618>

Universidad Tecnológica Indoamérica

Facultad de Jurisprudencia Ciencias Sociales

Políticas y Económicas Carrera de Derecho

Latacunga – Ecuador

Jorge Mateo Villacrés López

<https://orcid.org/0000-0001-8915-3377>

Universidad Tecnológica Indoamérica

Latacunga – Ecuador

Artículo recibido: 20 octubre 2024

- Aceptado para publicación: 26 noviembre 2024

Conflictos de intereses: Ninguno que declarar

RESUMEN

En la actual era digital y tecnológica, la salvaguardia de datos personales es crucial con el fin de garantizar los derechos individuales. Este artículo analiza el Hábeas Data en la legislación ecuatoriana, considerando sus alcances y obstáculos frente a los avances tecnológicos. Para ello, se emplean métodos jurisprudenciales, doctrinarios y de legislación comparada. El análisis jurisprudencial examina las decisiones judiciales ecuatorianas sobre Hábeas Data, mientras que el enfoque doctrinario evalúa las opiniones de expertos en la materia. La comparación con legislaciones de otros países proporciona una perspectiva sobre enfoques globales en protección de datos. Aunque la Ley Orgánica de Protección de Datos Personales de 2021 busca salvaguardar la información personal, presenta limitaciones que afectan su efectividad. Los avances tecnológicos amplían el alcance de la protección de datos, impactando la privacidad y cuestionando la eficacia del Hábeas Data ante la vigilancia y el uso indebido de datos. Para enfrentar estos desafíos, se proponen programas de sensibilización y capacitación, buenas prácticas en la aplicación del Hábeas Data y cooperación internacional para adoptar estándares globales. En la creciente digitalización de la sociedad ecuatoriana, el Hábeas Data es fundamental para proteger los derechos individuales.

Palabras clave: hábeas data, avance tecnológico, efectividad, privacidad, cooperación internacional

ABSTRACT

In the current digital and technological era, the safeguarding of personal data is crucial in order to guarantee individual rights. This article analyzes Habeas Data in Ecuadorian legislation, considering its scope and obstacles in the face of technological advances. For this purpose, jurisprudential, doctrinal and comparative legislation methods are used. The jurisprudential analysis examines Ecuadorian judicial decisions on Habeas Data, while the doctrinal approach evaluates the opinions of experts in the field. Comparison with legislation from other countries provides a perspective on global approaches to data protection. Although the Organic Law on Personal Data Protection of 2021 seeks to safeguard personal information, it has limitations that affect its effectiveness. Technological advances expand the scope of data protection, impacting privacy and challenging the effectiveness of Habeas Data in the face of surveillance and data misuse. To address these challenges, awareness and training programs, best practices in the application of Habeas Data and international cooperation to adopt global standards are proposed. In the growing digitalization of Ecuadorian society, Habeas Data is essential to protect individual rights.

Keywords: habeas data, technological progress, effectiveness, privacy, international cooperation

INTRODUCCIÓN

El derecho de Hábeas Data, establecido constitucionalmente, garantiza a los ciudadanos la facultad de transigir, reemplazar, corregir y eliminar sus datos personales que han sido almacenados en bases o registros de carácter público o privado. Este derecho protege la autodeterminación informativa y la privacidad, permitiendo a los individuos mantener el control sobre sus datos personales y corregir cualquier información incorrecta o injusta que les afecte.

Hoy en día, en la era digital, la tecnología permea cada faceta de nuestra existencia, y la salvaguarda de la información personal constituye el fundamento esencial para el cuidado y prevalencia de los derechos individuales de los seres humanos. Este estudio profundiza dentro del complejo marco legal y social que rodea al Hábeas Data en Ecuador, explorando sus fundamentos legales y los desafíos que enfrenta en esta era tecnológica. Como Montaña Pinto & Porras Velasco (2011) expresan, es "una respuesta a las nuevas posibilidades de archivo, difusión y acceso a la información que facilita la exposición pública de datos personales y las consecuencias que eso puede tener en las personas y en sus intereses patrimoniales". (p. 178).

El ordenamiento jurídico ecuatoriano incluye el derecho de este recurso en la Ley Orgánica de Protección de Datos Personales y la Constitución de la República. Estas disposiciones establecen un marco jurídico que asegura que los individuos mantengan el control sobre su información personal y la confidencialidad de la misma. No obstante, resulta imprescindible evaluar cómo se implementan estas normativas en la práctica y su efectividad en el contexto de la era digital.

A pesar de los avances legislativos, el Hábeas Data sigue limitado en su capacidad para proteger los datos personales en la era digital. Los rápidos avances tecnológicos han ampliado el alcance de la protección de datos, pero también han revelado nuevas vulnerabilidades y desafíos. La aplicación efectiva de la legislación y la protección de datos como mecanismo de defensa contra prácticas de vigilancia y uso indebido de datos requiere un análisis en profundidad.

En Ecuador, el uso del Hábeas Data está protegido por procedimientos legales y garantías procesales que garantizan el derecho de los ciudadanos a controlar su información personal. Para Pérez Ordóñez (2001), el objeto del habeas data es:

Evitar que, por medio de uso incorrecto de la información, en la forma que ésta se encuentre, se pueda lesionar la intimidad y otros derechos de las personas como consecuencia de la difusión de datos erróneos, incompletos o inexactos con referencia a ellas o a sus bienes. (p. 133).

Según lo mencionado por el autor y en el marco del contexto de Ecuador, el Hábeas Data trasciende la simple prevención del mal uso de la información. Se configura como un pilar esencial para la defensa del derecho a la privacidad, el honor y la libertad individual ante el creciente volumen de datos personales en el mundo digital. La Ley Orgánica de Protección de

Datos Personales proporciona el marco jurídico necesario para la aplicación del Hábeas Data en el país. Dicha ley asegura a los ciudadanos el derecho de acceder a su información personal, conocer cómo se utiliza, corregir, actualizar, eliminar o restringir su uso, especialmente en casos donde los datos sean erróneos, incompletos o recabados de manera ilegítima.

Sin embargo, es crucial probar la eficacia de estos procedimientos y salvaguardias en la práctica. ¿Están disponibles para todos los ciudadanos? ¿Ofrecen protección suficiente contra posibles abusos por parte de organismos públicos y privados? Estas son algunas de las preguntas de investigación clave que este estudio pretende abordar.

Para abordar estos retos, es crucial implementar programas de capacitación y sensibilización que incrementen el conocimiento sobre la relevancia de la salvaguardia de información personal y fomenten prácticas adecuadas en su manejo. Incluir la protección de datos desde las primeras etapas educativas es fundamental para fomentar una cultura de resguardo de información personal en Ecuador. Además, la colaboración internacional y la adopción de normativas internacionales son fundamentales para robustecer el sistema legal ecuatoriano en lo que concierne a la protección de información privada. La coordinación con organizaciones internacionales puede proporcionar orientación y apoyo para implementar las mejores prácticas y alinear la legislación nacional con los estándares internacionales en esta área.

Este artículo tiene como objetivo analizar la configuración actual del Hábeas Data en el ordenamiento jurídico ecuatoriano, identificar las limitaciones en la protección de derechos individuales ante los avances tecnológicos y proponer un marco legal ampliado que salvaguarde desde la intimidad personal hasta la soberanía nacional, adaptándose a las complejidades de la sociedad digital moderna.

DESARROLLO

Fundamentos Jurídicos Del Hábeas Data En Ecuador

En este subtema, se analizarán en profundidad los fundamentos jurídicos del Hábeas Data en Ecuador, comenzando por una identificación y análisis de las leyes nacionales que lo respaldan. Posteriormente, se realizará una comparación exhaustiva de esta legislación con normativas internacionales relevantes, como el Reglamento General de Protección de Datos (GDPR) de la Unión Europea, para resaltar diferencias y similitudes en diferentes párrafos, profundizando en cada idea y aportando un amplio contenido. Finalmente, se examinarán casos específicos de la jurisprudencia ecuatoriana relacionados con el Hábeas Data para entender cómo se ha interpretado y aplicado este derecho en el país.

El Hábeas Data se origina en el ámbito del derecho comparado y responde a la creciente preocupación por la protección de la información personal en el contexto de la digitalización. En su estudio para la Revista Lex, Alejandro Suárez Cadena explica que esta figura legal comenzó a tomar forma en Europa durante la segunda mitad del siglo XX, principalmente como una

herramienta para controlar la recolección y difusión de datos. Suárez Cadena (2021) observa que la evolución del Hábeas Data estuvo fuertemente influenciada por la necesidad de regular el tratamiento de la información personal ante el avance tecnológico, con países como Alemania y Francia liderando la implementación de leyes para proteger la privacidad y los datos desde la década de 1970. Estos desarrollos europeos fueron fundamentales para que América Latina, incluido Ecuador, adoptara y adaptara el Hábeas Data en sus legislaciones.

Marco Normativo Nacional

En Ecuador, se ha establecido un sistema completo compuesto por normativas, leyes, decretos, reglamentos y otros mandatos legales que gobiernan el funcionamiento del Estado, las interacciones entre los ciudadanos y las entidades estatales, así como los derechos y obligaciones de las personas dentro de la sociedad. Este conjunto de disposiciones está formulado en la Constitución de la República, que actúa como cuerpo legal máximo y orienta la formulación y ejecución de todas las demás leyes y regulaciones.

Constitución de la República

El derecho estudiado, incorporado explícitamente en el artículo 92 de la Constitución de la República del Ecuador, proporciona un recurso constitucional que concede a los individuos mantener el control acerca de sus datos personales almacenados en archivos o bancos de datos, tanto públicos como privados. Este derecho es esencial para la protección de la privacidad y la intimidad en la era tecnológica, en la que, la gestión y almacenamiento de datos personales son prácticas comunes.

Dicho artículo garantiza que cada persona pueda conocer y acceder a cualquier documento o dato personal relacionado con ella o sus bienes, que esté almacenado en entidades tanto públicas como privadas, y esto independientemente de si la información se guarda en formato físico o digital. Este constitucionalismo abarca no solo el ingreso a datos personales, sino también la comprensión de cómo se utiliza, los propósitos para los cuales se recopila, su origen, a dónde se envían y cuánto tiempo se conservan los datos. Esta capacidad de supervisión es crucial, ya que permite a las personas asegurar un manejo adecuado y ético de su información personal.

Adicionalmente, el artículo estipula que los encargados de gestionar bases de datos restringidas a información personal solamente pueden compartir dicha información con el consentimiento explícito del titular o conforme a lo establecido por ley. Esta limitación es fundamental para prevenir la difusión no autorizada de información personal, asegurando que el consentimiento del titular es esencial antes de proceder con cualquier transferencia de datos.

Un aspecto crucial del Hábeas Data es la garantía del titular de la información para solicitar acceso sin costo al archivo, así como la actualización, rectificación, eliminación o anulación de los datos. Este derecho es particularmente relevante en el caso de datos sensibles, para los cuales la ley o el consentimiento del titular exigen medidas de seguridad adicionales. Si una solicitud de

este tipo no es atendida por el responsable del banco de datos, el titular puede acudir a una jueza o juez para hacer valer su derecho, y también puede demandar por los perjuicios ocasionados debido al incumplimiento de las obligaciones de protección de datos.

El Hábeas Data, en su rol de figura jurídica, emerge como respuesta a la creciente necesidad de asegurar la privacidad individual ante el uso expansivo de las TICS. Dentro del entorno donde la recopilación y el tratamiento de datos personales son fundamentales para diversas actividades económicas, sociales y gubernamentales, este derecho se convierte en un instrumento esencial para evitar malas prácticas y asegurar un manejo ético y seguro de la información personal.

Ley Orgánica de Protección de Datos Personales

La Ley Orgánica de Protección de Datos Personales en Ecuador configura un marco legal completo que ampara el ejercicio del derecho a la protección de datos personales. Este marco legal incluye principios, derechos y responsabilidades aplicables tanto a los propietarios de los datos como a las organizaciones que los procesan. Los nueve primeros artículos de la ley describen con precisión el alcance de aplicación, las definiciones cruciales y los requisitos para el procesamiento adecuado de los datos. Esta normativa es crucial para cuidar la privacidad y mantener la integridad de la información personal en un mundo cada vez más influenciado por la tecnología.

El propósito central de esta ley es garantizar la protección irrestricta del derecho a la intimidad de los datos personales. Esto facilita que los individuos puedan acceder a sus datos y tomar decisiones sobre los mismos, asegurando al mismo tiempo que estos estén adecuadamente protegidos. La ley se aplica a todo tipo de datos personales, sin importar si el almacenamiento es automático o manual. No obstante, hace excepciones en ciertos casos, como las actividades domésticas privadas, los datos que han sido anonimizados y los procesos de datos realizados en marcos de seguridad y defensa nacional.

Estas exclusiones son necesarias para equilibrar la protección de datos personales con otras necesidades sociales y de seguridad.

Dentro de las definiciones clave que ofrece la ley, se encuentran varios términos esenciales para comprender su alcance y aplicación práctica. Por ejemplo, la 'anonimización' describe el proceso por el cual se aplican técnicas que previenen la identificación fácil de individuos, salvaguardando así su privacidad. 'Consentimiento' implica una declaración voluntaria, clara, informada y precisa del titular de los datos, otorgando permiso para su procesamiento. Se convierte en un pilar fundamental para garantizar el control individual sobre la información personal. Otros términos definidos en la ley, como 'dato biométrico', 'dato genético', 'dato personal' y 'dato sensible', son cruciales por sus particularidades y las medidas de protección que cada uno requiere.

La legislación se fundamenta en varios albores esenciales que orientan el manejo de la información personal. Entre estos principios se encuentra la 'juridicidad', que impone una

adherencia rigurosa a las leyes y normativas vigentes; la 'lealtad', asegurando un procesamiento de datos justo y transparente; y la 'transparencia', facilitando que la información sobre el procesamiento de los datos sea clara y accesible para los propietarios de los datos.

Adicionalmente, el principio de 'finalidad' restringe la manera en la que son usados estos datos exclusivamente a los objetivos para los cuales se recopilaron; 'pertinencia y minimización', que restringen la recolección de datos al mínimo necesario; y 'seguridad', que exige la implementación de medidas apropiadas para prevenir accesos no autorizados o la pérdida de datos.

Los artículos 11 a 24 de la ley especifican una gama amplia y robusta de derechos para los titulares de datos, otorgándoles un control significativo sobre su información personal. Este conjunto de derechos comprende desde el derecho a mantenerse informado sobre el tratamiento de sus datos, el derecho de acceso para visualizar y recuperar sus datos personales, y el derecho de rectificación y actualización para corregir cualquier inexactitud o dato desactualizado.

Adicionalmente, los titulares ostentan el derecho de eliminación para solicitar la supresión de su información en ciertos parámetros, el derecho de oposición para rechazar el tratamiento de sus datos por motivos justificados, y el derecho a la portabilidad para garantizar la transmisión de sus datos entre distintos responsables del tratamiento.

La legitimidad del tratamiento de datos personales bajo la legislación actual requiere que se cumpla al menos una de varias condiciones predefinidas. Estas condiciones comprenden el consentimiento expreso del titular, que debe ser otorgado de manera voluntaria, específica, informada y clara; el cumplimiento de las obligaciones legales es un requisito fundamental para que el responsable del tratamiento pueda operar de forma lícita; decisiones judiciales; la necesidad de proteger el interés público o ejecutar un contrato; la defensa de intereses vitales del titular o de terceros; y las razones legítimas que fundamentan el tratamiento de datos por parte del responsable. Estos criterios están diseñados para avalar que el procesamiento de información se lleve a cabo de forma legal y ética, protegiendo los derechos de los ciudadanos y permitiendo el uso adecuado de los datos para propósitos legítimos.

Mejoras en la Legislación Actual: Propuestas para enmendar la Ley Orgánica de Protección de Datos Personales

La Ley Orgánica de Protección de Datos Personales en Ecuador, promulgada en 2021, representa un avance significativo en la protección de la privacidad de los individuos. Sin embargo, existen áreas que requieren mejoras para asegurar una protección más robusta y adaptada a las necesidades actuales.

Una de las propuestas más relevantes es la actualización periódica de la ley para incorporar las innovaciones tecnológicas y los nuevos riesgos asociados a la gestión de datos. Según Peralta Orosco (2021), la legislación debe ser dinámica y adaptable, permitiendo ajustes rápidos en respuesta a los cambios tecnológicos y sociales. Esto incluye la inclusión de

disposiciones específicas para la protección de datos en el contexto de tecnologías emergentes como la inteligencia artificial y el Internet de las Cosas (IoT).

Asimismo, es fundamental fortalecer las sanciones y mecanismos de cumplimiento para asegurar que las empresas y entidades públicas cumplan rigurosamente con las normativas de protección de datos. Esto podría implicar un aumento en las multas y la implementación de auditorías periódicas obligatorias para verificar el cumplimiento de las normas de protección de datos.

Nuevas Leyes y Normativas: Necesidad de nuevas regulaciones para abordar las lagunas actuales en la protección de datos

Aunque la ley actual proporciona una base sólida, existen lagunas que requieren la implementación de nuevas regulaciones específicas. Por ejemplo, la creación de una ley específica para la protección de datos en el ámbito laboral, que regule el manejo de información personal de los empleados y establezca derechos claros para los trabajadores.

Otra área que necesita atención es la protección de datos de menores de edad. Se debe desarrollar una normativa específica que contemple la recolección y uso de datos de menores, garantizando que cualquier tratamiento de esta información se realice con un consentimiento informado y específico de los padres o tutores.

Caso de estudio

Dentro del Juicio No. 09201-2020-00041, la acción de Hábeas Data fue interpuesta por Alexandra Jacqueline Zapata Santamaría contra el Hospital General Guasmo Sur debido a la negativa de esta institución a proporcionarle información detallada relacionada con su expediente laboral y médico. La acción fue admitida y calificada, y se convocó a una audiencia pública conforme a la ley. La ausencia de la parte demandada en la audiencia permitió que los argumentos de la accionante fueran considerados sin oposición.

La relevancia del Hábeas Data en este caso radica en su capacidad para garantizar el acceso a la información personal y proteger derechos conexos como la privacidad y la transparencia administrativa. La acción permitió a la demandante exigir transparencia y rendición de cuentas del hospital, fortaleciendo así el Estado de Derecho y asegurando que las instituciones públicas cumplan con sus obligaciones legales.

En conclusión, el Hábeas Data se destacó como un mecanismo esencial para la protección de derechos fundamentales, asegurando que la información personal sea accesible y que las entidades públicas sean transparentes en sus actuaciones. Este proceso judicial no solo buscó remediar la vulneración específica sufrida por la accionante, sino que también reforzó el compromiso de las instituciones con la transparencia y la rendición de cuentas.

Comparación con Normativas Internacionales

El Hábeas Data se establece como una figura jurídica crucial que responde a la necesidad imperativa de salvaguardar la privacidad de las personas ante el creciente uso de las TICS. En un

entorno donde el acopio y el procesamiento de datos personales son primordiales para algunas funciones económicas, sociales y gubernamentales, este derecho se presenta como un instrumento esencial para prevenir malas prácticas y asegurar un manejo ético y seguro de la información personal.

El poder de controlar y acceder a los datos personales constituye un pilar de la autodeterminación informativa, un principio vinculado intrínsecamente a la dignidad humana y que permite a las personas decidir cómo se utilizan sus datos personales. Este principio se alinea con normas internacionales de derechos humanos y protección de datos, como se refleja en el Reglamento General de Protección de Datos (RGPD) de la Unión Europea, estableciendo un estándar global de privacidad y seguridad de la información.

Ambos son marcos legales que establecen principios, derechos y obligaciones para la protección de datos personales. Ambos textos buscan salvaguardar la privacidad y la integridad de la información personal en sus respectivas jurisdicciones. A continuación, se presenta un análisis comparativo de estas normativas, destacando similitudes, diferencias y sus implicaciones en la protección de datos.

El RGPD, al ser una normativa pionera y estricta, ha establecido un marco de referencia global para la protección de la privacidad de los datos, sirviendo de modelo para las leyes de otros países. En diversas partes del mundo, incluyendo Ecuador. La severidad de sus sanciones y el detalle en sus disposiciones reflejan una respuesta a la creciente preocupación por la privacidad en la era digital. La LOPDP, aunque similar en muchos aspectos, debe enfrentarse a desafíos específicos de su contexto socioeconómico y tecnológico.

Ambos marcos normativos comparten varios principios y objetivos clave en la protección de datos personales:

Derechos de los Titulares: El Reglamento General de Protección de Datos y La Ley Orgánica de Protección de Datos Personales confieren a los individuos derechos esenciales relacionados con sus datos personales. Estos derechos, que abarcan el acceso, la rectificación, la eliminación (también conocida como 'derecho al olvido'), la oposición y la portabilidad, están concebidos para asegurar que los titulares puedan ejercer pleno control sobre su información personal.

Principios de Tratamiento de Datos: Ambos textos legales establecen principios fundamentales como la legalidad, lealtad, transparencia, finalidad, minimización y seguridad. Estos principios sirven como brújula para el tratamiento de datos personales, garantizando su manejo ético y conforme a la ley.

Consentimiento: Ambas normativas definen principios clave como legalidad, lealtad, transparencia, propósito específico, minimización de datos y seguridad. Estos principios fundamentales orientan la gestión de datos personales, garantizando un manejo que es tanto ético como conforme a la ley.

Obligaciones de los Responsables y Encargados del Tratamiento: En las dos legislaciones, el consentimiento informado y explícito del titular constituye una condición esencial para el procesamiento de datos personales. Este consentimiento debe ser otorgado libremente, de manera específica y clara, estableciendo una fundación legítima para la manipulación de los datos.

Autoridades de Control: Los dos sistemas normativos estipulan la necesidad de una autoridad reguladora independiente encargada de monitorear y asegurar la observancia de las leyes de protección de datos. En Ecuador, esta función la desempeña la Autoridad de Protección de Datos Personales, mientras que, en la Unión Europea, el Comité Europeo de Protección de Datos, que consta de representantes de las autoridades nacionales de cada Estado miembro, cumple esta labor.

No obstante, las coincidencias, existen diferencias notables entre el Reglamento General de Protección de Datos (RGPD) de la UE y la Ley Orgánica de Protección de Datos Personales de Ecuador:

Ámbito Territorial y Alcance: El RGPD se caracteriza por su explicitud extraterritorial, se aplica a todas las entidades que procesen datos personales de personas en la UE, sin importar dónde esté ubicada la entidad. Por otro lado, la LOPDP se centra más en las entidades que operan dentro de su jurisdicción nacional, aunque también extiende su aplicación a organizaciones extranjeras que procesen datos de ciudadanos ecuatorianos.

Sanciones: Las penalizaciones impuestas por el RGPD son notablemente más estrictas en comparación con las de la LOPDP. Este reglamento europeo puede imponer multas que pueden alcanzar los 20 millones de euros o el 4% de la facturación global anual de la empresa, según corresponda, reflejando la rigurosidad con la que la UE trata las infracciones.

Mecanismos de Cumplimiento: El RGPD incluye el mecanismo de ventanilla única, que permite a las empresas con operaciones en múltiples Estados miembros de la UE interactuar con una única autoridad de control principal. Este mecanismo busca simplificar la gestión y supervisión del cumplimiento normativo. La LOPDP no incluye un mecanismo similar debido a la estructura administrativa diferente y a su ámbito de aplicación más limitado.

Transferencias Internacionales de Datos: El RGPD establece un enfoque exhaustivo para la traspaso de información personal hacia países que no conforman la UE, que incluye revisiones de adecuación realizadas por la Comisión Europea y la implementación de cláusulas contractuales estándar. Por su parte, la LOPDP de Ecuador también supervisa las transferencias internacionales de datos, aunque los procedimientos y requisitos específicos pueden variar significativamente en comparación con los del RGPD.

Especificidad en el Tratamiento de Datos Sensibles: Mientras que ambos marcos reconocen la necesidad de proteger datos sensibles, el RGPD proporciona directrices más detalladas sobre la manipulación de datos personales de índole delicada, incluyendo datos

biométricos y genéticos. La LOPDP también reconoce estos tipos de datos, pero su tratamiento puede estar sujeto a regulaciones y enfoques específicos que difieren de la normativa europea.

Para que la LOPDP alcance su pleno potencial, es fundamental que se desarrollen y fortalezcan las capacidades de la Autoridad de Protección de Datos Personales. Además, se requiere una mayor sensibilización y educación tanto para las entidades que manejan datos como para los ciudadanos, garantizando que comprendan sus derechos y responsabilidades. La cooperación internacional y la adaptación continua a las mejores prácticas globales serán esenciales para mantener la relevancia y eficacia de la ley en un entorno digital en constante evolución.

Alcance y Limitaciones Del Hábeas Data En La Protección De Datos Personales

El Hábeas Data se establece como un derecho constitucional esencial en la protección de la información personal contra el manejo inapropiado por entidades de carácter público y privado. En el contexto actual de la era digital, donde la recolección, el almacenamiento y el procesamiento de datos son extensivos y constantes, el Hábeas Data se vuelve fundamental para garantizar la autodeterminación informativa y la privacidad de las personas.

Siguiendo esta línea, García (2007) argumenta que el derecho a la protección de los datos personales se incorporó originalmente en los sistemas jurídicos locales como una extensión del derecho a la privacidad. No obstante, con el avance tecnológico hacia el final del siglo XX, fue necesario replantear los límites tradicionales de este derecho humano, dada la creciente intrusión tecnológica en la esfera privada de los individuos.

Salmon Alvear (2008) destaca que el Hábeas Data salvaguarda información personal que incluye nombres, direcciones, identificaciones, detalles financieros, y datos delicados como la etnicidad, opiniones políticas, creencias religiosas, estado de salud y detalles de la vida sexual. En la era digital, con la constante recolección y procesamiento de datos por parte de entidades tanto públicas como privadas, esta protección se vuelve imprescindible. La posibilidad de que los individuos accedan, rectifiquen o eliminen sus datos es vital para asegurar la transparencia y responsabilidad en el tratamiento de información personal.

Limitaciones del Hábeas Data en el Contexto Digital

La regulación del uso y protección de datos personales a través del Hábeas Data representa un desafío que demanda un delicado balance entre proteger la privacidad y permitir el acceso a la información. Carballo (2012) subraya que, dado el contexto digital actual, los confines del Hábeas Data deben ser delineados teniendo en cuenta la naturaleza cambiante y global de la información, lo que incluye el manejo de datos a través de diversas jurisdicciones y complica la aplicación de las legislaciones nacionales sobre protección de datos.

En este contexto, se vuelve esencial adherirse a los principios de finalidad, proporcionalidad y minimización de datos. El principio de finalidad requiere que la recolección

de datos personales se realice con un objetivo claro, explícito y legítimo, y que su tratamiento no se desvíe de estos objetivos iniciales.

El principio de proporcionalidad dicta que el manejo de los datos debe ser compatible con las finalidades para las que fueron recabados y no exceder lo necesario respecto a los fines para los que fueron recolectados. Finalmente, el principio de minimización establece que la cantidad de datos personales recolectados y procesados debe limitarse estrictamente a lo esencial para alcanzar los propósitos definidos.

Alcances del Hábeas Data en la Era Digital

En la era digital, el Hábeas Data cubre diversos aspectos fundamentales en la protección de datos personales. En primer término, se reconoce a las personas el derecho de acceder a sus datos personales que se conservan en bases de datos, permitiéndoles verificar el origen, finalidad y destino de estos datos. Este derecho de acceso es crucial para asegurar tanto la transparencia como la responsabilidad en la gestión de la información personal.

Además, el Hábeas Data faculta a los individuos para requerir la corrección, actualización o supresión de datos personales que sean incorrectos, incompletos o que estén desfasados. Este derecho de rectificación es vital para certificar la precisión y la fiabilidad de estos datos, aspectos que pueden impactar significativamente la vida y el bienestar de las personas.

Por último, el Hábeas Data también contempla el derecho de oposición, que adjudica a los ciudadanos a rechazar el procesamiento de su información personal bajo ciertas condiciones. Este derecho adquiere especial importancia en el ámbito de la publicidad y el marketing digital, donde los datos personales son frecuentemente empleados sin un consentimiento claro y directo de los sujetos implicados.

Procedimientos y garantías en el ejercicio del hábeas data

Iniciar un proceso de Hábeas Data en Ecuador requiere que el interesado haga una solicitud formal ante la entidad o individuo que posee los datos. Esta solicitud debe ser clara y detallada, incluyendo los datos personales del solicitante, la información específica que desea acceder o corregir, y las razones detrás de la solicitud.

La entidad a la que se dirige tiene un plazo máximo de quince días para emitir una respuesta. Si la respuesta es insatisfactoria o no se recibe dentro del plazo estipulado, el solicitante puede llevar el caso ante un juez, presentando una acción de protección. Esta acción debe acompañarse de la solicitud original y cualquier prueba adicional que apoye el caso del solicitante.

En el ámbito judicial, el juez evaluará la validez de la solicitud y la respuesta (o ausencia de esta) por parte de la entidad o persona encargada de los datos. Si la acción de protección es aceptada, el juez puede imponer medidas cautelares para asegurar que los datos no se destruyan o alteren durante el proceso judicial.

El procedimiento culmina con una audiencia pública en la cual ambas partes pueden presentar sus argumentos y pruebas. El juez, basado en el principio pro-persona y los estándares

internacionales de protección de datos, debe emitir una resolución en un plazo no mayor a treinta días desde la presentación de la acción.

El resultado de la acción puede ser la orden de rectificación, actualización, eliminación de los datos, o cualquier otra medida que el juez considere necesaria para proteger los derechos del solicitante. Es importante destacar que las resoluciones judiciales en materia de Hábeas Data son apelables, lo cual garantiza un doble grado de jurisdicción.

La legislación ecuatoriana incorpora diversas garantías procesales que fortalecen al Hábeas Data como mecanismo esencial para garantizar la protección efectiva de los derechos individuales en materia de datos personales y privacidad. Entre estas garantías, destaca el derecho fundamental al acceso y control de información personal privada. Este derecho, establecido en el artículo 92 de la Constitución de Ecuador, otorga a los individuos la capacidad de monitorear de manera continua su propia información.

La consagración de este derecho en la Constitución no solo resalta la relevancia de la autodeterminación informativa, sino que también ofrece una herramienta robusta que permite a los individuos proteger su privacidad y garantizar la transparencia en el manejo de sus datos personales.

Los plazos procesales definidos en la legislación ecuatoriana, como los quince días para la respuesta inicial y los treinta días para la resolución judicial, constituyen una garantía de celeridad y eficiencia en la administración de justicia. Estos plazos buscan evitar dilaciones innecesarias, promoviendo la prontitud en la resolución de los casos de Hábeas Data. La especificación de estos plazos procesales asegura que los derechos de los individuos sean protegidos de manera oportuna, evitando que la inercia procesal pueda vulnerar los mecanismos legales que permiten verificar y modificar datos.

El derecho a una audiencia pública constituye una garantía procesal clave dentro del marco del Hábeas Data. Este derecho facilita que tanto el demandante como la entidad que posee los datos expongan sus puntos de vista ante un juez neutral. La naturaleza abierta y transparente de estos procedimientos no solo fomenta la confianza en el sistema judicial, sino que también garantiza que cada caso sea examinado de manera justa y equitativa.

La capacidad de argumentar y presentar pruebas públicamente es vital para mantener salvaguardar la imparcialidad y el correcto desarrollo del proceso judicial, garantizando así la tutela efectiva de los derechos individuales.

La posibilidad de que el juez ordene medidas cautelares durante el proceso es una garantía esencial para proteger los datos personales mientras se resuelve el caso. Estas medidas cautelares, que pueden incluir la prohibición de destruir o alterar los datos en cuestión, garantizan que la información se mantenga íntegra durante todo el proceso judicial. La implementación de medidas cautelares es crucial para prevenir cualquier daño irreparable a los derechos de privacidad de los individuos mientras se decide el fondo del asunto.

La capacidad de apelar las decisiones judiciales en casos de Hábeas Data es una garantía procesal fundamental. Este recurso permite que las sentencias sean evaluadas por un tribunal superior, proporcionando una protección adicional a los derechos del demandante. La implementación del doble grado de jurisdicción no solo refuerza la justicia y la equidad en el tratamiento de las disputas, sino que también ofrece una vía para rectificar errores judiciales, asegurando así una administración de justicia más efectiva y justa.

El sistema legal de Ecuador, a través de su legislación de Hábeas Data, muestra un claro compromiso hacia la protección de los datos personales y la privacidad. Las salvaguardias procesales que se han implementado no solo fortalecen los derechos individuales, sino que también fomentan un sistema judicial eficaz y transparente. Aspectos como los plazos definidos, el derecho a audiencias públicas, las medidas preventivas y el sistema de doble instancia son fundamentales para garantizar una defensa completa y efectiva de la información personal. Estos elementos reflejan una perspectiva jurídica moderna que valora la privacidad en la era digital y ofrece recursos significativos para la protección de derechos esenciales de los ciudadanos.

El Hábeas Data no solo salvaguarda la privacidad de los individuos, sino que también promueve una mayor transparencia y responsabilidad en la gestión pública. La aplicación efectiva de este derecho actúa como un poderoso mecanismo para que los ciudadanos supervisen y controlen cómo se maneja la información pública.

Educación y concientización sobre el hábeas data

En el contexto actual de rápida evolución tecnológica, la educación en derechos digitales se posiciona como un elemento esencial para velar por la privacidad y el manejo diligente de los datos de las personas. En su ponencia, Naranjo Godoy (2020) ex Directora Nacional de Registro de Datos Públicos nos resalta la incorporación de módulos educativos que abarquen la seguridad de la información, la privacidad digital y la ética en el uso de las tecnologías en los planes de estudio de escuelas y universidades es fundamental.

La ausencia de educación en estos aspectos puede derivar en violaciones de la privacidad y otros perjuicios legales y sociales, lo que subraya la urgencia de políticas públicas que fomenten una educación digital integral y accesible para todos.

El análisis del Hábeas Data realizado por Guanín-Collaguazo (2024) resalta una conciencia creciente sobre la protección de datos en Ecuador, impulsada por avances tecnológicos y la digitalización. Aunque no se mencionan estudios específicos, se sugiere una distribución desigual del conocimiento sobre derechos digitales, destacando la necesidad de una mayor educación en sectores menos informados.

Asimismo, la autora argumenta que la educación en derechos digitales es crucial para la efectividad del Hábeas Data. La falta de conocimiento puede llevar a violaciones de privacidad y otros derechos fundamentales. Se discute cómo el desconocimiento puede resultar en

consecuencias negativas, subrayando la importancia de programas educativos que empoderen a los ciudadanos en la gestión de sus datos personales.

Programas de Sensibilización y Capacitación: Propuestas para aumentar la conciencia pública y la capacitación profesional en protección de datos

La educación y la sensibilización son componentes clave para una protección de datos efectiva. Es necesario implementar programas de sensibilización dirigidos al público general para aumentar la conciencia sobre la importancia de la privacidad y los derechos relacionados con los datos personales.

Además, la capacitación profesional continua para aquellos que manejan datos personales es esencial. Esto incluye formación específica para funcionarios públicos y empleados del sector privado que trabajan en áreas relacionadas con la gestión de datos. La creación de certificaciones profesionales en protección de datos puede contribuir a mejorar la competencia técnica y el cumplimiento de las normativas.

Una población bien informada es crucial para el desarrollo de políticas más efectivas y la creación de tecnologías que respeten los derechos humanos y contribuyan al bienestar común, fortaleciendo así el tejido social y la democracia mediante la promoción de una mayor transparencia y responsabilidad en el manejo de datos personales. Además, esta educación ayuda a los individuos a comprender y ejercer efectivamente sus derechos, como el Hábeas Data, asegurando que puedan desafiar y corregir el uso indebido de su información personal.

En conclusión, fortalecer la protección de datos en Ecuador requiere un enfoque integral que combine mejoras legislativas, la adopción de estándares internacionales y programas de sensibilización y capacitación. Implementar estas recomendaciones contribuirá a crear un entorno más seguro y protegido para la información personal de todos los ciudadanos ecuatorianos.

Cooperación Internacional Y Estándares Globales

La colaboración internacional y la implementación de normativas globales son cruciales para la protección de datos personales. En un mundo globalizado y cada vez más conectado, estas iniciativas son esenciales para mejorar la gestión y la seguridad de la información personal, elementos clave para la salvaguarda de los derechos ciudadanos a nivel mundial. Este análisis explorará el impacto de la cooperación internacional y de los estándares globales en la legislación ecuatoriana, con el objetivo de fomentar un manejo de datos más seguro y bien regulado.

Existen diversos acuerdos internacionales que establecen mecanismos de cooperación para la protección de datos, como el Convenio Europeo de Protección de Datos Personales (1981) y el Convenio para la Protección de las Personas con Respecto al Tratamiento Automatizado de Datos de Carácter Personal (1995) (REDIPD, 2020).

La cooperación internacional en protección de datos personales trae beneficios significativos, como el intercambio de mejores prácticas y experiencias, que son cruciales para enfrentar desafíos comunes como los ciberataques y el uso indebido de datos. La coordinación

internacional en las leyes de protección de datos facilita una protección más eficaz y eficiente de los derechos ciudadanos en el ámbito digital.

Adopción de Estándares Internacionales: Implementación de mejores prácticas globales y cooperación con organismos internacionales.

La adopción de estándares internacionales es crucial para elevar el nivel de protección de datos en Ecuador. La implementación de mejores prácticas globales, como las establecidas por el Reglamento General de Protección de Datos (GDPR) de la Unión Europea, puede servir como un marco de referencia para fortalecer las leyes locales.

La cooperación con organismos internacionales y la participación en foros globales de protección de datos permiten a Ecuador aprender de las experiencias de otros países y adaptar estas prácticas a su contexto local. Además, esta cooperación puede facilitar la asistencia técnica y el acceso a recursos y herramientas avanzadas para la protección de datos.

La entrada en vigor del RGPD ha convertido a la Unión Europea en referente internacional en cuanto a la normativa sobre protección de datos., motivando a naciones fuera de Europa, incluyendo Ecuador, a evaluar y mejorar sus propias leyes de protección de datos. Normativas globales promovidas por organizaciones como la OCDE y la UNCTAD han creado un marco que promueve la tutela de la intimidad y el derecho a la autonomía informativa de las personas a través de múltiples jurisdicciones.

Ecuador ha tomado medidas para adaptar sus normativas internas a los estándares globales en materia de protección de datos. Un ejemplo significativo es la Ley Orgánica de Protección de Datos Personales (2021), la cual se basa en principios y conceptos alineados con el RGPD y otros instrumentos internacionales, como señala Maqueo Ramírez (2015)

CONCLUSIONES

Ecuador debe seguir adaptando su legislación de protección de datos para enfrentar los desafíos emergentes de la digitalización global. Esto incluye la adopción de estándares internacionales como el RGPD de la Unión Europea, que constituye un modelo confiable para el procesamiento y la protección de datos personales. Se recomienda la creación de un comité regulador dedicado a la evaluación continua y la actualización de las leyes de protección de datos, asegurando que estas sean efectivas y pertinentes en el contexto tecnológico actual.

Es crucial que el gobierno ecuatoriano invierta en programas educativos centrados en los derechos digitales y la protección de datos. Estos programas deberían estar dirigidos a todos los niveles educativos e incluir la capacitación de profesionales que manejan datos personales en su trabajo diario. Esta medida no solo contribuirá a un mayor entendimiento y sensibilización acerca de la relevancia de salvaguardar los datos personales, sino que también empoderará a los ciudadanos para que sepan cómo actuar efectivamente cuando sus derechos sean vulnerados.

La cooperación internacional es esencial para mantener los estándares de protección de datos a nivel global. Ecuador debería buscar activamente formar parte de foros y tratados internacionales sobre protección de datos, lo que facilitaría el intercambio de información sobre buenas prácticas y tecnologías avanzadas. Además, las alianzas internacionales pueden ayudar a Ecuador a implementar estrategias efectivas de ciberseguridad y a responder de manera coordinada a las amenazas a la privacidad que cruzan fronteras nacionales.

Los desafíos tecnológicos y de infraestructura requieren una respuesta integral que incluya la modernización de las herramientas tecnológicas y sistemas de datos del país. Además, es vital la formación continua de los encargados de aplicar la ley de protección de datos, asegurando que estos tengan los conocimientos y recursos necesarios para ejecutar la legislación de manera efectiva. Se sugiere la implementación de un plan nacional que aborde específicamente las necesidades de capacitación y las mejoras de infraestructura necesarias para proteger los datos personales de los ciudadanos ecuatorianos.

REFERENCIAS

- Carballo, D. L. (2012). *Legitimación y procedimiento del Hábeas Data en Ecuador*. Recuperado de <https://dlcarballo.com/2012/01/27/legitimacion-y-procedimiento-del-habeas-data-en-ecuador/>
- Constitución de la República del Ecuador, Asamblea Constituyente. (2008). Registro Oficial No. 449.
- DINARP. (2020, 4 septiembre). Habeas Data es la acción jurídica para proteger los datos personales hasta tener una legislación [Vídeo]. YouTube. <https://www.youtube.com/watch?v=-PQhEPjBujw>
- González, A. G. (2007). *La protección de datos personales: derecho fundamental del siglo XXI. Un estudio comparado*. Redalyc.org. Recuperado de <https://www.redalyc.org/articulo.oa?id=42712003>
- Guanín-Collaguazo, O. (2024). Hábeas Data como garantía de protección al derecho a la intimidad. *RECIHYS Revista Científica de Ciencias Humanas y Sociales*, 2(1), 20-25. Recuperado de <https://journal.espe.edu.ec/ojs/index.php/RECIHYS/article/view/3472>
- Ley Orgánica de Protección de Datos Personales, Registro Oficial Suplemento No. 459. (2021).
- Maqueo Ramírez, M. S. (2015). Identificación de instrumentos internacionales. Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales. https://home.inai.org.mx/wp-content/documentos/DocumentosDeInteres/Estudio_desarrollo_normativo_y_jurisprudencial.pdf
- Montaña Pinto, J., & Porras Velasco, A. (2011). *Apuntes de derecho procesal constitucional* (2.^a ed., Vol. 3). Juan Montaña Pinto y Angélica Porras Velasco. Recuperado de http://bivicce.corteconstitucional.gob.ec/bases/biblo/texto/Apuntes_2/Apuntes_derecho_procesal_constitucional_2.pdf
- Ordóñez Pineda, L. O. (2019). El Hábeas Data como garantía procesal frente a las tecnologías de la información y comunicación: situación en el contexto ecuatoriano. *Res Non Verba*, 9(2), 1-14. Recuperado de <https://revistas.ecotec.edu.ec/index.php/rnv/article/download/219/178/354>
- Peralta Orosco, G. (2023). Desafíos del derecho de la protección de datos en días de globalización. *Lucerna Iuris Et Investigatio* <https://revistasinvestigacion.unmsm.edu.pe/index.php/Lucerna/article/download/18376/16531/68637>
- Pérez Ordóñez, D. (2001). El Hábeas Data. *Iuris Dicto*, 2(3), 133. <https://revistas.usfq.edu.ec/index.php/iurisdictio/article/view/550/621>

- REDIPD. (2020). Estandares Internacionales sobre Protección de Datos Personales. Buenos Aires: REDIPD. Recuperado de https://www.redipd.org/sites/default/files/inline-files/Estandares_Esp_Con_logo_RIPD.pdf
- Reglamento General a la Ley Orgánica de Protección de Datos Personales, Registro Oficial Suplemento 435 de 13-nov.-2023.
- Reglamento General de Protección de Datos, Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de la Unión Europea. (2016). Diario Oficial de la Unión Europea. <https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A32016R0679>
- Salmon Alvear, C. (2008). *Nociones del Hábeas Data en Ecuador*. Revista Jurídica Online. Recuperado de <https://www.revistajuridicaonline.com/wp-content/uploads/2008/07/mp-nociones-del-habeas-data-ecuador.pdf>
- Suárez Cadena, A. (2021). El Hábeas Data: Orígenes y evolución en el derecho comparado. Revista Lex, 19(1), 125-150. Recuperado de <https://revistalex.org/index.php/revistalex/article/view/97/228#:~:text=Los%20primeros%20inicios%20del%20H%C3%A1beas,control%20en%20la%20recaudaci%C3%B3n%2C%20difusi%C3%B3n>