Artículo de Investigación DOI: https://doi.org/10.61154/holopraxis.v9i2.4177

Impacto global del Reglamento General de Protección de Datos en la protección de datos personales

Global impact of the General Data Protection Regulation on the protection of personal data

Leonardo Angelo Ramos-Villavicencio [a], Eduardo Sebastian Huatuco-Cruz [b], Leoncio Enrique Vásquez-Solis [c], José Luis Mandujano-Rubín [d]

[a] Universidad Nacional Hermilio Valdizán, Huánuco, Huánuco, Perú, Email: 2023120419@unheval.pe, Orcid: https://orcid.org/0009-0006-5634-172X

[b] Universidad Nacional Hermilio Valdizán, Huánuco, Huánuco, Perú, Email: 2023120048@unheval.pe Orcid: https://orcid.org/0009-0005-9243-4387

[c] Universidad Nacional Hermilio Valdizán, Huánuco, Huánuco, Perú, Email: lvasquez@unheval.edu.pe Orcid: https://orcid.org/0000-0002-8404-2368

[d] Universidad Nacional Hermilio Valdizán, Huánuco, Huánuco, Perú, Email: lvasquez@unheval.edu.pe Orcid: https://orcid.org/0000-0001-5905-3965

Recibido: 29 de abril de 2025

Aprobado: 2 de julio de 2025

RESUMEN

El estudio tuvo como objetivo examinar la implementación y el impacto del Reglamento General de Protección de Datos (GDPR) en las normativas de protección de datos personales en América Latina, con enfoque en Perú, Colombia y Ecuador. Se buscó identificar similitudes y diferencias entre las legislaciones nacionales y el GDPR, evaluar avances y desafíos, y proponer recomendaciones para alinearlas con estándares internacionales. La investigación adoptó un enfoque cualitativo y descriptivo, con diseño documental. Se analizaron leyes nacionales, informes regulatorios, estudios académicos y casos de filtraciones de datos, mediante matrices de análisis de contenido, se compararon principios claves, derechos de los titulares, requisitos de tratamiento de datos y sanciones entre el GDPR y las normativas de los tres países. Se identificó que

las legislaciones de Perú, Colombia y Ecuador incorporaron principios del GDPR, como consentimiento explícito y transparencia. Sin embargo, persistieron brechas en la implementación efectiva, ausencia del derecho al olvido (en Ecuador y Perú) y vulnerabilidades técnicas. Casos emblemáticos, como la filtración masiva en Ecuador (2019) y el acceso indebido a datos bancarios en Perú (2023), evidenciaron deficiencias en seguridad y cumplimiento. Además, se identificaron limitaciones en recursos de autoridades regulatorias y baja conciencia ciudadana sobre protección de datos. El GDPR influyó significativamente en la modernización de las leyes latinoamericanas, pero su efectividad requiere fortalecer infraestructuras regulatorias, inversión en educación digital y armonización normativa. Se concluyó que la colaboración multisectorial (gobiernos, empresas y sociedad) es esencial para garantizar la protección de datos en un entorno digital globalizado.

Descriptores: protección de datos; ética de la tecnología; gobernanza de internet (Tesauro UNESCO).

ABSTRACT

The study set out to investigate the implementation and impact of the General Data Protection Regulation (GDPR) on personal data protection laws in Latin America, specifically focusing on Peru, Colombia, and Ecuador. The aim was to identify both similarities and differences between national legislations and the GDPR, assess progress and challenges, and provide recommendations for alignment with international standards. Employing a qualitative and descriptive approach, the research utilized a documentary design. It involved an analysis of national laws, regulatory reports, academic studies, and cases of data breaches. Through content analysis matrices, key principles, data subject rights, data processing requirements, and sanctions were compared between the GDPR and the regulations of the three countries. The findings revealed that the legislations of Peru, Colombia, and Ecuador incorporated several GDPR principles, including explicit consent and transparency. However, notable gaps in effective implementation remained, alongside the absence of the right to be forgotten in Ecuador and Peru, as well as various technical vulnerabilities. Prominent cases, such as the significant data breach in Ecuador (2019) and unauthorized access to banking data in Peru (2023), highlighted deficiencies in security and compliance. Additionally, challenges were identified regarding the resources available to regulatory authorities and the overall low level of citizen awareness concerning data protection. Although the GDPR has significantly influenced the modernization of laws in Latin America, enhancing its effectiveness necessitates strengthening regulatory frameworks, investing in digital education, and harmonizing legal standards. The conclusion drawn from the study emphasizes that multisectoral collaboration among governments, businesses, and society is essential to ensure robust data protection in an increasingly digitalized global environment.

Descriptors: data protection; technology ethics; internet governance (UNESCO Thesaurus).

INTRODUCCIÓN

La implementación del Reglamento General de Protección de Datos (GDPR) ha representado un hito en la legislación de privacidad y protección de datos a nivel global. Este reglamento, adoptado por la Unión Europea en 2016 y en vigor desde 2018, establece un marco robusto y comprensivo para el tratamiento de los datos personales de los individuos dentro de la UE y de aquellos fuera de la misma que interactúan con los datos de ciudadanos europeos. A través de sus 11 capítulos, que abarcan desde disposiciones generales hasta sanciones, el GDPR busca armonizar la normativa sobre la protección de datos, reforzar los derechos de los ciudadanos y aumentar la responsabilidad de las organizaciones en el manejo de la información personal. Entre los aspectos clave del GDPR se incluyen los principios de tratamiento, los derechos de los interesados, y las medidas para la transferencia internacional de datos, todo bajo la supervisión de autoridades independientes que aseguran el cumplimiento.

Este artículo aborda el problema global de la protección de datos personales en un contexto digital cada vez más complejo, en el que las empresas, gobiernos e individuos deben equilibrar la innovación tecnológica con el derecho a la privacidad. En este sentido, se examinan los principales desafíos derivados de la implementación de la GDPR, tanto en Europa como en otras regiones del mundo, y cómo su aplicación ha influido en la creación de normativas similares en países fuera de la UE. A su vez, se discutirá el impacto de esta regulación sobre las prácticas de privacidad, la seguridad de los datos y la responsabilidad de los actores involucrados.

La creciente preocupación por la privacidad y la protección de los datos personales ha generado un amplio debate en los últimos años, especialmente a raíz del auge de la digitalización y la recolección masiva de información. Según el análisis de Kuner, Bygrave, Docksey, & Drechsler (2020), "El GDPR no solo ha transformado la privacidad en Europa, sino que se ha convertido en un modelo para legislaciones nacionales en todo el mundo, impulsando un nuevo paradigma de responsabilidad corporativa y derechos individuales". Esta afirmación resalta la influencia significativa que el GDPR ha tenido, no solo como una normativa regional, sino también como una guía normativa para países fuera de la UE, que ahora buscan emular sus principios para mejorar la protección de datos personales en sus propias jurisdicciones.

Uno de los principios más relevantes del GDPR es su extraterritorialidad, que obliga a las empresas fuera de la Unión Europea a cumplir con los estándares europeos si procesan los datos de ciudadanos de la UE. Chander & Lê (2020) subrayan que "el principio de extraterritorialidad del GDPR obliga a las empresas fuera de la UE a cumplir con los estándares europeos, generando un efecto de 'armonización regulatoria' incluso en jurisdicciones sin leyes equivalentes". Este principio ha propiciado un proceso de armonización de regulaciones de protección de datos a nivel mundial, llevando a muchos países a modificar sus legislaciones para alinearse con las normativas europeas.

El derecho al olvido, otro de los pilares fundamentales del GDPR, ha tenido un impacto significativo en las discusiones legales internacionales. Tzanou (2017) señala que "el derecho al olvido, consagrado en el GDPR, enfrenta desafíos de aplicación en países con marcos legales fragmentados, donde jurisdicciones como Perú aún no lo reconocen explícitamente". Esta afirmación refleja la disparidad en la aplicación de este derecho en distintos países, subrayando la necesidad de una armonización global más efectiva, que permita a los ciudadanos ejercer el control sobre sus datos en todas las jurisdicciones.

La influencia del GDPR se extiende más allá de Europa, generando un cambio significativo en la forma en que se abordan la protección de datos personales y la privacidad en otras partes del mundo. En América Latina, varios países han comenzado a adaptar sus normativas a los principios del GDPR. En Chile, Peña Gutiérrez (2022), en su tesis sobre la "Aplicación del principio de finalidad limitada en el reglamento general de datos personales de la Unión Europea y su aplicación en la normativa de datos personales en Chile", describe cómo los principios del GDPR, y especialmente la finalidad limitada, se han ido incorporando gradualmente en la legislación chilena. Sin embargo, aún persisten desafíos, ya que la adaptación de estos principios a los marcos jurídicos locales requiere no solo cambios normativos, sino también un cambio cultural hacia una mayor conciencia sobre la protección de la privacidad.

En Ecuador, Ellian (2024) en su análisis sobre "El impacto del RGPD en las políticas y prácticas de protección de datos en Ecuador" concluye que, si bien el país ha realizado avances significativos al adoptar principios clave del GDPR, como el consentimiento explícito y la transparencia, todavía enfrenta importantes desafíos en términos de infraestructura tecnológica y la capacitación tanto del sector público como privado. Las

organizaciones ecuatorianas deben realizar inversiones sustanciales para cumplir con las exigencias del GDPR, lo que representa un desafío para las pequeñas y medianas empresas. Sin embargo, la modernización del marco legal ecuatoriano ha sido vista como una oportunidad para alinearse con las mejores prácticas internacionales y mejorar la transparencia en el tratamiento de los datos personales.

En España, Francesch (2024) analiza cómo el GDPR se ha comparado con las normativas de protección de datos en otras regiones, como los Estados Unidos y China. En su investigación, "Análisis comparativo de la protección de datos y la ciberseguridad: Modelos europeo, americano y chino", destaca cómo el GDPR establece un marco regulatorio integral que prioriza la protección de datos personales y la privacidad, imponiendo altos estándares en el procesamiento y la transferencia de datos personales. A diferencia del modelo estadounidense, que se basa en la autorregulación corporativa y el cumplimiento voluntario, el GDPR exige un cumplimiento más riguroso y proporciona un mayor nivel de protección a los individuos. Además, el modelo chino, centrado en la soberanía de los datos, se enfrenta a críticas debido a su énfasis en la regulación gubernamental.

Por otro lado, en el contexto latinoamericano, Alvear Richards & Hernández Pesantes (2023) realizan un análisis comparativo entre las leyes de protección de datos de Ecuador y Perú, enfocándose en la ciberseguridad y los delitos informáticos. Su trabajo destaca que, aunque ambas legislaciones comparten principios fundamentales de protección de datos, la legislación peruana tiene una ventaja significativa al abordar explícitamente los delitos informáticos. A pesar de las diferencias, los dos países están trabajando en la implementación de sistemas de gestión de seguridad de la información (SGSI) para garantizar la protección de los datos personales de los ciudadanos.

El propósito central de esta investigación es examinar la implementación y el impacto del GDPR en las normativas de protección de datos en América Latina, con un enfoque específico en Perú, Colombia y Ecuador. A través de un análisis comparativo, se busca identificar las similitudes y diferencias en las legislaciones de estos países con respecto al GDPR, evaluando los avances, los desafíos y las oportunidades que presentan para la protección de los datos personales. Además, se pretende ofrecer recomendaciones para

mejorar la eficacia de las leyes de protección de datos en estos países, alineándolas más estrechamente con los estándares internacionales establecidos por el GDPR.

MÉTODOS

La investigación se desarrolló bajo un enfoque cualitativo, dado que se buscó un análisis profundo de las normativas de protección de datos en Perú, Colombia y Ecuador, comparándolas con el Reglamento General de Protección de Datos (GDPR). Este enfoque permitió comprender las características, similitudes y diferencias clave entre las leyes de estos países y el GDPR, centrando el análisis en su efectividad y alineación con los estándares internacionales.

El diseño fue documental, debido a que se centró en la revisión de documentos legales y académicos. Se analizó la legislación de protección de datos de los países seleccionados, y su relación con los principios establecidos por el Reglamento General de Protección de Datos.

La investigación fue descriptiva, porque se caracterizaron las leyes y regulaciones de protección de datos en los tres países, identificando sus similitudes y diferencias con el GDPR y evaluando su efectividad.

Se utilizó el análisis documental para revisar las leyes nacionales de protección de datos, informes de instituciones regulatorias y estudios previos. Además, se analizaron estudios de caso relacionados con filtraciones de datos y violaciones de privacidad en los países seleccionados, para evaluar la respuesta legal ante estos incidentes.

La información recopilada fue interpretada mediante matrices de análisis de contenido, facilitando la comparación de principios clave, derechos de los titulares, requisitos para el tratamiento de datos y sanciones entre las normativas de los tres países y el GDPR. Este análisis permitió identificar patrones y evaluar la efectividad de las leyes de protección de datos en el contexto latinoamericano.

RESULTADOS

Desarrollo y análisis del tema

En la actualidad, el robo de datos personales y las filtraciones masivas de información son problemas cada vez más prevalentes a nivel mundial, generando serias

preocupaciones sobre la privacidad y la seguridad. Los casos ocurridos en Perú, Ecuador y otros países latinoamericanos muestran cómo la falta de protección adecuada y la creciente sofisticación de los cibercriminales han dado lugar a incidentes significativos. La GDPR proporciona un marco normativo con altos estándares de protección de datos, que, aunque es más robusto que las leyes locales en muchos países, pone de manifiesto la necesidad de regulaciones más estrictas a nivel global, especialmente en países con normativas menos desarrolladas.

Un claro ejemplo de la falta de controles adecuados se encuentra en el caso de Ecuador, donde una grave vulnerabilidad expuso la información personal de casi toda la población del país. La filtración fue descubierta cuando se detectó que un servidor utilizado por una empresa de análisis de datos no contaba con los protocolos de seguridad necesarios, permitiendo que los datos fueran accesibles a cualquier persona con conocimientos técnicos básicos (BBC News, 2019)

La filtración de datos en Ecuador no solo evidenció deficiencias técnicas, sino también una falta de cultura organizacional en torno a la protección de datos. La ausencia de políticas claras de seguridad de la información y la falta de capacitación en ciberseguridad contribuyeron a la exposición masiva de datos personales. Además, la respuesta institucional ante el incidente fue insuficiente, lo que generó desconfianza entre los ciudadanos y resaltó la necesidad urgente de fortalecer las capacidades de las autoridades reguladoras en materia de protección de datos personales.

En Perú, el caso de Interbank ilustra, cómo los ciberdelincuentes pueden acceder a datos bancarios mediante el uso indebido de credenciales internas. Un atacante en la red oscura ofreció información de más de 3 millones de clientes del banco, incluidos detalles sobre sus cuentas y transacciones. La vulnerabilidad ocurrió a través de un servidor de New Relic, un proveedor de servicios externos que no aplicó las medidas de seguridad necesarias, y se descubrió que la entidad bancaria no informó adecuadamente a las autoridades competentes sobre el incidente (Cárdenas & Huaman, 2023)

Este caso resalta la falta de supervisión sobre las plataformas de terceros que tienen acceso a datos sensibles, lo que pone en evidencia la fragilidad de las medidas de seguridad que dependen de proveedores externos.

Además, la falta de una respuesta oportuna por parte de Interbank agravó la situación, ya que la falta de transparencia en el manejo del incidente afectó la confianza de los clientes en la entidad financiera. Este incidente pone de manifiesto la necesidad de una mayor responsabilidad en la gestión de proveedores externos y la importancia de implementar auditorías rigurosas y evaluaciones continuas de seguridad. Las instituciones bancarias deben reconocer que la seguridad no solo depende de sus sistemas internos, sino también de la solidez y fiabilidad de los sistemas de terceros con los que interactúan. En este sentido, fortalecer los contratos y acuerdos de seguridad con proveedores externos es crucial para mitigar riesgos y proteger la información de los clientes.

Asimismo, el fenómeno del escaneo de iris por parte de la empresa Worldcoin en Perú generó controversia sobre la recopilación de datos biométricos a cambio de criptomonedas, lo que ha suscitado preguntas sobre la transparencia en el uso de estos datos y las posibles implicaciones legales en un país que cuenta con una legislación de protección de datos personales aún en desarrollo (Arce, 2024)

Por último, el caso de Miraflores en Lima, donde se filtraron los datos de 82.000 vecinos, destaca la falta de controles internos en las administraciones públicas locales para proteger la información de los ciudadanos. La filtración incluyó información sensible como números de DNI, direcciones y datos de contacto, y fue posible debido a la falta de medidas de seguridad adecuadas por parte de la municipalidad (Carrasco Freitas, 2024)

Para entender mejor cómo el GDPR ha influido en las legislaciones de protección de datos en otros países, se presenta un cuadro comparativo de legislación de protección de datos. Este cuadro permite visualizar las similitudes y diferencias clave entre las normativas de protección de datos en Perú, Colombia y Ecuador, así como su relación con el GDPR.

Tabla 1
Cuadro Comparativo de Legislación de Protección de Datos

Aspecto	Perú	Colombia	Ecuador
Normativa Principal	Ley Nº 29733 - Ley de Protección de Datos Personales y su Reglamento (D.S. 003-2013-JUS)	Ley 1581 de 2012 - Régimen General de Protección de Datos Personales	Ley Orgánica de Protección de Datos Personales (2021)
Entidad Reguladora	Autoridad Nacional de Protección de Datos Personales (ANPD)	Superintendencia de Industria y Comercio (SIC)	Superintendencia de Protección de Datos Personales
Ámbito de Aplicación	Aplicable a datos personales en bancos de datos públicos y privados dentro de Perú	Datos personales tratados dentro de Colombia y de ciudadanos colombianos	Datos personales tratados en Ecuador o de ciudadanos ecuatorianos
Principios Fundamentales	Legalidad, consentimiento, seguridad, finalidad y proporcionalidad	Legalidad, finalidad, libertad, veracidad, acceso, seguridad y confidencialidad	Licitud, transparencia, minimización de datos, exactitud, integridad y confidencialidad
Derechos de los Titulares	Acceso, rectificación, cancelación, oposición (ARCO)	Acceso, actualización, rectificación y supresión	Acceso, rectificación, supresión, portabilidad, limitación y oposición

Requisitos para el Tratamiento de Datos	Consentimiento previo, salvo excepciones legales	Consentimiento previo, salvo excepciones legales	Consentimiento expreso, salvo excepciones legales
Transferencia Internacional de Datos	Requiere nivel suficiente de protección o autorización expresa	Requiere medidas adecuadas de seguridad y acuerdos específicos	Exige mecanismos de transferencia con garantías adecuadas
Sanciones por Incumplimiento	Multas de hasta 100 UIT	Sanciones económicas y administrativas (hasta 2,000 SMMLV)	Multas de hasta el 1% de los ingresos del infractor
Inspiración en la GDPR	Sí, especialmente en principios de consentimiento y derechos ARCO	Sí, con influencia en transparencia y responsabilidad proactiva	Sí, con especial énfasis en la portabilidad y seguridad de datos

Nota. Elaboración propia

Exposición de los hallazgos

El robo de datos personales y las filtraciones masivas de información se han convertido en problemas críticos a nivel mundial, afectando tanto a individuos como a organizaciones. En los casos analizados de Perú, Ecuador y otros países latinoamericanos, se observa que la falta de medidas de seguridad adecuadas ha permitido que ciberdelincuentes accedan a datos sensibles. Estos incidentes subrayan la creciente preocupación sobre la privacidad y la seguridad, y muestran la necesidad urgente de mejorar la protección de datos en un mundo cada vez más digitalizado. A pesar de la adopción de marcos regulatorios robustos, como el Reglamento General de Protección de Datos (GDPR) en Europa, la implementación efectiva de estas normativas sigue siendo un desafío en muchas regiones del mundo.

En Ecuador, un ejemplo claro de la falta de controles adecuados se presentó cuando una grave vulnerabilidad expuso la información personal de casi toda la población del país. La filtración se detectó cuando se descubrió que un servidor de una empresa de análisis de datos no tenía los protocolos de seguridad requeridos, lo que permitió que cualquier persona con conocimientos técnicos básicos pudiera acceder a los datos. Este incidente destaca no solo las fallas tecnológicas, sino también las deficiencias en la regulación y la supervisión, lo que facilitó la exposición masiva de datos. Además, muestra la necesidad de una infraestructura digital más robusta y de políticas claras que garanticen la protección de la información a nivel local.

En Perú, el caso de Interbank refleja cómo los ciberdelincuentes pueden aprovechar el uso indebido de credenciales internas para acceder a datos bancarios sensibles. A través de una vulnerabilidad en los sistemas de seguridad de un proveedor externo, New Relic, los atacantes lograron acceder a información de más de 3 millones de clientes del banco. Este incidente resalta la importancia de garantizar que no solo las bases de datos internas sean seguras, sino también las plataformas de terceros que manejan datos sensibles. El caso de Interbank subraya la necesidad de aplicar medidas de seguridad más rigurosas con proveedores externos y de asegurar que las entidades informen de manera adecuada a las autoridades competentes ante cualquier incidente de seguridad.

El fenómeno de Worldcoin en Perú, donde se realizó un escaneo de iris a cambio de criptomonedas, generó controversia sobre la recolección de datos biométricos. Este caso cuestiona la transparencia en el uso de datos sensibles y plantea interrogantes sobre las implicaciones legales en un país donde las leyes de protección de datos aún se encuentran en proceso de desarrollo. La falta de regulaciones claras y la aparición de prácticas que pueden poner en riesgo la privacidad de los individuos pone de manifiesto la necesidad urgente de fortalecer las normativas que protegen los datos personales, especialmente en el contexto de tecnologías emergentes como la biometría.

Finalmente, el caso de la filtración de datos en Miraflores, Lima, demuestra las fallas en la protección de datos en el ámbito público. La filtración afectó a 82.000 vecinos, exponiendo información sensible como números de DNI, direcciones y datos de contacto. Este incidente resalta la necesidad de mejorar la seguridad en las administraciones públicas y de implementar controles internos más estrictos para proteger la información

de los ciudadanos. La falta de medidas de seguridad adecuadas en las entidades públicas refleja una debilidad en las infraestructuras tecnológicas y la gestión de la información, lo que pone en riesgo la privacidad de la población.

En conclusión, los casos analizados evidencian la urgente necesidad de adoptar un enfoque más integral en la protección de datos personales. Esto incluye no solo la mejora de las leyes y regulaciones, sino también el fortalecimiento de las infraestructuras tecnológicas, la educación en ciberseguridad y la colaboración multisectorial entre gobiernos, empresas y ciudadanos. Solo mediante un compromiso conjunto se podrá garantizar una protección eficaz y segura de los datos personales en un entorno digital globalizado.

DISCUSIÓN

Los estudios previos sobre la protección de datos personales en América Latina reflejan las dificultades y desafíos que enfrentan los países en términos de legislación, implementación y cumplimiento de normativas internacionales como el Reglamento General de Protección de Datos (GDPR) de la Unión Europea. En Colombia, García Posada y Rebellón González (2022) concluyeron que, a pesar de los esfuerzos realizados por el país para regular la protección de datos personales, existen vacíos significativos en la Ley General de Protección de Datos de Colombia que dificultan su efectividad. Estos vacíos, junto con el atraso en la legislación, son evidentes cuando se comparan con las actualizaciones frecuentes de la GDPR, lo que deja al país vulnerable en términos de ciberseguridad y protección de datos personales

De manera similar, en Ecuador, Almache, Bustamante y Espinoza (2024) señalan que la Ley Orgánica de Protección de Datos Personales (LOPDP), aunque representa un avance en la alineación con estándares internacionales, enfrenta serias dificultades debido a la falta de regulaciones complementarias, lo que deja espacio para interpretaciones ambiguas. La implementación efectiva de principios clave como el consentimiento informado y el derecho al olvido es un reto en la práctica, reflejando un vacío en la cultura digital y la educación sobre protección de datos.

En el caso de Perú, Auccatoma Gozme (2023) reveló que, a pesar de la mejora progresiva en el marco legal de protección de datos, la Ley de Protección de Datos

Personales sigue siendo insuficiente para reducir las sanciones a las empresas que incumplen la normativa. Las empresas, especialmente en el sector de productos de consumo masivo, continúan siendo las más sancionadas por violaciones de la ley, como la exposición no autorizada de datos personales en sitios web.

Este hallazgo refleja la misma problemática observada en otros países latinoamericanos: la falta de efectividad en la implementación de las leyes existentes, lo que pone en riesgo la protección de los datos personales de los ciudadanos.

Impacto y relevancia en el derecho

El impacto de las normativas de protección de datos en países latinoamericanos es evidente, especialmente en la evolución de las leyes en comparación con las más avanzadas a nivel internacional, como el GDPR. Los estudios previos destacan cómo las leyes de protección de datos en países como Colombia, Ecuador y Perú han avanzado de manera progresiva, pero no lo suficiente como para garantizar una protección efectiva. Esto afecta directamente el derecho a la privacidad de los ciudadanos, que es un derecho fundamental reconocido tanto en la Constitución de Colombia como en las legislaciones ecuatorianas y peruanas.

En este sentido, la falta de un marco regulatorio claro y actualizado, como ocurre en Colombia, y la ausencia de principios clave como el derecho al olvido en la legislación ecuatoriana, disminuyen la efectividad de la protección de datos personales. Esto tiene implicaciones no solo para la seguridad de la información, sino también para la confianza de los ciudadanos en las plataformas digitales y las instituciones encargadas de regular y proteger sus derechos.

La relevancia de este tema también se extiende a nivel global, ya que las violaciones a la privacidad y el robo de datos personales no conocen fronteras. La extraterritorialidad del GDPR, que obliga a las empresas fuera de la UE a cumplir con sus estándares, subraya la necesidad de armonización de las leyes de protección de datos a nivel mundial. La implementación de marcos regulatorios más robustos es esencial para proteger los derechos de los individuos en un entorno digital cada vez más interconectado.

Perspectivas y limitaciones

El análisis realizado indica que, a pesar de los avances legislativos en Colombia, Ecuador y Perú, las principales limitaciones siguen siendo la falta de una implementación efectiva de las leyes, la falta de educación sobre protección de datos y la insuficiente regulación en áreas clave como el derecho al olvido. La perspectiva futura requiere que los países latinoamericanos se alineen más estrechamente con los estándares internacionales, como el GDPR, para garantizar una mayor seguridad y control de los datos personales.

Sin embargo, uno de los mayores retos es la falta de recursos y autonomía de las autoridades de protección de datos en países como Ecuador, que dificultan la supervisión efectiva y la aplicación de sanciones a las entidades incumplidas. La creación de campañas educativas y la sensibilización sobre la importancia de proteger los datos personales son esenciales para fortalecer la legislación existente.

A pesar de estas limitaciones, los estudios también sugieren que los avances en la regulación digital y la protección de datos ofrecen un camino hacia una mayor protección de los derechos individuales, siempre que se tomen medidas preventivas y se refuercen las infraestructuras regulatorias y educativas.

CONCLUSIONES

La implementación del Reglamento General de Protección de Datos (GDPR) ha representado un avance significativo en la protección de la privacidad a nivel global, convirtiéndose en un modelo a seguir para muchos países fuera de la Unión Europea. En América Latina, especialmente en Perú, Colombia y Ecuador, se ha observado un esfuerzo por adaptar las normativas locales a estos estándares internacionales. Sin embargo, las legislaciones nacionales aún enfrentan importantes desafíos para garantizar una implementación efectiva.

Aunque existen avances, como la incorporación de principios clave del GDPR en las leyes locales, se siguen presentando brechas, especialmente en áreas fundamentales como el derecho al olvido y la transferencia internacional de datos. Casos recientes de filtraciones masivas de información en Ecuador y Perú evidencian las deficiencias en la protección de los datos personales, reflejando la necesidad de reforzar las medidas de seguridad tanto en el ámbito público como privado.

A pesar de las sanciones previstas por violaciones de privacidad, la falta de recursos en las autoridades de protección de datos y la insuficiente educación sobre privacidad y seguridad digital limitan la efectividad de las normativas. Es imperativo que los países de la región no solo adopten las leyes de protección de datos, sino que también inviertan en el fortalecimiento de sus infraestructuras regulatorias y educativas.

A futuro, será necesario un compromiso más sólido para alinear las legislaciones locales con los estándares internacionales, con el fin de garantizar una protección más eficaz de los derechos de los ciudadanos en un entorno digital cada vez más complejo. Solo mediante un esfuerzo conjunto entre gobiernos, empresas y ciudadanos se podrá asegurar una mayor seguridad y confianza en el manejo de los datos personales.

Conflicto de interés

Los autores no tienen conflictos de interés

Financiación

Este proyecto no contó con ninguna fuente de financiación

Responsabilidades Éticas

El proyecto fue aprobado por el comité de ética de la institución.

REFERENCIAS

Almache, E. L., Bustamante, J. L., & Espinoza, J. J. (2024). Implementación y desafíos de los principios de la Ley Orgánica de Protección de Datos Personales en Ecuador, Un enfoque de revisión sistemática. *Pro Sciencies: Revista de producción, ciencias e investigación*. https://journalprosciences.com/index.php/ps/article/view/753

Alvear Richards, G. E., & Hernández Pesantes, E. A. (2023). Análisis comparativo de la ley orgánica de protección de datos personales del Ecuador con la legislación peruana desde un enfoque de ciberseguridad y delitos informáticos. *Universidad Politécnica Salesiana*. https://dspace.ups.edu.ec/handle/123456789/25257

Arce, J. (2024, 3 de junio). Fenómeno del escaneo de iris por dinero en el Perú: Las dudas entorno a Worldcoin y por qué ya se le investiga. *Infobae*.

https://www.infobae.com/peru/2024/06/03/fenomeno-del-escaneo-de-iris-por-dinero-en-el-peru-las-dudas-entorno-a-worldcoin-y-por-que-ya-se-le-investiga/

Auccatoma Gozme, E. (2023). Análisis Del Impacto De La Ley De Protección De Datos Personales Del Consumidor Peruano En Empresas Comerciales. *Universidad Peruana de Ciencias e Información*. https://repositorio.upci.edu.pe/handle/upci/744

BBC News. (2019, 16 de septiembre). Filtración de datos en Ecuador: la "grave falla informática" que expuso la información personal de casi toda la población del país sudamericano. https://www.bbc.com/mundo/noticias-america-latina-49721456

Cárdenas, A., & Huaman, G. (2023, 30 de octubre). El negocio ilegal de la información personal: la ruta detrás del robo de datos de Interbank. *Ojo Público*. https://ojo-publico.com/

Carrasco Freitas, M. (2024, 12 de octubre). Filtran datos personales de 82 mil vecinos de Miraflores en portal web ilegal, incluido el alcalde Carlos Canales. *Infobae*. https://www.infobae.com/peru/2024/10/13/filtran-datos-personales-de-82-mil-vecinos-de-miraflores-en-portal-web-ilegal-incluido-el-alcalde-carlos-canales/

Congreso de la República del Perú. (2011, 3 de julio). *Ley N.ª 29733: Ley de protección de datos personales*. https://www.leyes.congreso.gob.pe/documentos/leyes/29733.pdf

Chander, A., & Lê, U. P. (2020). Data Nationalism. *Emory law Journal*, 677-739. https://scholarlycommons.law.emory.edu/elj/vol64/iss3/2/

Ellian, G. R. (2024). El impacto del RGPD en las políticas y prácticas de protección de datos en Ecuador. *Universidad Laica Eloy Alfaro De Manabi*. https://repositorio.uleam.edu.ec/handle/123456789/6426

Francesch, J. L. (2024). Análisis comparativo de la protección de datos y la ciberseguridad. Modelos europeo, americano y chino. *Universidad Autónoma de Barcelona*. https://ddd.uab.cat/record/306209

García Posada, J. D., & Rebellón González, L. I. (2022). La Ley general de protección de datos de Colombia frente al reglamento general de protección de datos de la Unión Europea. *Unidad Central del Valle del Cauca*. https://repositorio.uceva.edu.co/handle/20.500.12993/2833

Kuner, C., Bygrave, L. A., Docksey, C., & Drechsler, L. (2020). *The EU General Data Protection Regulation (GDPR): A Commentary*. Reino Unido: Oxford. https://doi.org/10.1093/oso/9780198826491.001.0001

Noticias de la BBC. (2019, 16 de septiembre). Filtración de datos en Ecuador: la "grave falla informática" que expuso la información personal de casi toda la población del país sudamericano. *BBC Noticias Mundo*. https://www.bbc.com/mundo/noticias-america-latina-49721456

Peña Gutiérrez, M. C. (2022). El principio de finalidad limitada en el reglamento general de datos personales de la Unión Europea y su aplicación en la normativa de datos personales en Chile. *Universidad de Chile*. https://repositorio.uchile.cl/handle/2250/184113

Reglamento General de Protección de Datos. (2024, 10 de febrero). *gdpr-info.eu*. https://gdpr-info.eu/

Tzanou, M. (2017). *The fundamental right to data protection: normative value in the context of counter-terrorism surveillance*. Reino Unido: Oxford. https://cadmus.eui.eu/handle/1814/46835