HORIZON NEXUS JOURNAL
ISSN: 3073-1275

DOSO EDITORIAL CIENTÍFICA

Evolución y desafíos de la protección de datos personales en el contexto de la globalización

Evolution and challenges of personal data protection in the context of globalization

Bonilla-Morejón, Diego Marcelo [1*]; Samaniego-Quiguiri, Delia Paulina [2]

[1] Consejo de la Judicatura, Ecuador, Bolivar; https://orcid.org/0000-0001-5481-151X, diego.bonilla@funcionjudicial.gob.ec
[2] Fiscalía General del Estado, Ecuador, Bolivar; https://orcid.org/0000-0002-2051-3431, samaniegod@fiscalia.gob.ec

* Autor Correspondencia

https://doi.org/10.70881/hnj/v2/n1/34

Cita: Bonilla-Morejón, D. M., & Samaniego-Quiguiri, D. P. (2024). Evolución y desafíos de la protección de datos personales en el contexto de la globalización. *Horizon Nexus Journal*, *2*(1), 62-74. https://doi.org/10.70881/hnj/v2/n1/34.

Recibido: 19/12/2023
Revisado: 29/12/2023
Aceptado: 06/01/2024
Publicado: 31/01/2024

Resumen: La protección de datos personales enfrenta desafíos en un contexto de globalización y digitalización acelerada, donde el intercambio de información a nivel internacional expone a riesgos de privacidad. Este estudio realiza una revisión bibliográfica para analizar la evolución de las normativas de protección de datos, centrada en el impacto del Reglamento General de Protección de Datos (GDPR) de la Unión Europea en diversas regiones. Los métodos incluyen la identificación de normativas inspiradas en el GDPR, adaptadas en países como Brasil y Japón, y el análisis de conflictos entre privacidad y seguridad nacional, donde algunas jurisdicciones priorizan la vigilancia. Los hallazgos muestran que, aunque el GDPR establece un marco regulatorio robusto, su implementación enfrenta limitaciones debido a diferencias culturales, económicas y políticas. En países con menor capacidad regulatoria, como en América Latina y África, los recursos insuficientes obstaculizan una supervisión efectiva. El estudio concluye que la armonización global de las normativas de protección de datos es un desafío pendiente, y destaca la necesidad de un enfoque colaborativo y de infraestructura robusta que permita una protección de datos efectiva y adaptable a los contextos regionales.

Palabras clave: protección de datos; globalización; GDPR; privacidad; vigilancia.

Abstract: The protection of personal data faces challenges in a context of globalization and accelerated digitization, where the international exchange of information exposes privacy risks. This study conducts a literature review to analyze the evolution of data protection regulations, focusing on the impact of the European Union's General Data Protection Regulation (GDPR) in various regions. Methods include identifying GDPR-inspired regulations adapted in countries such as Brazil and Japan, and analyzing conflicts between privacy and national security, where some jurisdictions prioritize surveillance. The findings show that, although the GDPR establishes a robust regulatory framework, its implementation faces limitations due to cultural, economic and political differences. In countries with lower regulatory capacity, such as in Latin America and Africa, insufficient resources hinder effective oversight. The study concludes that global harmonization of data protection regulations is a pending challenge, and highlights the need for a collaborative approach and robust infrastructure to enable effective data protection that is adaptable to regional contexts.

Keywords: data protection; globalization; GDPR; privacy; surveillance.

1. Introducción

En el contexto de la globalización y la digitalización acelerada, la protección de datos personales se ha convertido en una preocupación global que involucra no solo a los individuos, sino también a los gobiernos y empresas en todo el mundo. La libre circulación de datos, impulsada por tecnologías avanzadas y plataformas digitales, permite que la información personal traspase fronteras a una velocidad sin precedentes, generando una serie de desafíos legales y éticos. En particular, la creciente cantidad de datos sensibles compartidos en plataformas digitales ha hecho evidente la necesidad de fortalecer los marcos regulatorios que protejan la privacidad de los individuos y armonicen la normativa a nivel global (Gentimir, 2021; Bagheri & Hassan, 2016).

Uno de los problemas principales en la protección de datos personales radica en las diferencias entre los marcos legales de diversas regiones. Por ejemplo, el Reglamento General de Protección de Datos (GDPR, por sus siglas en inglés) de la Unión Europea ha establecido un estándar global de protección de datos que muchos otros países han adoptado en parte, generando un “efecto Bruselas” que influye en las políticas de otras naciones (Li & Chen, 2024). Sin embargo, los países que adoptan normativas similares al GDPR enfrentan dificultades en su implementación debido a contextos legales y culturales diversos, como es el caso de China y Brasil, que han ajustado sus normativas a sus necesidades internas, creando leyes de protección de datos que difieren en puntos clave, como el derecho a la privacidad frente a la seguridad pública (da Silva et al., 2020; Li & Chen, 2024).

Entre los factores que exacerban estos desafíos se encuentran la falta de armonización legislativa y las tensiones entre la protección de la privacidad y la necesidad de garantizar la seguridad nacional. En este sentido, muchos países enfrentan presiones para flexibilizar sus leyes de privacidad para permitir la vigilancia en áreas como la seguridad nacional y la prevención del crimen, lo que en ocasiones puede llevar a violaciones de derechos fundamentales (Bagheri & Hassan, 2016; Gentimir, 2021). Además, el crecimiento del comercio electrónico y el uso de tecnologías emergentes, como la inteligencia artificial y el Internet de las Cosas, han multiplicado las vías de recopilación y procesamiento de datos personales, lo que dificulta aún más la supervisión y protección efectiva de la información privada (Hamzah et al., 2019).

La justificación de este estudio radica en la necesidad de comprender cómo los distintos enfoques en la protección de datos personales, en especial en el contexto de la globalización, generan ventajas y limitaciones. Dado el impacto del GDPR como modelo de referencia, es fundamental explorar cómo los países no europeos están adoptando, adaptando o resistiendo estos estándares y qué efectos tiene esto en la privacidad de sus ciudadanos. Además, en un escenario donde las amenazas cibernéticas y el acceso no autorizado a la información son comunes, el desarrollo de regulaciones efectivas y universalmente aceptadas resulta crucial para proteger los derechos de los individuos (Gentimir, 2021; Hamzah et al., 2019). Este análisis bibliográfico se vuelve esencial no solo para identificar las brechas actuales en la normativa, sino también para ofrecer una perspectiva crítica sobre la viabilidad de implementar un marco de protección de datos que sea efectivo y adaptable a distintos contextos culturales y legales.

El objetivo de este artículo es realizar una revisión bibliográfica exhaustiva sobre la evolución y los desafíos de la protección de datos personales en el marco de la

globalización, centrándose en la influencia del GDPR en diferentes regiones, especialmente fuera de Europa, y las adaptaciones que se han realizado en respuesta a sus principios. Mediante el análisis de la literatura existente, se busca identificar los elementos que facilitan o dificultan la implementación de normativas de protección de datos efectivas y explorar las tendencias futuras en este campo (Li & Chen, 2024; da Silva et al., 2020). Esta investigación también tiene como fin evaluar cómo los desafíos relacionados con la privacidad y la protección de datos personales afectan a la soberanía nacional y la seguridad, considerando las variaciones en la implementación de políticas y la efectividad de los marcos regulatorios en un mundo cada vez más interconectado.

Este estudio es viable y pertinente, dado que, al concentrarse en una revisión bibliográfica, se tiene acceso a un amplio conjunto de datos secundarios que permiten comprender la evolución y los desafíos de la protección de datos sin necesidad de recolección de datos primarios. Además, este enfoque es ideal para delinear las tendencias y desafíos generales que enfrenta la protección de datos a nivel global, lo que aporta al conocimiento en este ámbito sin incurrir en limitaciones logísticas o éticas significativas (Gentimir, 2021; Hamzah et al., 2019). Con una metodología basada en el análisis crítico de estudios y regulaciones vigentes, este artículo ofrecerá una visión comprensiva sobre los avances y las áreas que aún requieren atención en la protección de datos personales.

2. Materiales y Métodos

La metodología de este estudio se fundamenta en un enfoque de revisión bibliográfica exhaustiva y exploratoria, orientada a analizar de manera integral la evolución y los desafíos de la protección de datos personales en un contexto de globalización acelerada. El carácter exploratorio de esta revisión permite examinar las variaciones normativas y los conflictos ético-legales que emergen al aplicar marcos de protección de datos en diferentes jurisdicciones. Al estar focalizada en una revisión de fuentes secundarias, esta metodología posibilita un análisis descriptivo y comparativo sin necesidad de recolección de datos primarios, lo cual es adecuado para el tipo de estudio propuesto.

Para desarrollar la revisión, se emplearon bases de datos académicas reconocidas como Scopus y Web of Science, priorizando artículos científicos, libros y reportes legales publicados en los últimos cinco años, con el fin de asegurar la actualidad y relevancia de las fuentes. La selección de fuentes fue rigurosa, enfocándose en trabajos que aborden desde perspectivas multidisciplinarias el impacto de las normativas de protección de datos, como el Reglamento General de Protección de Datos (GDPR) de la Unión Europea, y su influencia a nivel global, especialmente en regiones fuera de Europa. Adicionalmente, se incluyeron estudios que exploran el contexto socio-político y cultural de la implementación de estas normativas, para obtener una visión completa y matizada de los desafíos específicos que enfrentan diferentes países en la adaptación de políticas de protección de datos.

El análisis de la información recopilada se realizó mediante técnicas cualitativas de categorización y síntesis de datos. Se organizaron los contenidos en temas clave, tales como la influencia del GDPR en legislaciones de países no europeos, los conflictos entre privacidad de datos y seguridad nacional, las limitaciones en la implementación efectiva de normativas y las particularidades culturales que influyen en la adopción de políticas de privacidad. Para ello, se adoptó un enfoque interpretativo que permitió relacionar conceptos y teorías previas con hallazgos actuales en la literatura, facilitando así una comprensión profunda y crítica del tema en estudio.

El proceso de síntesis incluyó la identificación de patrones comunes, tendencias y vacíos en la legislación de protección de datos a nivel global, permitiendo reconocer áreas que requieren mayor investigación o desarrollo normativo. Además, se evaluaron las tendencias emergentes en políticas de protección de datos, considerando tanto las implicaciones de las normativas vigentes como las direcciones futuras en este ámbito. La metodología adoptada permite no solo describir el estado actual de la legislación sobre protección de datos, sino también reflexionar sobre la viabilidad de un marco regulatorio que responda de forma efectiva a los desafíos derivados de la globalización y la digitalización.

La elección de una metodología de revisión bibliográfica responde a la necesidad de un análisis exhaustivo y detallado sin incurrir en las limitaciones logísticas, éticas o temporales asociadas con la recolección de datos primarios. Al contar con un corpus amplio y diverso de estudios previos, el enfoque metodológico permite establecer conexiones y contrastes entre diferentes enfoques normativos y contextos de aplicación, enriqueciendo el conocimiento en torno a los temas de privacidad y protección de datos personales en el escenario internacional.

3. Resultados

3.1. Influencia del Reglamento General de Protección de Datos (GDPR) en las Normativas Internacionales

El Reglamento General de Protección de Datos (GDPR) ha transformado profundamente el enfoque global hacia la protección de datos, estableciendo un marco que ha sido adoptado, adaptado e interpretado de diversas maneras en diferentes jurisdicciones. Esta influencia se evidencia a través de la adopción de principios clave del GDPR, su adaptación en contextos culturales diversos y los desafíos persistentes en la armonización de las normativas globales.

3.1.1. Adopción de principios de GDPR

La adopción de principios de GDPR en normativas de protección de datos de países no pertenecientes a la Unión Europea representa un fenómeno impulsado por la necesidad de alinearse con los estándares europeos para acceder al mercado de la UE. El GDPR ha establecido principios fundamentales, como el consentimiento explícito, la minimización de datos y el derecho de los usuarios a acceder, rectificar y borrar sus datos. La Ley de Protección de Datos Personales (LGPD) de Brasil es un ejemplo directo de esta adopción, pues incorpora elementos de transparencia y responsabilidad presentes en GDPR, adaptados a la realidad legislativa y social brasileña (GDPR

Advisor, 2021; Pinsent Masons, 2023). Otros países, como Canadá, han revisado sus leyes de protección de datos, como la Ley de Protección de Información Personal y Documentos Electrónicos (PIPEDA), buscando implementar reformas que incorporen elementos de GDPR. Estas reformas incluyen mayores protecciones para los datos de los usuarios y requisitos más estrictos de consentimiento, facilitando así el intercambio de datos entre empresas canadienses y la UE (Pinsent Masons, 2023).

Este proceso ha sido descrito como el "efecto Bruselas", un fenómeno donde las regulaciones europeas se convierten en estándares globales debido a la influencia económica de la UE. Las empresas multinacionales, al cumplir con el GDPR para sus operaciones en Europa, optan por aplicar los mismos estándares a nivel global para simplificar sus prácticas y evitar riesgos legales. Esto ha creado un nuevo estándar de mejores prácticas en la gestión de datos personales, incentivando a legisladores de otros países a adoptar principios similares para facilitar el comercio y la confianza en el mercado global (Cambridge Core, 2020; Privacy International, 2023).

3.1.2. Adaptación en contextos culturales diversos

Sin embargo, la adopción de estos principios no es homogénea. Cada país enfrenta el desafío de adaptar las normas del GDPR a sus propios contextos culturales, jurídicos y económicos. En Estados Unidos, por ejemplo, el enfoque fragmentado de protección de datos a través de leyes sectoriales ha resultado en un sistema que, aunque influido por el GDPR, sigue siendo distinto. La Ley de Privacidad del Consumidor de California (CCPA) es un ejemplo de cómo ciertos estados han incorporado derechos de privacidad inspirados en GDPR, como el derecho al acceso y eliminación de datos personales, aunque sin llegar a una regulación integral como la europea (Privacy International, 2023). Otros estados, como Virginia y Colorado, han desarrollado leyes de privacidad que reflejan principios de GDPR, aunque adaptados a un enfoque menos centralizado y más orientado al control sectorial de datos.

En Asia, Japón ha reformado su Ley de Protección de Información Personal (APPI) para alinearse parcialmente con el GDPR, lo que facilitó un acuerdo de adecuación mutua con la UE en 2019. Esto permite el flujo libre de datos entre Japón y la UE, ilustrando cómo la influencia del GDPR se extiende más allá de Europa y fomenta la cooperación internacional en la protección de datos. Sin embargo, la adecuación implica que Japón ajuste ciertos aspectos de su normativa, adaptándola a su contexto sociocultural sin una copia exacta del GDPR (Pinsent Masons, 2023; GDPR Advisor, 2021).

China, por otro lado, ha desarrollado su propia Ley de Protección de Información Personal (PIPL), inspirada en los principios de GDPR, pero ajustada a las prioridades del gobierno chino en términos de seguridad y control estatal sobre los datos. La PIPL no permite, por ejemplo, el uso de "intereses legítimos" como base legal para procesar datos sin consentimiento explícito, lo que limita la flexibilidad de las empresas en comparación con el GDPR y subraya las diferencias regulatorias influenciadas por la política nacional (Pinsent Masons, 2023). Esta adaptación muestra cómo cada jurisdicción puede integrar los principios de protección de datos con una estructura regulatoria y cultural propia, evitando conflictos de soberanía y facilitando una adopción ajustada a su realidad particular.

3.1.3. Desafíos en la armonización global

La extraterritorialidad del GDPR y su aplicación a empresas y entidades de otros países que manejan datos de ciudadanos de la UE han creado desafíos significativos en términos de armonización global. Aunque el GDPR ha elevado los estándares de privacidad a nivel mundial, su imposición a empresas no europeas ha generado tensiones, especialmente con Estados Unidos, donde el enfoque legislativo hacia la privacidad es menos uniforme y se basa en leyes específicas para cada sector (Cambridge Core, 2020). A pesar de los intentos de algunos estados de adoptar normativas semejantes a GDPR, como la CCPA en California, el país aún carece de una ley federal de protección de datos, lo que dificulta una armonización global.

Esta falta de armonización también se manifiesta en las relaciones comerciales. Los países que desean mantener relaciones comerciales con la UE deben cumplir con las normativas de GDPR, lo que ha llevado a algunos, como India y Australia, a revisar sus leyes de privacidad para alinearse con los estándares europeos, aunque con diferencias significativas que reflejan sus prioridades locales. En Australia, por ejemplo, las revisiones de la Ley de Privacidad de 1988 han incluido propuestas para introducir notificaciones obligatorias de violación de datos y normas de retención que se asemejan al GDPR, pero adaptadas a un enfoque de privacidad basado en principios propios (Pinsent Masons, 2023).

La armonización enfrenta también el desafío de equilibrar la privacidad y la seguridad nacional, ya que algunos países priorizan el control gubernamental sobre los datos en aras de la seguridad, lo que puede entrar en conflicto con los principios de GDPR, especialmente en cuanto al consentimiento y los derechos de los usuarios. Estas diferencias subrayan que, si bien el GDPR ha influido profundamente en las políticas de protección de datos, alcanzar una regulación universal que respete las particularidades locales y permita un flujo de datos seguro y justo sigue siendo un objetivo ambicioso.

3.2. Conflictos entre privacidad de datos y seguridad nacional

El conflicto entre la privacidad de los datos y la seguridad nacional constituye un reto fundamental en el entorno global contemporáneo, donde las amenazas emergentes impulsan a los gobiernos a implementar medidas de vigilancia que, aunque justificadas por razones de seguridad, pueden comprometer los derechos individuales. A continuación, se analizan tres aspectos clave de este conflicto: las excepciones para la vigilancia, las limitaciones al derecho a la privacidad y el debate sobre los “enemigos del Estado”.

3.2.1. Excepciones para la vigilancia

Las leyes de seguridad nacional incluyen excepciones que permiten la vigilancia intensiva, especialmente en contextos de terrorismo y amenazas cibernéticas. Herramientas de vigilancia como el programa PRISM de la Agencia de Seguridad Nacional (NSA) en Estados Unidos, que permite la recolección masiva de datos de comunicaciones, son justificadas bajo la ley de la Foreign Intelligence Surveillance Act (FISA) y se utilizan para interceptar comunicaciones internacionales que puedan cruzar por servidores estadounidenses. Este tipo de programas, que no requieren una orden judicial para interceptar comunicaciones entre extranjeros, son vistos como medidas

necesarias para la protección nacional, aunque generan inquietud por sus implicaciones en los derechos de privacidad de los individuos (Judicature, 2023; OHCHR, 2022).

Estas prácticas de vigilancia masiva a menudo se llevan a cabo bajo una supervisión limitada, ya que los tribunales especializados, como el Tribunal de Vigilancia de Inteligencia Extranjera (FISC) en Estados Unidos, suelen aceptar las solicitudes gubernamentales sin un análisis profundo. Aunque en algunos casos el FISC ha impuesto restricciones para proteger los datos de ciudadanos estadounidenses, la amplia aplicación de estas excepciones crea una tendencia hacia una vigilancia que afecta derechos fundamentales (Judicature, 2023).

3.2.2. Limitaciones en el derecho a la privacidad

El derecho a la privacidad se ve limitado significativamente por el uso de tecnologías avanzadas en la vigilancia estatal, como el reconocimiento facial, los sistemas biométricos y la recolección de datos en espacios públicos y plataformas digitales. La proliferación de cámaras de seguridad, bases de datos biométricas y monitoreo de redes sociales permite a los gobiernos acumular y analizar grandes cantidades de datos, lo que aumenta el riesgo de abuso y erosiona la privacidad de los ciudadanos (OHCHR, 2022). Las naciones justifican estas medidas argumentando su necesidad para prevenir crímenes y asegurar la seguridad pública, pero estas prácticas invaden el espacio privado de las personas y reducen su capacidad para ejercer libremente derechos como la expresión y el acceso a la información (Indique Law Journal, 2023).

La retención masiva de datos también plantea el problema del control estatal sobre la información personal, donde gobiernos con menos controles democráticos pueden usar la vigilancia para monitorizar disidentes, periodistas y activistas, violando los principios básicos de libertad de expresión y de privacidad. Este tipo de limitaciones cuestiona el balance entre el derecho a la privacidad y la seguridad pública, destacando la necesidad de políticas y normas internacionales que establezcan límites claros y salvaguardias efectivas para proteger los derechos humanos (Judicature, 2023; OHCHR, 2022).

3.2.3. Debate sobre los “enemigos del Estado”

El concepto de “enemigos del Estado” se utiliza para justificar la vigilancia de ciertos individuos o grupos considerados amenazas potenciales para la seguridad nacional. Este enfoque permite la identificación y monitoreo de personas en función de su etnia, religión o postura política, lo cual genera preocupaciones sobre discriminación y abuso de poder. Países como India han sido criticados por utilizar sistemas de vigilancia masiva, como el Central Monitoring System (CMS), que centraliza la recolección de datos y permite el monitoreo extensivo de comunicaciones. Este tipo de vigilancia puede derivar en la estigmatización de minorías y en la represión de la disidencia política, socavando la confianza en las instituciones y afectando gravemente los derechos civiles (Indique Law Journal, 2023; OHCHR, 2022).

La categorización de individuos como “enemigos del Estado” no solo cuestiona los principios de igualdad y no discriminación, sino que también establece un precedente peligroso en la legitimación de políticas de vigilancia que impactan negativamente en la cohesión social y en la confianza pública. A nivel internacional, se debate la necesidad de establecer marcos éticos y legales que permitan a los Estados actuar en defensa de

la seguridad sin incurrir en prácticas de vigilancia que discriminen a grupos específicos o afecten sus derechos fundamentales.

3.3. Desafíos en la implementación y cumplimiento de normativas de protección de datos

La implementación y el cumplimiento de las normativas de protección de datos, como el Reglamento General de Protección de Datos (GDPR), presentan desafíos importantes en múltiples contextos y niveles. Estos retos incluyen la falta de recursos adecuados para supervisión, la educación insuficiente en temas de privacidad para los usuarios, y la existencia de prácticas de evasión o elusión normativa que limitan la efectividad de estas leyes. Estos problemas subrayan la necesidad de una infraestructura más robusta y estrategias innovadoras para la aplicación de las normativas, especialmente en un contexto global donde las amenazas a la privacidad evolucionan rápidamente.

3.3.1. Recursos limitados para supervisión

Un problema crítico para las autoridades de protección de datos (DPAs) radica en la falta de recursos humanos y financieros, que dificulta su capacidad para implementar las normativas de manera efectiva. Las DPAs de países en desarrollo suelen tener presupuestos y personal significativamente menores que sus contrapartes en regiones como Europa o América del Norte. Por ejemplo, las DPAs en África y América Latina cuentan con un presupuesto promedio de solo 500,000 USD, comparado con los 58 millones USD en América del Norte. Esto limita su capacidad de supervisión y su independencia funcional, dado que con frecuencia estas autoridades están vinculadas a ministerios gubernamentales, lo que incrementa el riesgo de interferencia política y reduce su capacidad de sancionar a otras instituciones (Center for Global Development, 2021; European Commission, 2020).

Además, esta falta de recursos afecta directamente la capacidad de las DPAs para asesorar a otras entidades en el cumplimiento de las normativas. En muchos casos, las DPAs carecen del personal especializado para asesorar a los entes gubernamentales y empresas en temas complejos, como el uso de tecnologías avanzadas o la implementación de políticas de privacidad en nuevos sectores, lo cual subraya la necesidad de mayor financiamiento y capacitación en estos organismos (European Union Agency for Fundamental Rights, 2020). La Unión Europea ha recomendado incrementar los recursos asignados a las DPAs y desarrollar guías prácticas para el cumplimiento de las normativas, sin embargo, muchos Estados miembros aún enfrentan dificultades significativas para cumplir con estas recomendaciones debido a restricciones presupuestarias (Inside Privacy, 2020).

3.3.2. Educación y concientización del usuario

La falta de educación y concientización entre los usuarios en temas de privacidad constituye otro desafío significativo. Sin un conocimiento adecuado de sus derechos y de las implicaciones del manejo de sus datos, los usuarios no pueden ejercer efectivamente sus derechos ni exigir transparencia a las empresas. Esta situación es particularmente grave en países y regiones donde las leyes de protección de datos son recientes o están poco difundidas, y donde los ciudadanos desconocen los procedimientos para hacer valer sus derechos, como el derecho de acceso, rectificación o eliminación de sus datos personales.

Además, muchos usuarios no son conscientes de las prácticas invasivas de seguimiento y recopilación de datos que ocurren en línea. La implementación de políticas de privacidad claras y de fácil acceso, junto con campañas de concientización masiva, podría fortalecer la percepción pública sobre la importancia de la privacidad de datos y fomentar prácticas de uso seguro de la información personal en plataformas digitales. La Comisión Europea ha subrayado la importancia de fomentar la transparencia y ha propuesto el desarrollo de herramientas educativas para ayudar a los usuarios a comprender mejor sus derechos en el contexto digital (European Commission, 2020).

3.3.3. Evasión y elusión normativa

Un desafío adicional en el cumplimiento de las normativas de protección de datos es la evasión o elusión de estas por parte de las organizaciones. Aunque el GDPR y otros marcos legales establecen sanciones significativas por incumplimiento, muchas empresas encuentran formas de evitar cumplir completamente con las normativas. En particular, las pequeñas y medianas empresas suelen enfrentar dificultades para adaptarse a los complejos requisitos del GDPR, lo que las lleva a priorizar sus intereses económicos sobre las obligaciones de privacidad, utilizando métodos para eludir ciertas disposiciones (European Commission, 2020; Inside Privacy, 2020).

En algunos casos, las empresas intentan evadir la aplicación extraterritorial del GDPR, lo que subraya la necesidad de fortalecer los mecanismos de cooperación internacional y de desarrollar herramientas para facilitar el cumplimiento en distintos contextos legales. En respuesta a estas limitaciones, la Unión Europea ha sugerido la creación de códigos de conducta y herramientas automatizadas que simplifiquen el proceso de cumplimiento para las empresas, especialmente para aquellas que operan en múltiples jurisdicciones y se ven sujetas a diferentes normativas (Inside Privacy, 2020).

En síntesis, los desafíos en la implementación y cumplimiento de las normativas de protección de datos son variados y complejos, y reflejan una necesidad de mayor inversión en recursos, educación pública y mecanismos efectivos para evitar la elusión normativa. Un enfoque integral y colaborativo entre reguladores, empresas y usuarios es esencial para mejorar la protección de datos a nivel global, permitiendo a los usuarios ejercer sus derechos de manera efectiva y asegurando que las empresas cumplan con sus obligaciones de privacidad.

4. Discusión

La implementación y el cumplimiento de las normativas de protección de datos en el contexto global presenta una serie de desafíos que resaltan tanto las limitaciones estructurales de las autoridades reguladoras como las dificultades en promover una cultura de privacidad robusta y efectiva. A pesar de que el Reglamento General de Protección de Datos (GDPR) ha impulsado un cambio paradigmático en el ámbito de la protección de datos personales, su implementación práctica ha puesto de manifiesto limitaciones sustanciales, derivadas en gran medida de la disparidad en recursos, la falta de concientización pública y la frecuente elusión de sus disposiciones por parte de organizaciones que operan a nivel internacional (Center for Global Development, 2021; European Union Agency for Fundamental Rights, 2020).

Un factor crucial en la dificultad de implementación efectiva del GDPR y otras normativas similares radica en los recursos limitados de las autoridades de protección de datos (DPAs), particularmente en regiones con menores presupuestos y capacidad institucional. Estudios revelan que mientras las DPAs en Europa cuentan con financiamientos significativos, sus contrapartes en países de ingresos bajos y medianos suelen operar con un personal reducido y un presupuesto limitado, lo cual afecta su capacidad para supervisar y hacer cumplir las normativas de manera exhaustiva (European Commission, 2020; Center for Global Development, 2021). Estas limitaciones de recursos no solo comprometen la efectividad regulatoria, sino que también dificultan la independencia de las DPAs frente a presiones políticas, limitando su capacidad para actuar imparcialmente en la vigilancia del cumplimiento de la normativa (European Union Agency for Fundamental Rights, 2020).

Además de las limitaciones estructurales, la falta de concientización entre los usuarios sobre sus derechos de privacidad representa un obstáculo significativo para el cumplimiento de las normativas. Sin una comprensión clara de sus derechos y de las obligaciones de las empresas respecto a la gestión de datos personales, los usuarios no pueden ejercer plenamente sus prerrogativas, lo cual limita la efectividad de las normativas en la práctica. La Comisión Europea ha señalado la necesidad de mejorar la educación pública en torno a la privacidad de los datos, recomendando campañas informativas y la elaboración de políticas de privacidad accesibles y claras. La falta de concientización no solo afecta a los individuos, sino que también expone a las empresas al incumplimiento, ya que la complejidad de los requisitos legales aumenta el riesgo de errores no intencionados o de prácticas negligentes en la gestión de datos.

Otro desafío relevante se relaciona con la evasión y elusión normativa, un fenómeno que ha adquirido relevancia en los últimos años debido a la aplicación extraterritorial del GDPR. Aunque el GDPR establece sanciones significativas para quienes no cumplen con sus disposiciones, muchas empresas, especialmente aquellas con operaciones en múltiples jurisdicciones, intentan eludir las regulaciones mediante prácticas que minimizan su responsabilidad legal o trasladan sus operaciones de tratamiento de datos a ubicaciones donde las normativas son menos estrictas (Inside Privacy, 2020; European Commission, 2020). Este comportamiento evasivo destaca la necesidad de una mayor cooperación internacional y de acuerdos bilaterales que refuercen el cumplimiento transnacional, además de fortalecer los mecanismos de supervisión y sanción para disuadir la elusión normativa.

En conjunto, estos factores resaltan que, si bien las normativas de protección de datos como el GDPR han establecido un marco robusto y detallado para la protección de la privacidad en la era digital, su efectividad depende en gran medida de las capacidades locales de implementación y de una cultura de privacidad que trascienda las disposiciones legales formales. Sin un apoyo adecuado en términos de recursos, educación pública y cooperación internacional, la normativa enfrenta serias limitaciones para alcanzar su potencial de protección integral y universal de la privacidad de los individuos. Es evidente que se requiere un enfoque colaborativo que integre esfuerzos entre gobiernos, sector privado y sociedad civil, buscando construir una infraestructura regulatoria que esté a la altura de los desafíos tecnológicos y globales de la protección de datos en el siglo XXI.

5. Conclusiones

En conclusión, la implementación y el cumplimiento de normativas de protección de datos como el Reglamento General de Protección de Datos (GDPR) presentan múltiples desafíos complejos, especialmente en un contexto global donde las capacidades de los países y la comprensión pública sobre estos derechos varían significativamente. La falta de recursos adecuados para las autoridades de protección de datos limita su capacidad para supervisar y sancionar efectivamente a quienes incumplen las normativas, destacando la necesidad urgente de fortalecer la infraestructura de supervisión y aumentar la inversión en recursos humanos y financieros.

Además, la insuficiente concientización de los usuarios sobre sus derechos y sobre las prácticas de privacidad necesarias para proteger sus datos personales sigue siendo un obstáculo crítico. Sin una educación efectiva, los usuarios no pueden exigir responsabilidad ni tomar decisiones informadas sobre su información personal, lo que debilita la efectividad de las normativas de protección de datos y dificulta el cumplimiento normativo a nivel organizacional. La educación pública y la transparencia de las políticas de privacidad son, por lo tanto, esenciales para construir una cultura sólida de privacidad.

Por otro lado, la evasión y elusión de las normativas de protección de datos son prácticas que persisten debido a la complejidad de los requisitos regulatorios y a las dificultades de aplicar sanciones transnacionales. Estas prácticas subrayan la importancia de una cooperación internacional más estrecha y de la creación de acuerdos que fortalezcan el cumplimiento extraterritorial de normativas como el GDPR. La implementación de códigos de conducta globales y el uso de herramientas de automatización pueden ser estrategias efectivas para facilitar el cumplimiento, especialmente para pequeñas y medianas empresas que enfrentan mayores desafíos en este aspecto.

En conjunto, estos factores sugieren que, aunque las normativas actuales representan un avance significativo en la protección de datos, su efectividad depende de un enfoque integral que combine recursos adecuados, una educación pública sólida y una cooperación global. Solo mediante una infraestructura reguladora fortalecida y una cultura de respeto a la privacidad podrá alcanzarse una protección de datos que responda a los desafíos complejos de la era digital.

Referencias Bibliográficas

Arcos-Chaparro, I. A., & Epia-Silva, M. A. (2024). La transverzalización del debido proceso en las relaciones laborales particulares. *Journal of Economic and Social Science Research*, *4*(2), 17–43. https://doi.org/10.55813/gaea/jessr/v4/n2/100

Bagheri, P., & Hassan, K. H. (2016). Data Privacy in Electronic Commerce: Analysing Legal Provisions in Iran. Journal of Politics and Law, 9(7), 133. https://doi.org/10.5539/jpl.v9n7p133

Barahona-Martinez, G. E., Barzola-Plúas, Y. G., & Peñafiel-Muñoz, L. V. (2024). El Derecho a la Protección de Datos y el Avance de las Nuevas Tecnologías en Ecuador: Implicaciones Legales y Éticas. *Journal of Economic and Social Science Research*, *4*(3), 46–64. https://doi.org/10.55813/gaea/jessr/v4/n3/113

Barzola-Plúas, Y. G. (2022). Reformas Constitucionales en Ecuador: Impacto y Perspectivas. *Revista Científica Zambos*, *1*(1), 86-101. https://doi.org/10.69484/rcz/v1/n1/23

Bonilla-Morejón, D. M. (2023). Derecho Penal y Políticas de Seguridad en Ecuador: Análisis de la Eficacia. *Revista Científica Zambos*, *2*(3), 59-74. https://doi.org/10.69484/rcz/v2/n3/50

Bonilla-Morejon, D. M., Bonilla-Morejón, J. S., Guano-Fogacho, J. E., Meléndez-Carrasco, P. V., Murillo-Ramos, F. R., Peña-Chauvín, S. M., Samaniego-Quiguiri, D. P., Solis-Miranda, D. F., Vásquez-Quinatoa, L. H., & Núñez-Ribadeneyra, R. A. (2023). *Los gritos silenciosos de las víctimas de violencia de género: Un enfoque desde la perspectiva pre procesal y procesal penal en el Ecuador.* Editorial Grupo AEA. Retrieved from. Editorial Grupo AEA. https://doi.org/10.55813/egaea.l.2022.41

Bonilla-Morejón, D. M., Samaniego-Quiguiri, D. P., & Paredes-Fierro, E. J. (2023). Los Derechos Humanos y su enfoque en las poblaciones vulnerables. In *Sinergia Científica: Integrando las Ciencias desde una Perspectiva Multidisciplinaria* (pp. 15–48). Editorial Grupo AEA. https://doi.org/10.55813/egaea.cl.2022.21

Cambridge Core. (2020). The GDPR as Global Data Protection Regulation?. American Journal of International Law. https://www.cambridge.org/core/journals

Center for Global Development. (2021). Why Data Protection Matters for Development: The Case for Strengthening Inclusion and Regulatory Capacity.

Erazo-Luzuriaga, A. F. (2023). Uso de la minería de datos para la prevención de fraudes en el sector financiero. *Horizon Nexus Journal*, *1*(1), 63-76. https://doi.org/10.70881/hnj/v1/n1/13

Estrada-Ayre, C. P., & Porras-Sarmiento, S. (2023). *Peculado Doloso y el Principio de Proporcionalidad de la Pena*. Editorial Grupo AEA. https://doi.org/10.55813/egaea.l.2022.32

European Commission. (2020). 2-Year Report on the Implementation of the GDPR. https://doi.org/10.1145/3389685

European Union Agency for Fundamental Rights. (2020). GDPR in practice – Experiences of data protection authorities.

García Moreno, M., & Vargas Fonseca, A. D. (2023). Restitución de derechos territoriales y ordenamiento ambiental en territorios étnicos en Colombia. *Journal of Economic and Social Science Research*, *3*(3), 76–96. https://doi.org/10.55813/gaea/jessr/v3/n3/74

GDPR Advisor. (2021). How GDPR is Shaping Global Data Protection Policies Beyond the EU. https://www.gdpr-advisor.com

Gentimir, A. (2021). Protection of Personal Data: Intricate Challenge of the Right to Privacy in Era of Globalization. Legal Appraisal, 37LAW (2021). https://ibimapublishing.com/articles/LAW/2021/37185321/

Guerrero-Velástegui, C. A. (2023). *Entorno Empresarial desde la Gestión del Derecho Laboral: Breves Apuntes desde una Perspectiva Académica. Editorial Grupo AEA.* https://doi.org/10.55813/egaea.l.2022.42

Hamzah, M. A., Ahmad, A. R., Hussin, N., & Ibrahim, Z. (2019). Personal Data Privacy Protection: A Review on Malaysia's Cyber Security Policies. International Journal of Academic Research in Business and Social Sciences, 8(12). https://doi.org/10.6007/ijarbss/v8-i12/5251

Indique Law Journal. (2023). Conflict and Scope of Fundamental Right to Privacy https://www.ilawjournal.org

Judicature. (2023). National Security. Civil Liberties. Can We Have Both?. https://judicature.duke.edu

Li, W., & Chen, J. (2024). From Brussels Effect to Gravity Assists: Understanding the Evolution of the GDPR-Inspired Personal Information Protection Law in China. Computer Law & Security Review, 54. https://doi.org/10.1016/j.clsr.2024.105994

Mendoza-Armijos, H. E. (2023). Desafíos jurídicos en el marco del derecho marítimo y la protección de los recursos oceánicos. *Horizon Nexus Journal*, *1*(3), 57-69. https://doi.org/10.70881/hnj/v1/n3/24

Núñez-Ribadeneyra, R. A. (2023). Derechos Humanos y Justicia Social en el Contexto Ecuatoriano. *Revista Científica Zambos*, *2*(3), 42-58. https://doi.org/10.69484/rcz/v2/n3/49

OHCHR. (2022). Spyware and surveillance: Threats to privacy and human rights growing. https://www.ohchr.org

Pinsent Masons. (2023). International impact of the GDPR felt five years on. https://www.pinsentmasons.com

Samaniego Quiguiri, D. P., Bonilla-Morejón, D. M., Martínez-Tapia, J. D., Navarrete-Valladolid, M. I., Solis-Miranda, D. F., Zambrano-Villacrés, D. E., Bucheli-Cárdenas, C. M., Murillo-Ramos, F. R., Erazo-Zela, V. H., & Guala-Agualongo, C. J. (2023). *El derecho a ser padres: Rompiendo los paradigmas del derecho de familia, bajo una concepción legal o ilegal.* Editorial Grupo AEA. https://doi.org/10.55813/egaea.l.2022.51

Samaniego-Quiguiri, D. P. (2023). Acceso a la Justicia y Equidad en el Sistema Legal Ecuatoriano. *Revista Científica Zambos*, *2*(2), 50-62. https://doi.org/10.69484/rcz/v2/n2/45

Silva, M. V. V., Scherf, E. D. L., & Da Silva, J. E. (2020). The Right to Data Protection versus "Security". Revista Direitos Culturais, 15(36), 209-232.

Vargas-Fonseca, A. D., Borja-Cuadros, O. M., & Cristiano-Mendivelso, J. F. (2023). *Estructura Ecológica Principal de la Localidad de Engativá: Estudio desde una perspectiva de ordenamiento territorial y sus instrumentos jurídicos.* Editorial Grupo AEA. https://doi.org/10.55813/egaea.l.2022.38

CONFLICTO DE INTERESES

"Los autores declaran no tener ningún conflicto de intereses".