Tipo de artículo: Artículo original

La afectación del derecho de oposición y el consentimiento informado en el proceso de entrega de datos personales en plataformas bancarias en Ecuador

The impact on the right to object and informed consent in the process of providing personal data on banking platforms in Ecuador

Jean Carlos Pardo Zhingri [1*], **https://orcid.org/0009-0007-3825-9455**
Johanna Irene Escobar Jara [2], **https://orcid.org/0000-0002-9053-8060**
Duniesky Alfonso Caveda [3], **https://orcid.org/0000-0001-7889-8066**

[1] Maestrante, Universidad Bolivariana del Ecuador (UBE). Ecuador. Correo electrónico: jcpardoz@ube.edu.ec
[2] Docente, Universidad Bolivariana del Ecuador (UBE). Ecuador. Correo electrónico: jiescobarj@ube.edu.ec
[3] Docente, Universidad Bolivariana del Ecuador (UBE). Ecuador. Correo electrónico: dalfonsoc@ube.edu.ec

*** Autor para correspondencia: jcpardoz@ube.edu.ec**

Resumen

La protección de datos personales está constituida por un conjunto de normas y prácticas que se implementan para salvaguardar la privacidad y la seguridad de la información personal de los individuos. Las empresas que recopilan, procesan y utilizan datos personales deben cumplir con la legislación sobre privacidad de datos. Una Ley de Protección de Datos se refiere a la legislación que tiene como objetivo salvaguardar los datos personales, garantizar la privacidad y establecer pautas para el procesamiento legal de datos por parte de las organizaciones. En mayo de 2021, Ecuador aprobó la Ley Orgánica de Protección de Datos Personales (LOPDP), marcando un hito significativo en la protección de la privacidad y los datos personales en el país, sin embargo, la implementación efectiva de esta ley enfrenta algunos desafíos, como es el caso de la implementación en las plataformas bancarias de dicho país. En esta investigación se estableció como objetivo proponer una modificación al artículo 16 de la LOPDP, que exprese las condiciones para ejercer el derecho de oposición en el manejo de datos personales de las plataformas bancarias. La propuesta se sustentó en un análisis integral que abarcó diversas dimensiones, incluyendo la revisión de las normativas vigentes. Este estudio comparativo permitió identificar las mejores prácticas en la protección de datos personales, especialmente en el ámbito bancario, donde la seguridad de la información es fundamental. Además, se incorporaron los resultados de encuestas y entrevistas a expertos en materia técnica y legal, quienes señalaron las limitaciones de la legislación actual y la necesidad de adaptarla a todos los escenarios posibles. La propuesta de modificación fue validada mediante criterio de expertos, con un alto por ciento de aceptación.

Palabras clave: Protección de Datos Personales; gestión de la información; plataformas bancarias; privacidad de los datos

Abstract

Personal data protection is made up of a set of rules and practices that are implemented to safeguard the privacy and security of individuals' personal information. Companies that collect, process, and use personal data must comply with data privacy legislation. A Data Protection Law refers to legislation that aims to safeguard personal data, ensure privacy, and establish guidelines for the lawful processing of data by organizations. In May 2021, Ecuador approved the Organic Law on Personal Data Protection (LOPDP), marking a significant milestone in the protection of privacy and personal data in the country. However, the

effective implementation of this law faces some challenges, such as the implementation in banking platforms in that country. This research aimed to propose a modification to article 16 of the LOPDP, which expresses the conditions for exercising the right to object in the handling of personal data by banking platforms. The proposal was based on a comprehensive analysis that covered various dimensions, including the review of current regulations. This comparative study allowed us to identify the best practices in the protection of personal data, especially in the banking sector, where information security is essential. In addition, the results of surveys and interviews with experts in technical and legal matters were incorporated, who pointed out the limitations of current legislation and the need to adapt it to all possible scenarios. The proposed modification was validated by expert criteria, with a high percentage of acceptance.

Keywords: *Personal Data Protection; information management; banking platforms; data privacy*

Recibido: 17/06/2024
Aceptado: 1/09/2024
En línea: 03/09/2024

Introducción

La era digital puede describirse como un conjunto de diferentes soluciones tecnológicas, como entornos virtuales, servicios digitales, aplicaciones inteligentes, aprendizaje automático, sistemas basados en el conocimiento, que determinan las características específicas de las comunicaciones electrónicas, el intercambio de información y la virtualización (Romansky & Noninska, 2020). Sin embargo, existe la posibilidad de que las tecnologías de la era digital violen algunos principios básicos de la seguridad de la información y la privacidad, mediante el acceso no regulado a la información y los datos personales almacenados en diferentes nodos de la red global (Mantelero, 2016). La jurisprudencia y la normativa vigentes no son suficientes para abordar los posibles riesgos y problemas relacionados con este cambio de paradigma en la era digital.

El rápido desarrollo tecnológico debido a la convergencia del progreso de la potencia de cálculo, el aumento de la capacidad de almacenamiento y la tecnología avanzada de redes hace posible que las empresas recopilen, procesen e interconecten datos de una manera ampliada (Tikkinen-Piri et al., 2018). Cada vez más, tienden a utilizar estos datos para diversos fines, como servicios personalizados y marketing. Como resultado del desarrollo tecnológico, junto con la globalización, han surgido nuevos y mayores desafíos para la protección de datos personales.

La protección de datos personales está constituida por un conjunto de normas y prácticas que se implementan para salvaguardar la privacidad y la seguridad de la información personal de los individuos (De Hert & Papakonstantinou, 2016). En este contexto, se enfatiza la importancia del consentimiento explícito de los individuos para la recopilación y el procesamiento de sus datos. Además, se establece que los datos deben ser recolectados con fines específicos y legítimos, limitándose a la información necesaria y asegurando su precisión y actualización. La protección de datos también implica la implementación de medidas de seguridad adecuadas para prevenir el acceso no autorizado y la pérdida de información, garantizando así la integridad y confidencialidad de los datos personales (Van Dijk et al., 2018).

Las empresas que recopilan, procesan y utilizan datos personales deben cumplir con la legislación sobre privacidad de datos. Una Ley de Protección de Datos se refiere a la legislación que tiene como objetivo salvaguardar los datos personales, garantizar la privacidad y establecer pautas para el procesamiento legal de datos por parte de las organizaciones (van Loenen et al., 2016).

En el Ecuador, se ha realizado en los últimos cinco años, la introducción de derechos de nuevas tecnologías que conllevan a la protección de datos tanto de forma análoga como digital. Al ser un tiempo reducido en el que se están dando estas prácticas, tiene como consecuencias el desconocimiento de la población sobre sus derechos dentro de la sociedad del conocimiento y la arbitrariedad de ciertas entidades para forzar el tratamiento de los datos personales en procesos que no son necesarios utilizarlos.

En mayo de 2021, Ecuador aprobó la Ley Orgánica de Protección de Datos Personales (LOPDP), marcando un hito significativo en la protección de la privacidad y los datos personales en el país (Ochoa et al., 2024), sin embargo, la implementación efectiva de esta ley enfrenta algunos desafíos como la falta de concienciación pública, la insuficiente infraestructura tecnológica, y la necesidad de fortalecer las capacidades regulatorias y de cumplimiento. En 2024, implementar todos los requisitos regulatorios para dar cumplimiento de forma eficaz al tratamiento de datos personales de la población ecuatoriana, se ha vuelto un desafío al momento de aplicar la normativa.

En esta investigación se analiza en forma particular, la práctica de las compañías bancarias en Ecuador, las cuales solicitan amplias autorizaciones para el manejo de datos personales, sin permitir a los clientes seleccionar cuáles datos desean compartir, lo que resulta en una invasión de la privacidad y en una gestión de datos que no cumple con los principios de minimización y proporcionalidad. En este sentido, es necesario evaluar las políticas de manejo de datos personales de las compañías bancarias en Ecuador; y analizar cómo estas afectan la privacidad de los clientes, así como la limitación del ejercicio de los derechos de oposición y de consentimiento informado (Fuel Rodríguez, 2024).

El derecho de oposición es aquel que permite garantizar la privacidad e integridad de los datos personales, lo que refuerza el control sobre la información sensible que le concierne al titular (Contreras & Felipe, 2020). Este derecho es esencial para proteger la intimidad de los usuarios, ya que permite a los individuos oponerse al uso no autorizado de sus datos en las plataformas digitales dando como resultado la prevención de violaciones a su privacidad. De este modo, el derecho de oposición es parte de un marco amplio que busca salvaguardar los derechos de los titulares frente a la circulación ilimitada de datos por lo que se vuelve un mecanismo para que los individuos puedan controlar el uso que se da a su información personal en un contexto digitalizado (Hondares et al., 2021).

El derecho de oposición es mencionado dentro de la Ley Orgánica de Protección de Datos Personales, el cual indica que el titular tiene derecho a oponerse o negarse al tratamiento de sus datos personales siempre que no se violenten

derechos de terceros, no se trate de información pública o que tenga por objeto la comercialización de productos o servicios.

Para llegar a invocar el derecho de oposición, en primer lugar, tiene que existir la manifestación del consentimiento informado, el cual se define como una declaración expresa y afirmativa por parte del titular, que manifiesta su acuerdo específico e inequívoco para el tratamiento de sus datos personales conforme a los principios de transparencia y responsabilidad (Zanfir-Fortuna & Ianc, 2022). El consentimiento informado debe ser específico, explícito, y otorgado de forma voluntaria, asegurando que el individuo esté consciente a plenitud de las implicaciones de su decisión de permitir el tratamiento de sus datos. Es importante que los ciudadanos comprendan que el consentimiento informado implica la comprensión clara y la aceptación voluntaria por parte del individuo de los propósitos, riesgos y beneficios del tratamiento de sus datos personales, asegurando que dicho consentimiento no sea ambiguo ni coaccionado.

Una vez analizados estos supuestos teóricos y continuando con el objeto de estudio, las entidades bancarias de Ecuador tienen políticas de tratamiento de datos debatibles, porque dentro de sus pliegos de términos y condiciones existen cláusulas de entrega voluntaria para el tratamiento de los datos personales para acceder a los servicios de canales de acceso electrónico, en donde el titular autoriza que sus datos puedan ser utilizados para uso de mercadotecnia donde puedan publicitar sus servicios y a la vez, el delegado puede transferir a terceros los datos para servicios de publicidad, incumpliendo con el artículo 16 numeral 2 de la Ley Orgánica de Protección de Datos Personales (LOPDP, 2021).

Sin embargo, dentro de las pautas que se expresan en los pliegos de las entidades bancarias, se especifica que si no se da la autorización para el dar ese tipo de tratamiento a los datos personales, no podrá funcionar de forma correcta los canales electrónicos de las entidades bancarias y, solo en el caso de oposición, primero hay que aceptar los términos y condiciones para luego acercarse a la entidad bancaria y solicitar el ejercicio de sus derechos de oposición y no ser objeto de decisiones automatizadas, lo que resulta en un proceso innecesario si tan solo desde el comienzo se le diera oportunidad al titular para elegir las condiciones que autoriza para el tratamiento de sus datos y las que se niega a aceptar.

Los sistemas de autorización dentro de las plataformas bancarias no son amigables porque muestran un documento extenso de letras pequeñas sin opciones de elección de cláusulas que el titular quiere aceptar y solo te permiten acceder a la plataforma de servicios en línea cuando aceptes todas sus condiciones; esto ocasiona una coacción al derecho de consentir de forma libre y voluntaria al tratamiento de datos personales lo que vulnera la privacidad (de Marcos, 2023).

En Ecuador, los principales bancos tienen una distribución significativa en el mercado de clientes. Según los datos recientes, Banco Pichincha sigue siendo el líder del mercado, con una participación considerable, siendo el banco más grande del país en términos de activos y número de clientes ya que tiene una ventaja notable en el mercado ecuatoriano,

le sigue Banco del Pacífico el cual ha mostrado un crecimiento sólido, alcanzando un nuevo récord de utilidades en 2024, lo que lo coloca como un fuerte competidor, incrementando su presencia en el mercado. Este crecimiento podría traducirse en una mayor cuota de mercado en términos de clientes y Banco Guayaquil también mantiene una posición sólida, siendo el tercer banco más grande del país en términos de activos. Su participación en el mercado se mantiene estable, con un enfoque en la diversificación de su portafolio de préstamos y productos financieros.

Estas tres entidades tienen en común canales electrónicos para que los usuarios accedan a servicios en línea donde puedan revisar sus cuentas bancarias, realizar transferencias de dinero a otros usuarios y otros procesos como pagos de servicios, tarjetas de crédito, pólizas o cuentas de ahorros flexibles, lo que resulta atractivo para la clientela porque les permite acceder a los servicios bancarios de su interés desde la comodidad de su hogar o establecimiento dando como resultado el ahorro de tiempo y ayuda a agilitar los procesos, sin embargo; cuando se instala las aplicaciones bancarias, lo primero que tienen que otorgar es el consentimiento de aceptación del tratamiento de datos personales, es aquí cuando se manifiesta el problema, ya que el pliego contiene cláusulas amplias del uso de los datos personales lo que les da autoridad a los responsables de hacer uso de los mismos a discrecionalidad del banco.

Problema de la investigación

La manifestación del problema proviene de la falta de cumplimiento con el artículo 16 numeral 2 de la Ley Orgánica de Protección de Datos Personales de Ecuador, la cual manifiesta el derecho de oposición en el caso de utilizar sus datos personales para mercadotecnia directa. Los tres bancos mencionados tienen estipulaciones de cómo van a tratar los datos y entre ellas expresan que, el titular entrega de forma voluntaria sus datos para el uso de publicidad tanto de sus servicios de la entidad y a la vez, entregar a terceros los datos para que puedan desarrollar perfiles automatizados donde se pueda realizar ofertas de productos y servicios.

Aunque es una violación flagrante, los bancos se protegen a través de otras cláusulas explicativas que indican que si no se acepta los términos que estipulan para el tratamiento de datos no pueden brindar el servicio de los canales electrónicos con la excusa de que no se ejecutarán de manera eficaz, lo que obliga al titular de los datos a acceder de forma coercitiva a la aceptación del tratamiento de sus datos a la conveniencia de la entidad bancaria. Además, dentro de ese documento, dan la salida de que, si uno no está conforme con el tratamiento de datos, puede direccionarse a la entidad bancaria para ejercer su derecho de oposición, pero para ello; se puede evitar desde el inicio si dieran acceso a elegir la forma en que el titular quiere que sus datos sean tratados.

Con el desarrollo del sustento teórico, surge la siguiente pregunta de investigación: ¿Qué impacto tiene la afectación del derecho de oposición y el consentimiento informado en el proceso de entrega de datos personales en las plataformas bancarias en Ecuador? A partir de la formulación del problema, se establece como objetivo general lo siguiente:

Proponer una modificación al artículo 16 de la Ley Orgánica de Protección de Datos Personales del Ecuador que exprese las condiciones para ejercer el derecho de oposición.

Materiales y métodos

Este estudio es una investigación jurídica. El enfoque de investigación utilizado fue el enfoque comparativo y el enfoque estatutario. Los materiales jurídicos utilizados son todas las regulaciones sobre protección de datos personales que se aplican en Ecuador. La técnica de recopilación de materiales jurídicos se realiza mediante técnicas de investigación bibliográfica para comparar la Ley Orgánica de Protección de Datos Personales del Ecuador con las normativas de España, Reino Unido y otros países de la región sudamericana.

En esta investigación se seguirá la metodología propuesta en la figura 1, la cual permite abordar el tema de la protección de datos personales desde tres perspectivas integrales. En primer lugar, desde la perspectiva legal, se centrará en analizar el marco normativo actual para garantizar la protección de los datos personales. Esto implica la recopilación de información sobre las leyes y regulaciones aplicables en Ecuador, España, Reino Unido y Sudamérica, para realizar un análisis comparado e identificar los estándares legales existentes y las áreas que requieren mejoras.

La perspectiva técnica se enfoca en la seguridad de los datos, evaluando las medidas y prácticas de seguridad implementadas en diversas organizaciones, especialmente en instituciones bancarias. Se analiza la eficacia de dichas prácticas y las tecnologías disponibles que puedan contribuir a un mejor resguardo de la información personal y sensible de los usuarios.

Finalmente, la metodología considera la perspectiva subjetiva, donde el análisis se centra en las inquietudes y percepciones del usuario final. Se realizarán encuestas e entrevistas que se centran en conocer el conocimiento factual de los usuarios sobre la protección de sus datos, sus preocupaciones relacionadas con la seguridad y la privacidad, así como su sensación de control sobre la información personal. También se exploran factores como la confianza y la percepción del riesgo, junto con los antecedentes culturales que pueden influir en su comportamiento respecto a la gestión de datos personales.

El enfoque empírico de la metodología consta de tres pasos fundamentales. En el paso 1, se realiza una conceptualización y definiciones legales y técnicas en los contextos mencionados, que servirán como base para el análisis posterior. En el paso 2, se realizará un análisis exhaustivo de políticas y procedimientos utilizados en las instituciones bancarias para el tratamiento de datos personales, buscando identificar posibles deficiencias o áreas de mejora. Por último, en el paso 3, se llevarán a cabo encuestas y entrevistas dirigidas a expertos en la perspectiva técnica y legal, con el fin de obtener información valiosa y comprensiva que complemente las etapas anteriores.

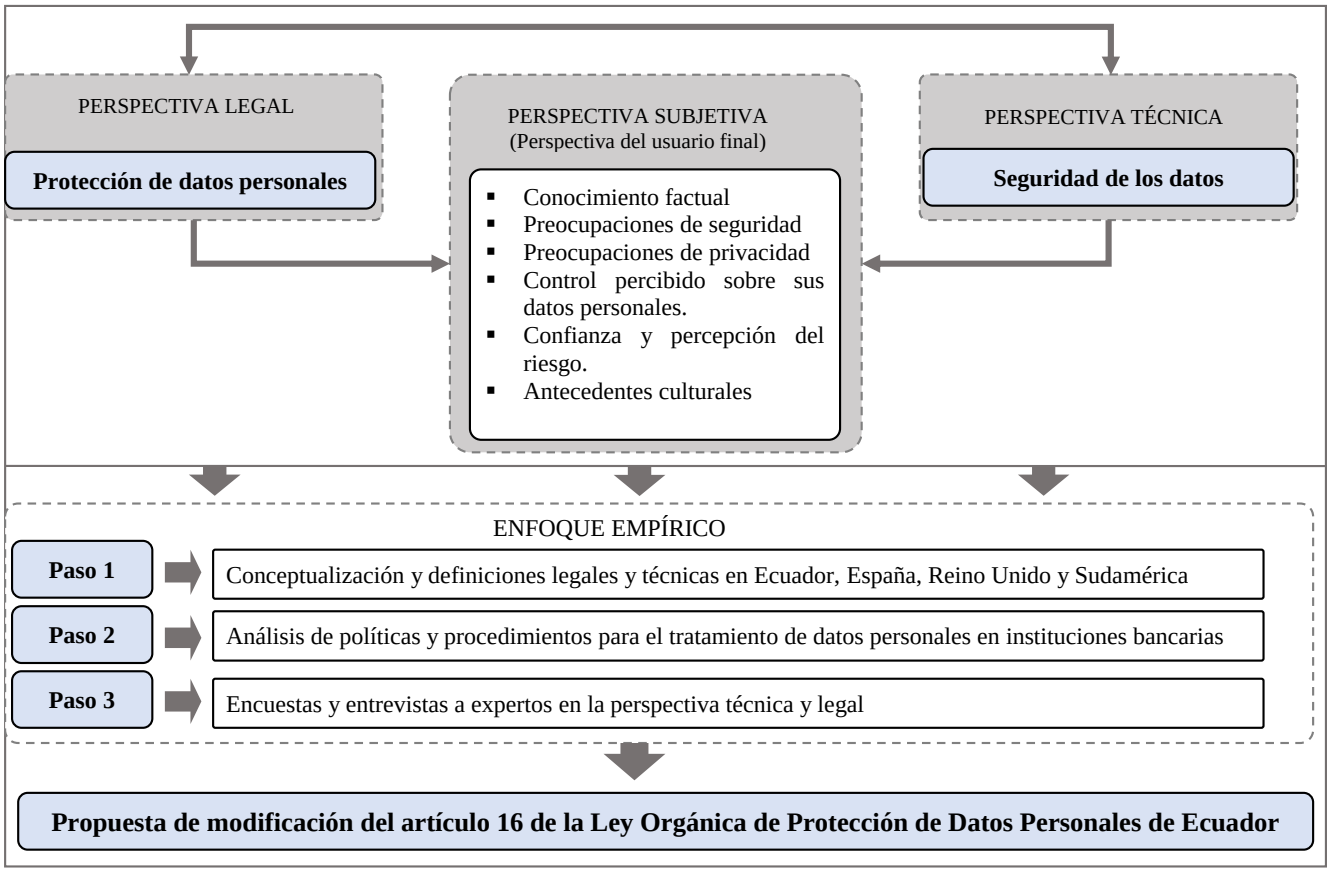

Figura 1. Metodología diseñada para la realización de la propuesta.

Tras el desarrollo de esta metodología, se formulará una propuesta de modificación del artículo 16 de la Ley Orgánica de Protección de Datos Personales de Ecuador. Esta propuesta buscará incorporar las recomendaciones y hallazgos surgidos a lo largo del proceso de investigación para fortalecer la protección de los datos personales en el país.

La validación de la propuesta de modificación del artículo 16 de la LOPDP en Ecuador, se llevará a cabo mediante la presentación de la propuesta a un panel de 11 expertos en diversas materias, incluyendo derecho penal, derecho administrativo, protección de datos, ciberseguridad, y ética en el manejo de información. Cada experto será seleccionado en función de su experiencia y conocimiento en su respectiva área, garantizando así una evaluación integral y multidisciplinaria de la propuesta.

Durante la sesión de validación, se presentará la propuesta de reforma, destacando la necesidad de proteger los datos personales de los clientes de las entidades bancarias y el derecho a la oposición desde el inicio de los trámites bancarios. Los expertos tendrán la oportunidad de discutir, hacer preguntas y proporcionar retroalimentación sobre la propuesta. Posteriormente, se llevará a cabo una evaluación cuantitativa para determinar la viabilidad y efectividad de la

modificación propuesta, asegurando que se consideren las perspectivas legales y técnicas necesarias para su implementación. A continuación, se presenta una tabla con las dimensiones y criterios evaluativos que serán empleados por los expertos para evaluar la propuesta de modificación:

Tabla 1. Dimensiones y criterios empleados para evaluar la propuesta de modificación del artículo 16 de la LOPDP de Ecuador.

Dimensiones	Criterios evaluativos
Relevancia legal	Adecuación a la normativa vigente y alineación con estándares internacionales.
	Claridad y precisión en la redacción legal de la propuesta.
	Capacidad de la propuesta para prevenir abusos por parte de las entidades bancarias.
Derechos del usuario	Garantía del derecho a la oposición desde el inicio de los trámites bancarios.
	Protección efectiva de la privacidad del cliente y sus datos personales.
	Mecanismos propuestos para la supervisión y cumplimiento de la normativa.
Viabilidad técnica	Implementación práctica de las medidas propuestas en el contexto bancario.
	Evaluación de los recursos necesarios para la implementación y mantenimiento de las medidas.
Impacto social	Efecto de la propuesta en la confianza del consumidor en las entidades bancarias.
	Percepción pública sobre la protección de datos y la privacidad tras la implementación de la propuesta.

Los expertos utilizarán una escala de evaluación de 1 a 5, donde: 1: Muy Insuficiente (no cumple con los criterios); 2: Insuficiente (cumple parcialmente con los criterios); 3: Aceptable (cumple con los criterios de manera básica); 4: Bueno (cumple con la mayoría de los criterios de manera efectiva); 5: Excelente (cumple con todos los criterios de manera sobresaliente). Esta metodología de evaluación permitirá obtener una visión clara y estructurada sobre la propuesta de modificación, facilitando la identificación de áreas de mejora y asegurando que se aborden adecuadamente las preocupaciones sobre la protección de datos personales en el ámbito bancario.

Resultados y discusión

La protección de datos personales ha cobrado una importancia creciente en el derecho internacional y nacional debido al avance de las tecnologías digitales y la globalización de la información, es por ello que se requiere comparar la Ley Orgánica de Protección de Datos Personales (LOPDP) de Ecuador con las normativas de España, Reino Unido y otros países de la región sudamericana, analizando sus similitudes, diferencias y el impacto de estos marcos legales en la protección de los derechos de los titulares de los datos. Este análisis se enfoca en la estructura normativa, los principios fundamentales, los derechos de los titulares de los datos, las obligaciones de los responsables y encargados del tratamiento, y las sanciones establecidas en cada jurisdicción.

Estructura Normativa

La Ley Orgánica de Protección de Datos Personales de Ecuador, promulgada en mayo de 2021, se alinea en gran medida con el Reglamento General de Protección de Datos (RGPD) de la Unión Europea, que ha establecido un estándar global en la protección de datos personales. La LOPDP establece un marco legal que regula el tratamiento de datos personales, lo que asegura el respeto por los derechos fundamentales de privacidad y protección de datos (Zanfir-Fortuna & Ianc, 2022). Similar al Reglamento General de Protección de Datos (RGPD) de la Unión Europea, la ley ecuatoriana define roles claros para el Responsable y el Encargado del tratamiento, además de introducir principios como la transparencia, minimización de datos, y responsabilidad proactiva (LOPDP, 2021).

En comparación, la normativa española, que está basada de forma directa en el RGPD, refuerza estos principios a través de la Ley Orgánica 3/2018 de Protección de Datos Personales y Garantía de los Derechos Digitales (LOPDGDD). Esta ley complementa el RGPD con disposiciones específicas adaptadas al contexto español, abordando aspectos como el tratamiento de datos en el ámbito laboral, la protección de menores y la regulación de los derechos digitales en un entorno conectado (Kuner, 2023). La estructura normativa en España es, por tanto, robusta y alineada de forma amplia con los estándares europeos, lo que garantiza una protección efectiva de los datos personales.

En el Reino Unido, la *Data Protection Act* 2018 (DPA) complementa y adapta el RGPD al contexto británico, de forma particular tras el Brexit (Acts, 2018). Aunque el Reino Unido se desvinculó de la Unión Europea, su legislación de protección de datos sigue alineada a los principios establecidos por el RGPD, aunque con algunas adaptaciones específicas para el entorno post-Brexit (Erdos, 2022). La DPA 2018 establece un marco similar al de la LOPDP y la LOPDGDD, pero con un enfoque particular en la soberanía británica y el control local sobre la normativa de protección de datos (Finck & Pallas, 2020).

En la región sudamericana, la legislación sobre protección de datos varía de manera significativa entre países. Por ejemplo, en Argentina, la Ley de Protección de los Datos Personales (Ley 25.326) fue una de las primeras en la región, aunque su actualización ha sido limitada y no se ha alineado en su totalidad con el RGPD. Brasil, en cambio, adoptó la Ley General de Protección de Datos (LGPD) en 2018, que sigue de cerca los principios del RGPD y ha establecido un marco legal sólido para la protección de datos en el país (Peters & Milanski, 2021).

Principios fundamentales

La LOPDP de Ecuador establece principios fundamentales similares a los del RGPD, incluyendo la licitud, lealtad y transparencia en el tratamiento de datos personales; la limitación de la finalidad; la minimización de datos; y la exactitud de los datos tratados. Estos principios están diseñados para garantizar que los datos personales se manejen de manera responsable y en el mejor interés de los titulares de los datos (Zanfir-Fortuna & Ianc, 2022).

En España, los principios fundamentales están igualmente alineados con el RGPD. La LOPDGDD refuerza estos principios y añade aspectos específicos relacionados con el entorno digital y la protección de menores, haciendo hincapié en la necesidad de consentimiento explícito y la protección de datos sensibles. La normativa española es fuerte en cuanto a la transparencia y la responsabilidad proactiva, exigiendo a las empresas que implementen medidas adecuadas para proteger los datos desde el diseño y por defecto (Estella & García, 2023).

La DPA 2018 del Reino Unido también se adhiere a estos principios, con un enfoque en la proporcionalidad y la equidad en el tratamiento de datos. Sin embargo, la normativa británica introduce algunas particularidades, como las excepciones para el tratamiento de datos en interés público y la seguridad nacional, que reflejan las preocupaciones específicas del Reino Unido en el contexto post-Brexit (Wittershagen, 2022).

En Sudamérica, los principios varían en su aplicación. Argentina, por ejemplo, establece principios similares a los del RGPD, pero con menos rigor en la aplicación y supervisión (Peruzzotti, 2024). Brasil, con su LGPD, ha adoptado principios casi idénticos a los del RGPD, asegurando un alto nivel de protección para los titulares de datos (Linares, 2021).

Derechos de los titulares de los datos

La LOPDP de Ecuador reconoce una amplia gama de derechos para los titulares de los datos, incluidos el derecho de acceso, rectificación, cancelación y oposición (ARCO), que están en línea con los derechos establecidos por el RGPD (Zanfir-Fortuna & Ianc, 2022). Además, la ley ecuatoriana introduce el derecho a la portabilidad de los datos y el derecho a no ser objeto de decisiones automatizadas sin intervención humana, reflejando un enfoque moderno y orientado al titular de los datos.

En España, la LOPDGDD amplía los derechos del RGPD, incluyendo garantías adicionales para el ejercicio de los derechos digitales, como el derecho a la desconexión digital y el derecho al olvido en entornos específicos. Estos derechos están diseñados para proteger a los individuos en un entorno cada vez más digitalizado, asegurando que tengan control sobre su información personal en todas las etapas del tratamiento (Sarrión, 2023).

El Reino Unido, bajo la DPA 2018, también garantiza estos derechos, aunque con ciertas variaciones en la implementación, de manera singular en lo que respecta a la portabilidad de datos y las decisiones automatizadas. El enfoque británico es pragmático; busca un equilibrio entre la protección de los derechos individuales y las necesidades de las empresas y el gobierno (Wolff & Atallah, 2021).

En Sudamérica, los derechos de los titulares de los datos están reconocidos en varias legislaciones, pero su implementación es desigual. Argentina reconoce los derechos ARCO, pero la portabilidad de datos no está tan

desarrollada como en Europa. En Brasil, la LGPD proporciona un conjunto completo de derechos similar al del RGPD, lo que representa un avance significativo en la protección de los datos en la región (Díaz, 2023).

Obligaciones de los responsables y encargados del tratamiento

La LOPDP de Ecuador impone obligaciones claras a los responsables y encargados del tratamiento, que incluyen la implementación de medidas técnicas y organizativas adecuadas para garantizar la seguridad de los datos personales, la realización de evaluaciones de impacto sobre la privacidad, y la notificación de brechas de seguridad (Ordóñez Pineda & Quezada, 2022). Estas obligaciones reflejan un enfoque proactivo y preventivo en la gestión de riesgos relacionados con la protección de datos.

En España, la LOPDGDD refuerza estas obligaciones, haciendo especial hincapié en la necesidad de adoptar medidas desde el diseño y por defecto. Las empresas están obligadas a realizar evaluaciones de impacto cuando el tratamiento de datos implique un alto riesgo para los derechos y libertades de los individuos, y a notificar cualquier brecha de seguridad a la Agencia Española de Protección de Datos (AEPD) dentro de las 72 horas (de Marcos, 2023).

El Reino Unido, con la DPA 2018, mantiene un enfoque similar, aunque con algunas adaptaciones para el contexto británico. Las obligaciones de los responsables y encargados del tratamiento incluyen la necesidad de contar con un Delegado de Protección de Datos (DPO) en ciertas circunstancias, y la obligación de realizar evaluaciones de impacto y notificaciones de brechas de seguridad (Goshadze, 2020).

En Sudamérica, las obligaciones varían de forma significativa. En Argentina, las obligaciones de los responsables del tratamiento son menos detalladas, lo que a veces lleva a una implementación inconsistente. En contraste, la LGPD de Brasil impone obligaciones muy estrictas, incluyendo la necesidad de realizar evaluaciones de impacto y la obligación de nombrar un DPO, similar al RGPD (Lorenzon, 2021).

Sanciones

La LOPDP de Ecuador establece un régimen sancionador para las infracciones de la ley, con multas que varían en función de la gravedad de la infracción y el tamaño de la entidad infractora. Estas sanciones son comparables a las establecidas en el RGPD, que prevé multas de hasta el 4% de la facturación anual global o 20 millones de euros, lo que sea mayor (Zanfir-Fortuna & Ianc, 2022).

En España, la LOPDGDD refuerza el régimen sancionador del RGPD, con sanciones que pueden llegar a los máximos establecidos por la normativa europea. La AEPD tiene la autoridad para imponer sanciones y llevar a cabo inspecciones para asegurar el cumplimiento de la ley (Ordóñez Pineda & Quezada, 2022)

En el Reino Unido, la DPA 2018 también establece un régimen sancionador robusto, alineado en gran medida con el RGPD. La Oficina del Comisionado de Información (ICO, por sus siglas en inglés) tiene la potestad de imponer

sanciones significativas por infracciones de la ley, que pueden alcanzar hasta el 4% de la facturación anual global de una empresa o 17.5 millones de libras, lo que sea mayor (Hewson & Tumbridge, 2020). El enfoque del Reino Unido es pragmático y busca garantizar la protección efectiva de los datos personales, mientras proporciona un marco de sanciones que disuada conductas negligentes o malintencionadas en el tratamiento de datos.

En Sudamérica, el régimen sancionador varía entre países. Argentina, bajo la Ley de Protección de Datos Personales (Ley 25.326), establece sanciones que incluyen multas (Peruzzotti, 2024), pero estas tienden a ser menores en comparación con las establecidas por el RGPD o la LOPDP de Ecuador. Las sanciones en Argentina se ven limitadas por la falta de una estructura de cumplimiento robusta, lo que puede llevar a una aplicación inconsistente de la ley.

Brasil, en cambio, con la Ley General de Protección de Datos (LGPD), ha adoptado un enfoque más estricto, estableciendo sanciones que pueden llegar hasta el 2% de la facturación anual de una empresa, con un límite de 50 millones de reales por infracción (Heffes, 2022). Este marco se asemeja al del RGPD y muestra un compromiso significativo con la protección de datos en la región. La LGPD también prevé otras medidas sancionadoras, como la suspensión de actividades relacionadas con el tratamiento de datos y la divulgación pública de la infracción, lo que puede afectar considerablemente la reputación de una empresa.

En comparación, la LOPDP de Ecuador establece un régimen sancionador que busca no solo castigar las infracciones, sino también prevenir futuros incumplimientos mediante la imposición de multas proporcionales a la gravedad de la infracción y la capacidad económica de la entidad infractora. La ley prevé una escala de sanciones que va desde amonestaciones hasta multas económicas significativas, que pueden variar según factores como el número de afectados, el tipo de datos comprometidos y la intencionalidad del infractor (Zanfir-Fortuna & Ianc, 2022)

El análisis comparado de la Ley Orgánica de Protección de Datos Personales de Ecuador con las normativas de España, Reino Unido y otros países sudamericanos revela una tendencia hacia la armonización de principios y derechos en la protección de datos personales, impulsada en gran medida por la influencia del RGPD de la Unión Europea. La LOPDP de Ecuador, aunque joven en su implementación, muestra un compromiso serio con la protección de datos, reflejando principios clave del RGPD y estableciendo un marco sancionador robusto.

Sin embargo, las diferencias en la aplicación y el rigor de las normativas entre estos países también destacan los desafíos en la implementación efectiva de estas leyes. Mientras que países como España y Brasil han adoptado marcos legales completos y bien desarrollados, otros países de la región sudamericana aún enfrentan desafíos en la modernización de sus leyes y en la aplicación consistente de las sanciones.

El estudio comparativo subraya la importancia de no solo adoptar marcos legales basados en mejores prácticas internacionales, sino también de garantizar su efectiva implementación y cumplimiento. En este sentido, la LOPDP de

Ecuador representa un paso importante hacia la protección de los derechos de los titulares de los datos en el país, pero su éxito dependerá en gran medida de la capacidad de las autoridades ecuatorianas para aplicar la ley de manera efectiva y justa y lo primero que se debe establecer son sistemas oportunos y adecuados para el acceso a plataformas digitales donde se manifieste los términos y condiciones de forma clara para dar libertad de elegir los acuerdos que el titular de los datos quiere aceptar.

Encuestas y entrevistas a expertos y clientes de las entidades bancarias

A partir de la conceptualización y definición de los términos legales y técnicos relevantes en los contextos mencionados; se llevaron a cabo encuestas y entrevistas con clientes de entidades bancarias y expertos en la materia, con el objetivo de obtener datos concretos y perspectivas variadas que puedan enriquecer la propuesta que se pretende realizar en esta investigación.

Encuesta a clientes de las entidades bancarias

Se realizó una encuesta diseñada para los clientes de entidades bancarias, con el objetivo de recopilar información sobre sus inquietudes y percepciones relacionadas con la protección de datos personales. Durante 1 mes los autores intercambiaron con diferentes clientes, quienes aceptaron a participar en la encuesta. Se logró una intención de participación de 407 clientes, y finalmente respondieron 304. Los resultados se resumen a continuación:

Pregunta 1 ¿Está usted consciente de las políticas de protección de datos personales de su entidad bancaria?

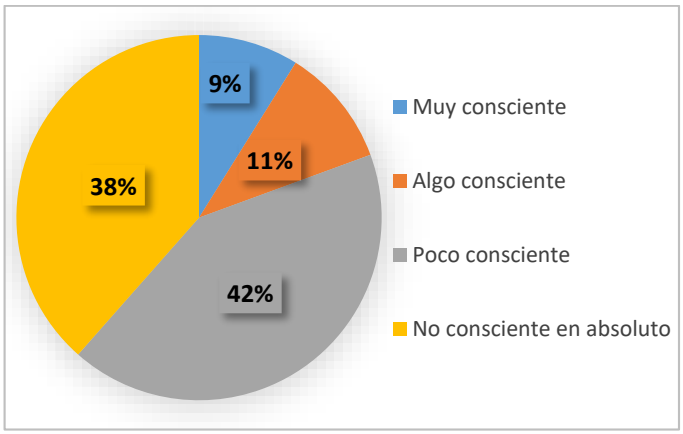

Figura 2. Conocimiento sobre las políticas de protección de datos personales de su entidad bancaria.

Pregunta 2. ¿Considera que su entidad bancaria protege adecuadamente sus datos personales?

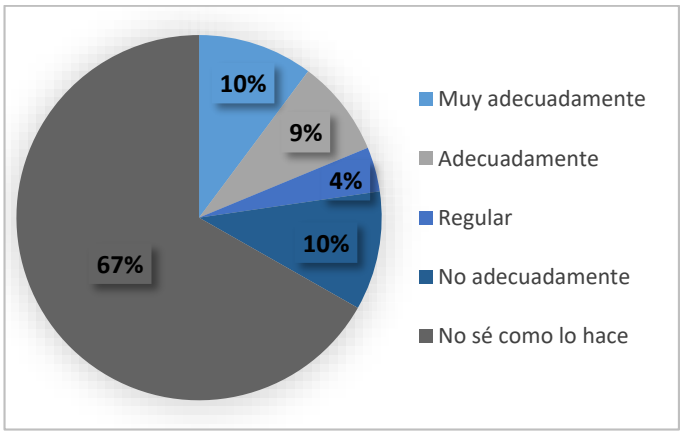

Figura 3. Percepción sobre la protección de sus datos personales.

Pregunta 3. ¿Siente que tiene control sobre la información personal que comparte con su entidad bancaria?

Pregunta 4. ¿Confía en que su entidad bancaria maneja sus datos personales de manera responsable?

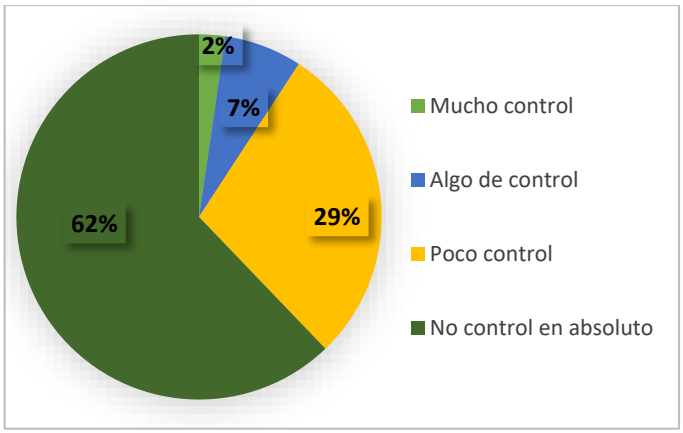

Figura 4. Percepción de control sobre sus datos personales.

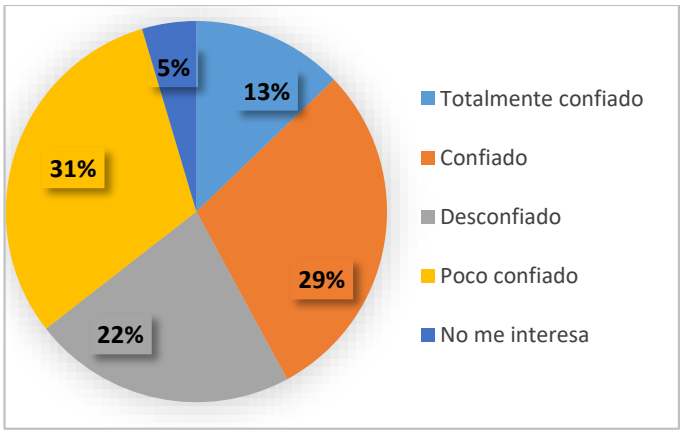

Figura 5. Confianza en el manejo de sus datos personales.

Al analizar los resultados de la encuesta se evidencia que la mayoría de los encuestados (80.6%) se muestra poco consciente o no consciente en absoluto sobre las políticas de protección de datos de su entidad bancaria. Esto indica una falta de información y educación por parte de las instituciones bancarias respecto a sus políticas de protección de datos, lo que evidencia que los clientes no están bien informados sobre sus derechos y cómo se gestionan sus datos.

Además, una gran mayoría (66.8%) de los encuestados no sabe cómo su entidad bancaria protege sus datos personales, lo que sugiere que existe una falta de transparencia en la comunicación de las prácticas de seguridad. Solo un 18.8% considera que la protección es adecuada. Esto definitivamente genera desconfianza y un sentimiento de vulnerabilidad entre los clientes.

Por otra parte, la gran mayoría de los encuestados (91.1%) siente que tiene poco o ningún control sobre la información personal que comparte, lo que refleja una preocupación significativa por la gestión de sus datos. Esto resalta la necesidad urgente de que las entidades bancarias implementen medidas que empoderen a sus clientes para que se sientan más en control de su información. Además, solo un 12.8% de los encuestados se siente totalmente confiado en que su entidad bancaria maneja sus datos de manera responsable; y solo un 5 % manifestó que no le interesa. Cuando se relaciona este resultado con el conocimiento de los mecanismos de protección de datos, es evidente que, aunque las personas no conocen como funciona técnica y legalmente la protección de sus datos personales, sí les interesa que sean protegidos.

Resultados de encuesta aplicada a expertos en protección de datos personales

La encuesta realizada a 11 expertos en protección de datos tuvo como objetivo evaluar la eficacia y los desafíos del manejo de datos personales en las plataformas bancarias de Ecuador. A través de una serie de preguntas diseñadas para medir la efectividad del consentimiento informado actual, se buscó comprender si los usuarios realmente comprenden

cómo se utilizarán sus datos, y se enfatizó la importancia del derecho de oposición frente a los tratamientos de datos por parte de las entidades bancarias. Los principales resultados de la encuesta, se muestran en la tabla 2.

Tabla 2. Encuesta aplicada a expertos en protección de datos personales

Preguntas	M	DE
En su opinión, ¿cuán efectivo es el consentimiento informado actual en las plataformas bancarias de Ecuador para garantizar que los titulares comprendan completamente el uso de sus datos personales? (1 = Nada efectivo, 10 = Muy efectivo)	5,64	1,29
¿Qué tan grave considera que es la afectación del derecho de oposición de los usuarios al tratamiento de sus datos personales por parte de las entidades bancarias en Ecuador? (1 = No es grave, 10 = Extremadamente grave)	8,18	1,25
¿En qué medida cree que las prácticas de consentimiento en las plataformas digitales bancarias en Ecuador respetan los principios de transparencia y claridad establecidos en la ley? (1 = No respetan en absoluto, 10 = Respetan completamente)	5,45	1,75
¿Cuán importante considera que es una modificación al artículo 16 de la Ley Orgánica de Protección de Datos Personales para mejorar el ejercicio del derecho de oposición en el sector bancario? (1 = Nada importante, 10 = Extremadamente importante)	9,03	0,47
¿Qué tan adecuadamente cree que las entidades bancarias en Ecuador gestionan los procedimientos de oposición al tratamiento de datos personales cuando los titulares ejercen este derecho? (1 = Muy inadecuadamente, 10 = Muy adecuadamente)	4,73	0,47
¿Cuán efectivo cree que sería un aumento en las sanciones para las entidades bancarias que no respeten el derecho de oposición y el consentimiento informado? (1 = Nada efectivo, 10 = Muy efectivo)	8,45	1,51
¿En qué medida considera que las políticas actuales de protección de datos en el sector bancario ecuatoriano son suficientes para proteger los derechos de los titulares de datos personales? (1 = Nada suficientes, 10 = Totalmente suficientes)	5,45	0,69

Sobre el impacto de la falta de claridad en el consentimiento informado sobre los derechos de los usuarios al entregar sus datos personales en las plataformas bancarias en Ecuador, los expertos coinciden que la falta de transparencia en el consentimiento informado afecta negativamente los derechos de los titulares, al impedirles tomar decisiones informadas sobre el uso de sus datos. Esto podría resultar en prácticas abusivas por parte de las entidades bancarias, disminuyendo la confianza del usuario y vulnerando principios fundamentales de privacidad y autodeterminación informativa.

Con relación a las prácticas bancarias y el derecho de oposición al tratamiento de los datos de las entidades bancarias en Ecuador, como la imposición de términos complejos, falta de información clara y procedimientos engorrosos, limitan significativamente el ejercicio del derecho de oposición. Estas barreras dificultan que los titulares comprendan sus opciones y actúen en consecuencia, desincentivando su participación en el control de sus datos personales y favoreciendo un entorno de opacidad y falta de transparencia.

Al analizar las modificaciones necesarias en la Ley Orgánica de Protección de Datos Personales para garantizar que el consentimiento informado y el derecho de oposición sean respetados en el sector bancario existe similitud en afirmar la necesidad de establecer requisitos estrictos para el consentimiento informado, prohibir cláusulas abusivas, simplificar el lenguaje de los términos y condiciones, y exigir procedimientos claros para ejercer el derecho de oposición. Además, se podrían sugerir sanciones severas para las entidades que incumplan, asegurando así una protección efectiva de los datos personales en el sector bancario.

Con relación a las buenas prácticas normativas internacionales los expertos destacaron ejemplos como el Reglamento General de Protección de Datos (GDPR) de la Unión Europea, que exige consentimiento explícito y claro, y el modelo de "opt-in" obligatorio de Canadá, donde los usuarios deben aceptar activamente el tratamiento de sus datos. También podrían mencionar la normativa australiana, que promueve la transparencia en la recopilación y uso de datos personales con especificidad a la actividad bancaria y financiera.

Se expresaron como desafíos la falta de infraestructura tecnológica adecuada, la necesidad de capacitación del personal en políticas de protección de datos, y la complejidad de armonizar las normativas internas con las leyes internacionales. Además, se mencionan los costos asociados con la implementación de medidas de seguridad más estrictas y las dificultades para adaptar procesos operativos existentes a nuevas regulaciones.

Los instrumentos y el análisis dogmático doctrinal revelan una percepción generalizada de que la falta de claridad en el consentimiento informado y las prácticas bancarias actuales limitan significativamente el ejercicio del derecho de oposición en Ecuador. Se podría identificar la necesidad de modificar el artículo 16 de la Ley Orgánica de Protección de Datos Personales para incluir medidas que garanticen transparencia y claridad en las plataformas digitales bancarias. Los expertos destacan ejemplos internacionales como modelos a seguir y sugerir la introducción de sanciones más severas para mejorar el cumplimiento.

Propuesta de modificación al artículo 16 de la Ley Orgánica de Protección de Datos Personales del Ecuador

La propuesta de modificación al artículo 16 de la Ley Orgánica de Protección de Datos Personales del Ecuador se sustentó en un análisis integral que abarcó diversas dimensiones, incluyendo la revisión de las normativas vigentes.

Este estudio comparativo permitió identificar las mejores prácticas en la protección de datos personales, especialmente en el ámbito bancario, donde la seguridad de la información es fundamental. Además, se incorporaron los resultados de encuestas y entrevistas a expertos en materia técnica y legal, quienes señalaron las limitaciones de la legislación actual y la necesidad de adaptarla a los estándares internacionales. De esta manera, la propuesta busca no solo fortalecer la protección de los datos personales en Ecuador, sino también garantizar la confianza de los usuarios en las instituciones financieras, promoviendo un entorno más seguro y transparente en el tratamiento de su información personal.

Objetivo de la propuesta:

Proponer una modificación al artículo 16 de la Ley Orgánica de Protección de Datos Personales del Ecuador que prohíba a las entidades bancarias imponer obstáculos al derecho de oposición, garantizando su ejercicio sin restricciones indebidas y estableciendo sanciones claras para asegurar el cumplimiento de la ley.

Justificación de la propuesta:

El artículo 16 de la Ley Orgánica de Protección de Datos Personales, manifiesta en tres numerales, los casos en donde el titular puede ejercer el derecho de oposición del tratamiento de sus datos personales, a lo que se propone introducir un cuarto numeral para regular las prácticas de las entidades bancarias que solicitan la autorización de tratamiento de datos personales de forma amplia otorgando un uso exorbitante que pueden vulnerar el derecho de privacidad del titular.

El artículo está redactado de la siguiente forma en la Ley Orgánica de Protección de Datos Personales de Ecuador:

> ***Art. 16.-****Derecho de oposición. El titular tiene el derecho a oponerse o negarse al tratamiento de sus datos personales, en los siguientes casos:*
>
> 1) No se afecten derechos y libertades fundamentales de terceros, la ley se lo permita y no se trate de información pública, de interés público o cuyo tratamiento está ordenado por la ley.
> 2) El tratamiento de datos personales tenga por objeto la mercadotecnia directa; el interesado tendrá derecho a oponerse en todo momento al tratamiento de los datos personales que le conciernan, incluida la elaboración de perfiles; en cuyo caso los datos personales dejarán de ser tratados para dichos fines.
> 3) Cuando no sea necesario su consentimiento para el tratamiento como consecuencia de la concurrencia de un interés legítimo, previsto en el artículo 7, y se justifique en una situación concreta personal del titular, siempre que una ley no disponga lo contrario. El responsable de tratamiento dejará de tratar los datos personales en estos casos, salvo que acredite motivos legítimos e imperiosos para el tratamiento que prevalezcan sobre los intereses, los derechos y las libertades del titular, o para la formulación, el ejercicio o la defensa de reclamaciones. Esta solicitud deberá ser atendida dentro del plazo de quince (15) días.

La propuesta de la presente investigación consiste en agregar el numeral 4, que quedaría redactado de la siguiente forma:

4) Prohibición de obstáculos por entidades bancarias: Las entidades bancarias, financieras o de crédito no podrán imponer términos, condiciones o procedimientos adicionales que resulten onerosos, engañosos o poco transparentes para los titulares que deseen ejercer su derecho de oposición al tratamiento de sus datos personales, incluyendo la negativa a aceptar cláusulas que condicionen el acceso a sus servicios digitales al tratamiento de datos personales no necesarios para la prestación de dichos servicios. El uso de tales prácticas se considerará un incumplimiento de la presente ley, y las entidades infractoras serán sancionadas conforme a las disposiciones establecidas en la normativa vigente.

Validación de la propuesta de modificación

Para la validación de la propuesta de modificación del artículo 16 de la LOPDP de Ecuador, se contó con un equipo de 11 expertos de alto prestigio en el sector. Se evaluaron los 10 criterios de las 4 dimensiones definidas en la tabla 1. Las figuras 6-9 muestran el resultado de la evaluación promedio de los indicadores en las dimensiones Relevancia legal, Derechos del usuario, Viabilidad técnica, e Impacto social.

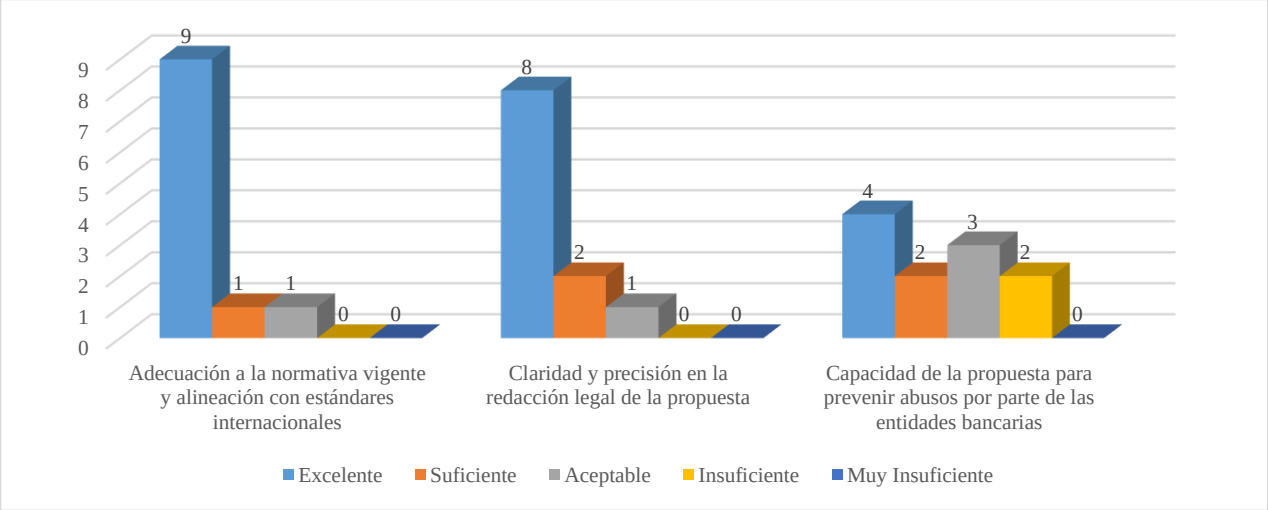

Figura 6. Evaluación promedio de los indicadores de la dimensión Relevancia legal, empleados para evaluar la propuesta de modificación del artículo 16 de la LOPDP de Ecuador.

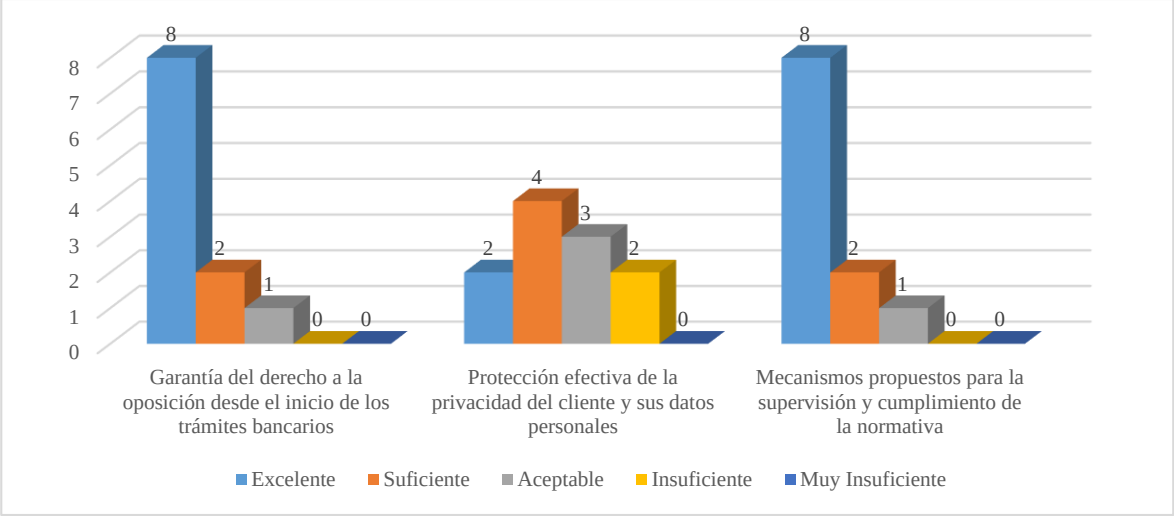

Figura 7. Evaluación promedio de los indicadores de la dimensión Derechos del usuario, empleados para evaluar la propuesta de modificación del artículo 16 de la LOPDP de Ecuador.

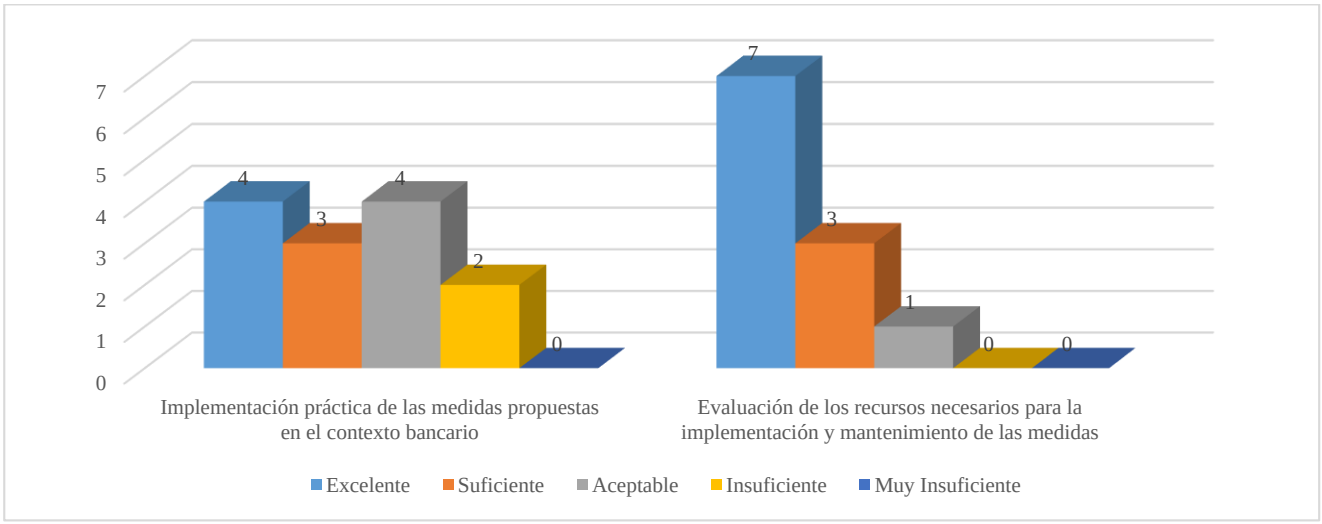

Figura 8. Evaluación promedio de los indicadores de la dimensión Viabilidad técnica, empleados para evaluar la propuesta de modificación del artículo 16 de la LOPDP de Ecuador.

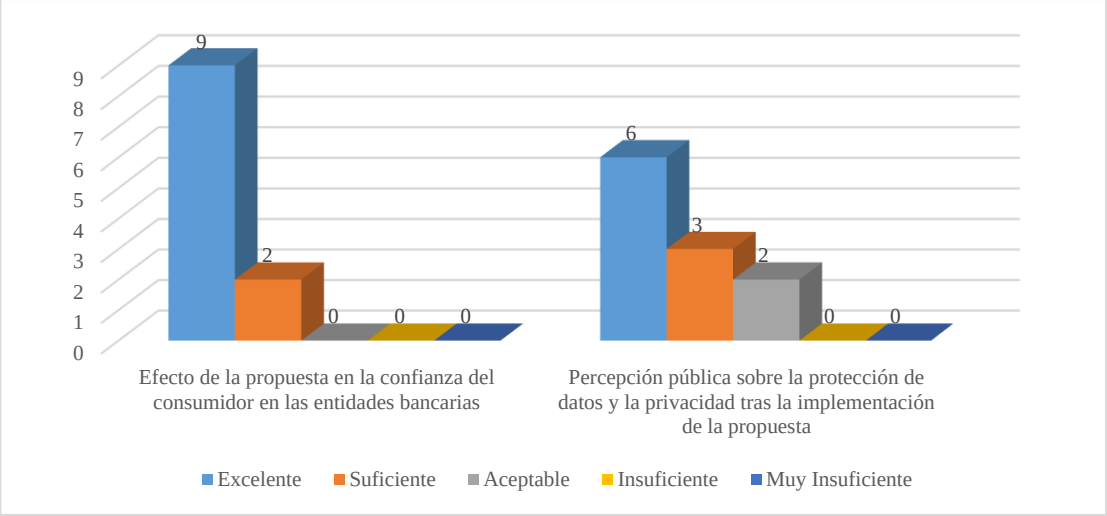

Figura 9. Evaluación promedio de los indicadores de la dimensión Impacto social, empleados para evaluar la propuesta de modificación del artículo 16 de la LOPDP de Ecuador.

Los resultados expresados por los expertos sobre la propuesta de modificación al artículo 16 de la LOPDP del Ecuador, revelaron un fuerte respaldo en diversas dimensiones clave. En la dimensión de relevancia legal (figura 6), se observa que la adecuación a la normativa vigente y la alineación con estándares internacionales fue calificada predominantemente como excelente, con 9 evaluaciones en la máxima categoría. Sin embargo, la capacidad de la propuesta para prevenir abusos por parte de las entidades bancarias recibió una calificación mixta, reflejando la preocupación de los expertos ante posibles violaciones.

Respecto a los derechos del usuario (figura 7), la garantía del derecho a la oposición desde el inicio de los trámites bancarios mostró resultados positivos, aunque la protección efectiva de la privacidad del cliente presentó mayores desafíos, con un número significativo de evaluaciones en rangos inferiores. Esto se debe a que aún son insuficientes los mecanismos de regulación legales y técnicos fundamentalmente.

En la dimensión de viabilidad técnica (figura 8), la implementación práctica de las medidas propuestas fue considerada aceptable, evidenciando la necesidad de un análisis más profundo sobre los recursos requeridos para su adecuación en el ámbito bancario. Los expertos argumentaron, que la práctica ha demostrado la resistencia de ciertas instituciones a introducir modificaciones en sus plataformas digitales. Por último, en el impacto social, la propuesta logró un notable consenso en su potencial para influir positivamente en la confianza del consumidor en las entidades bancarias (figura 9). No obstante, la percepción pública sobre la protección de datos y la privacidad sugiere áreas que requieren atención para asegurar una adecuada recepción de la normativa.

En conjunto, estos resultados apuntan a una propuesta con fundamentos sólidos, que permiten garantizar su efectividad y aceptación en la práctica.

Discusión

Los resultados de la encuesta demostraron que, a pesar de la armonización jurídica que se persigue en Ecuador, siguen existiendo diferencias prácticas en la implementación, interpretación y cumplimiento de las leyes, normas y políticas públicas, específicamente en la protección de los datos personales.

Los resultados del estudio comparado demuestran que la asimetría de datos conduce a espirales negativas en las que las poblaciones más vulnerables se enfrentan a la mayor exposición. Quienes tienen menos poder y menos protección de la privacidad generan más datos debido a la necesidad económica o la vigilancia. Luego, sus datos se comercializan o se utilizan indebidamente en contra de sus intereses (Gulyamov & Raimberdiyev, 2023). Por ejemplo, los grupos de bajos ingresos tienden a utilizar dispositivos y servicios con características de seguridad más débiles. El desgaste de datos que producen se recolecta, lo que aumenta las disparidades de poder que los obligan a generar más datos. Estas desigualdades luego se integran en los sistemas de toma de decisiones automatizadas, lo que afianza la desventaja.

Para frenar la explotación de los datos personales es necesario restablecer la agencia y la rendición de cuentas en torno a los flujos de datos. Los usuarios no deben ser puntos de datos pasivos, sino agentes empoderados con una comprensión real de cómo se maneja su información. Esto significa brindar opciones para compartir datos de manera voluntaria y selectiva, al tiempo que se establecen restricciones claras sobre el uso indebido. Pero los usuarios no pueden actuar como individuos solitarios. Los derechos deben ir acompañados de marcos de gobernanza sólidos y receptivos que supervisen las prácticas de datos en interés público.

Conclusiones

Los resultados de la encuesta a clientes de entidades bancarias reflejaron falta de conciencia, confianza y control por parte de los clientes en relación con la protección de sus datos personales. La mayoría de los encuestados no se siente seguro ni informado, lo que sugiere que las entidades bancarias necesitan mejorar la transparencia, la educación y las prácticas de protección de datos. Esto podría ayudar a construir una mayor confianza y una relación más sólida con sus clientes.

La propuesta realizada tiene gran importancia dado que el derecho de oposición es aquel recurso que tiene el titular para oponerse al tratamiento ilimitado de sus datos personales, lo que le permite proteger su intimidad dentro de la esfera digital y a la vez mantiene el control de su información sensible.

Se espera que los resultados de las recomendaciones de este estudio desarrollen y fortalezcan la protección de datos personales en las compañías bancarias en Ecuador. Además de apuntar a prevenir el uso indebido de datos personales, la regulación apunta a proteger a los consumidores y acelerar el crecimiento de la economía digital.

Conflictos de intereses

Los autores no poseen conflictos de intereses.

Contribución de los autores

1. Conceptualización: Johanna Irene Escobar Jara, Duniesky Alfonso Caveda
2. Curación de datos: Jean Carlos Pardo Zhingri
3. Análisis formal: Jean Carlos Pardo Zhingri
4. Investigación: Jean Carlos Pardo Zhingri, Johanna Irene Escobar Jara, Duniesky Alfonso Caveda
5. Metodología: Johanna Irene Escobar Jara, Duniesky Alfonso Caveda
6. Administración del proyecto: Johanna Irene Escobar Jara, Duniesky Alfonso Caveda
7. Software: Jean Carlos Pardo Zhingri
8. Supervisión: Johanna Irene Escobar Jara, Duniesky Alfonso Caveda
9. Validación: Jean Carlos Pardo Zhingri
10. Visualización: Jean Carlos Pardo Zhingri, Johanna Irene Escobar Jara, Duniesky Alfonso Caveda
11. Redacción – borrador original: Jean Carlos Pardo Zhingri, Johanna Irene Escobar Jara, Duniesky Alfonso Caveda
12. Redacción – revisión y edición: Jean Carlos Pardo Zhingri, Johanna Irene Escobar Jara, Duniesky Alfonso Caveda

Financiamiento

La investigación no requirió fuente de financiamiento externa.

Referencias

Acts, U. P. G. (2018). *Data Protection Act 2018*. https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted

Contreras, P., & Felipe, A. (2020). Marco normativo de la historia clínica electrónica y su incidencia en el ámbito de la protección de datos personales en Colombia (Regulatory Framework of the Electronic Medical Record and Its

Incidence in the Field of Personal Data Protection in Colombia). *La Propiedad Inmaterial*(29). https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3641731

De Hert, P., & Papakonstantinou, V. (2016). The new General Data Protection Regulation: Still a sound system for the protection of individuals? *Computer Law & Security Review*, *32*(2), 179-194. https://www.sciencedirect.com/science/article/pii/S0267364916300346

de Marcos, E. D. F. (2023). Memoria de la Agencia Española de Protección de Datos (AEPD) 2022. Puntos a destacar. *La Ley privacidad*, *16*. https://portalcientifico.universidadeuropea.com/documentos/64c160d6062e79589ae15527?lang=en

Díaz, M. F. S. (2023). El derecho a la protección de datos personales en la era digital. *Revista Eurolatinoamericana de Derecho Administrativo*, *10*(1), 1-21. https://www.redalyc.org/journal/6559/655977607008/655977607008.pdf

Erdos, D. (2022). The UK and the EU personal data framework after Brexit: A new trade and cooperation partnership grounded in Council of Europe Convention 108+? *Computer Law & Security Review*, *44*, 105639. https://www.sciencedirect.com/science/article/pii/S0267364921001126

Estella, F. D., & García, B. O. (2023). La nueva Carta de Derechos Digitales en España, y los nuevos reglamentos comunitarios DSA, DMA e IA:¿ hacia un constitucionalismo digital? *CEFLegal. Revista práctica de derecho*, 39-74. https://revistas.cef.udima.es/index.php/ceflegal/article/view/18805

Finck, M., & Pallas, F. (2020). They who must not be identified—distinguishing personal from non-personal data under the GDPR. *International Data Privacy Law*, *10*(1), 11-36. https://academic.oup.com/idpl/article-pdf/doi/10.1093/idpl/ipz026/33151834/ipz026.pdf

Fuel Rodríguez, G. V. (2024). *Implementación de la ley orgánica de protección de datos personales en la Cooperativa de Ahorro y Crédito "Pablo Muñoz Vega" considerando los estándares ISO/IEC 27001: 2022, ISO/IEC 27002: 2022, ISO/IEC27701: 2019 y el SGSI institucional* https://repositorio.utn.edu.ec/handle/123456789/16197

Goshadze, K. (2020). The Data Protection Officer (DPO)-Ensuring Greater Data Protection Compliance. *Law & World*, *14*, 41. https://heinonline.org/hol-cgi-bin/get_pdf.cgi?handle=hein.journals/lwwrld14&section=7

Gulyamov, S., & Raimberdiyev, S. (2023). Personal data protection as a tool to fight cyber corruption. *International Journal of Law and Policy*, *1*(7). https://irshadjournals.com/index.php/ijlp/article/view/119

Heffes, G. (2022). Impacto del Reglamento General de Protección de Datos (GDPR) en las empresas con modelo de negocio de monetización de datos.

https://repositorio.udesa.edu.ar/jspui/bitstream/10908/19632/1/%5BP%5D%5BW%5D%20M.%20Ges%20Heffes,%20Guido.pdf

Hewson, V., & Tumbridge, J. (2020). Who Regulates the Regulators? The Information Commissioner's Office. *The Information Commissioner's Office (July 15, 2020). Institute of Economic Affairs*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3851959

Hondares, Y. P., Almora, R. M., & Véliz, A. P. (2021). La protección de datos personales. Presupuestos constitucionales para su protección en los procesos judiciales en cuba: The protection of personal data. Constitutional budgets for your protection in judicial processes In Cuba. *Revista Científica Ecociencia*, *8*, 126-161. https://revistas.ecotec.edu.ec/index.php/ecociencia/article/view/644

Kuner, C. (2023). Protecting EU data outside EU borders under the GDPR. *Common Market Law Review*, *60*(1). https://kluwerlawonline.com/journalarticle/Common+Market+Law+Review/60.1/COLA2023004

Linares, R. M. O. (2021). La influencia regulatoria de la Unión Europea: el ejemplo del Reglamento General de Protección de Datos de la Unión Europea. *El derecho penal en el siglo XXI: Liber amicorum en honor al profesor José Miguel Zugaldía Espinar*, 817-852. https://www.academia.edu/download/79580715/El_Reglamento_General_de_Proteccion_de_Datos_de_la_Union_Europea.pdf

LOPDP. (2021). Ley Orgánica de Protección de Datos Personales. https://www.registroficial.gob.ec/index.php/registro-oficial-web/publicaciones/suplementos/item/14305-suplemento-al-registro-oficial-no-548

Lorenzon, L. N. (2021). Análise comparada entre regulamentações de dados pessoais no Brasil e na União Europeia (LGPD e GDPR) e seus respectivos instrumentos de enforcement. *Revista do Programa de Direito da União Europeia*, *1*, 39-52. http://periodicos.fgv.br/rpdue/article/view/83423

Mantelero, A. (2016). Personal data for decisional purposes in the age of analytics: From an individual to a collective dimension of data protection. *Computer law & security review*, *32*(2), 238-255. https://www.sciencedirect.com/science/article/pii/S0267364916300280

Ochoa, N. V. V., Álvarez, M. Á. M., & Manzano, R. L. M. (2024). Implementación de medidas de seguridad y principio de conservación de datos según la ley orgánica de protección de datos personales en instituciones públicas de Babahoyo, Ecuador. *Dilemas contemporáneos: Educación, Política y Valores*. https://dilemascontemporaneoseducacionpoliticayvalores.com/index.php/dilemas/article/view/4080

Ordóñez Pineda, L., & Quezada, C. (2022). Políticas públicas y protección de datos personales en Ecuador: reflexiones desde la emergencia sanitaria. *Estado & comunes, revista de políticas y problemas públicos*, *2*(15), 77-97. http://scielo.senescyt.gob.ec/scielo.php?script=sci_arttext&pid=S2477-92452022000200077

Peruzzotti, M. (2024). Actualidad en materia de protección de datos personales en Argentina. *Cuadernos del Centro de Estudios de Diseño y Comunicación*(217). https://dspace.palermo.edu/ojs/index.php/cdc/article/download/11237/19304

Peters, E. L., & Milanski, A. (2021). El nuevo marco de protección de los ciberdatos personales en Brasil como derechos humanos. *Artificial intelligence and human rights*, 143-154. https://www.torrossa.com/gs/resourceProxy?an=5109969&publisher=FZ1825

Romansky, R. P., & Noninska, I. S. (2020). Challenges of the digital age for privacy and personal data protection. *Mathematical Biosciences and Engineering*, *17*(5), 5288-5303. https://www.aimspress.com/article/10.3934/mbe.2020286/abstract.html

Sarrión, J. (2023). Challenges and perspectives in biomedical research with data in Spain. *Derecho y salud*, 1133-7400. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4642670

Tikkinen-Piri, C., Rohunen, A., & Markkula, J. (2018). EU General Data Protection Regulation: Changes and implications for personal data collecting companies. *Computer Law & Security Review*, *34*(1), 134-153.

Van Dijk, N., Tanas, A., Rommetveit, K., & Raab, C. (2018). Right engineering? The redesign of privacy and personal data protection. *International review of law, computers & technology*, *32*(2-3), 230-256. https://www.tandfonline.com/doi/abs/10.1080/13600869.2018.1457002

van Loenen, B., Kulk, S., & Ploeger, H. (2016). Data protection legislation: A very hungry caterpillar: The case of mapping data in the European Union. *Government Information Quarterly*, *33*(2), 338-345. https://www.sciencedirect.com/science/article/pii/S0740624X16300326

Wittershagen, L. (2022). *The Transfer of Personal Data from the European Union to the United Kingdom post-Brexit* (Vol. 1). Walter de Gruyter GmbH & Co KG. https://books.google.com/books?hl=es&lr=&id=f_qjEAAAQBAJ&oi=fnd&pg=PR7&dq=United+Kingdom,+the+Data+Protection+Act+2018&ots=82N3LmoCNZ&sig=vZKGbNRk4XqM6xdMplxSuIht8ow

Wolff, J., & Atallah, N. (2021). Early GDPR penalties: Analysis of implementation and fines through May 2020. *Journal of Information Policy*, *11*, 63-103. https://scholarlypublishingcollective.org/psup/information-policy/article-abstract/11/1/63/291999

Zanfir-Fortuna, G., & Ianc, S. (2022). *Data protection and competition law: The dawn of uberprotection*. Edward Elgar Publishing. https://www.elgaronline.com/edcollchap/edcoll/9781786438508/9781786438508.00020.xml