Systematic review of implemented technologies on e-commerce and banking platforms for data protection laws compliance

Eduardo Emmanuel, Bayona Silva[1], Nathaly Mariel, Segura Marcelo[2],
Víctor Angel Ancajima Miñán[3], Luis Alberto Casaverde Pacherrez[4]
[1,2,3,4]Universidad Tecnológica del Perú, Perú, *U20233665@utp.edu.pe, U20305093@utp.edu.pe, C25994@utp.edu.pe, C23941@utp.edu.pe*

Abstract

Exist Diverse technologies that are implemented on E-commerce and Banking platforms to comply with the data protection laws and ensure operational efficiency. However, strengths and weaknesses were identified in its implementation which affect its effectiveness. Therefore, the objective of this study is to analyze the main technologies used on these platforms for compliance with regulations such as the General Data Protection Regulation and California Consumer Privacy Act and evaluate their impact on operational efficiency. A non-experimental, descriptive, qualitative-quantitative design was used, corresponding to a systematic literature review without meta-analysis. Thirty-five articles from Scopus, Redalyc, and Web of Science databases were selected, following inclusion-exclusion specific criteria. The results show that key technologies such as encryption and identity management are fundamentals for regulatory compliance, but face challenges related to high integration costs, technical capacitation, and cultural resistance in some regions. It concludes that although these technologies allow good compliance with data protection laws, their effectiveness varies according to regulatory framework and region. It's recommended to promote technological innovation and intersectoral cooperation to overcome economic and operative barriers, thus ensuring a more efficient digital platform regulatory compliance.

Keywords—Data Protection, Privacy Protection, E-Commerce, Payment Security, GDPR

Revisión sistemática de tecnologías implementadas en plataformas de comercio electrónico y bancarias para el cumplimiento de la ley de protección de datos

Eduardo Emmanuel, Bayona Silva[1], Nathaly Mariel, Segura Marcelo[2],
Víctor Angel Ancajima Miñán[3], Luis Alberto Casaverde Pacherrez[4]
[1,2,3,4]Universidad Tecnológica del Perú, Perú, *U20233665@utp.edu.pe, U20305093@utp.edu.pe, C25994@utp.edu.pe, C23941@utp.edu.pe*

Resumen

Existen diversas tecnologías implementadas en plataformas de comercio electrónico y bancarias para cumplir con las leyes de protección de datos y garantizar la eficiencia operativa. Sin embargo, se han identificado puntos fuertes y débiles en su aplicación que afectan su efectividad. Por lo tanto, el objetivo de este estudio fue analizar las principales tecnologías utilizadas en estas plataformas para cumplir con normativas como el Reglamento General de Protección de Datos y la California Consumer Privacy Act, y evaluar su impacto en la eficiencia operativa. Se utilizó un diseño no experimental, descriptivo, cualitativo-cuantitativo, correspondiente a una revisión sistemática de la literatura sin metaanálisis. Se seleccionaron 35 artículos de libre acceso de las bases de datos Scopus, Redalyc y Web of Science, siguiendo criterios de inclusión y exclusión específicos. Los resultados mostraron que las tecnologías clave como la encriptación y la gestión de identidades son fundamentales para el cumplimiento normativo, pero enfrentan desafíos relacionados con los altos costos de integración, la capacitación técnica y la resistencia cultural en algunas regiones. Se concluyó que, aunque estas tecnologías permiten un buen cumplimiento de las leyes de protección de datos, su efectividad varía según el marco regulatorio y la región. Se recomienda fomentar la innovación tecnológica y la cooperación intersectorial para superar las barreras económicas y operativas, y así garantizar un cumplimiento normativo más eficiente en plataformas digitales.

Palabras clave-- Protección de datos, Protección privada, Comercio electrónico, Seguridad de pago, RGPD

I. Introducción

En los últimos años, el crecimiento del comercio electrónico y plataformas digitales ha sido notable, con ventas minoristas globales que alcanzaron los 4,28 billones de dólares en 2020 e ingresos proyectados de 5,4 billones de dólares para el 2022, según un informe de Statista [1]. Este rápido incremento, acelerado aún más por la pandemia de COVID-19, colocó al comercio electrónico en una posición central en la venta al por menor aumentando los riesgos asociados con el uso indebido de datos personales [1] y con ello, la necesidad de proteger la información personal; lo que las ha impulsado a adoptar tecnologías avanzadas como la encriptación, la gestión de identidades y el monitoreo de seguridad para garantizar la seguridad de sus operaciones y cumplir con regulaciones estrictas como el Reglamento General de Protección de Datos (GDPR) en Europa [2], [3]. Como resultado, el cumplimiento de las leyes de protección de datos se ha convertido en una prioridad crucial para las empresas que realizan transacciones digitales, en especial, aquellas que manejan datos sensibles de clientes como nombres, documentos de identidad, números de tarjetas, cuentas bancarias, códigos de verificación, contraseñas y otros datos personales.

La privacidad se suele considerar como la capacidad de una persona o un grupo para auto determinar, proteger y compartir selectivamente la información sobre sí mismos, y esto se relaciona con el ámbito de la seguridad, que incluye elementos de confidencialidad y protección. Las leyes de privacidad en algunos países y naciones, incluso las constituciones, protegen el derecho a no ser expuesto a invasiones de privacidad por parte del gobierno, empresas o individuos. En particular, el GDPR ha establecido un precedente global, influenciando la adopción de regulaciones similares en otras regiones, como sería la California Consumer Privacy Act (CCPA)b en 2020 [2].

Por desgracia, este marco legal varía entre países, con diferentes grados de protección de datos personales y privacidad, lo que añade complejidad al comercio electrónico [1], pues afecta la capacidad de la empresa manejar datos y aplicar personalizaciones avanzadas sin infringir la privacidad del usuario [3]. Además, la integración de estas tecnologías en los sistemas existentes sigue siendo un desafío complejo y costoso, ya que las empresas deben encontrar un equilibrio entre la protección de datos y la eficiencia operativa [4].

Un ejemplo de la importancia de implementar tecnologías para poder garantizar la protección de datos, se evidencia en la comparación entre los modelos *"bussiness to consumer"* tradicionales y mejorados, donde se simuló la intrusión en la base de datos de una tienda en línea. En el modelo tradicional, la información sensible de los clientes, como números de tarjeta bancaria y contraseñas de pago, era accesible tras una intrusión exitosa. Sin embargo, en el modelo B2C mejorado, esta información estaba protegida mediante asteriscos conectados a un servidor de terceros, lo que impedía el acceso

directo tanto para el comerciante como para el intruso, mejorando significativamente la confidencialidad y protección de los usuarios [4]. Este tipo de tecnologías subrayan la importancia de adoptar medidas de protección de datos efectivas para proteger no solo a los clientes, sino también a las mismas empresas de verse afectadas por las sanciones que conlleva el incumplimiento de medidas preventivas; pues con la implementación de la nueva Ley de Protección de Datos Personales (LPDP) en febrero de 2020, se establecieron sanciones más estrictas para garantizar el cumplimiento de la normativa. Esta ley incrementa las multas en un 2% para las infracciones de categoría I y en un 4% para las infracciones de categoría II del ingreso anual total de las empresas. Estas medidas buscan asegurar que las entidades que procesan datos personales, incluidas aquellas que operan en el comercio electrónico, se alineen con las normativas europeas como el GDPR, reforzando la protección de los derechos de los ciudadanos y la confidencialidad de sus datos [1].

La situación actual evidencia la existencia de vacíos de conocimiento en la interacción entre las tecnologías de protección de datos y las normativas vigentes de cada país, lo que requiere una visión más amplia y un enfoque integral para abordar las vulnerabilidades en la protección de la información del cliente. Este estudio se motiva por la necesidad de revisar y entender cómo las empresas pueden mejorar la integración de tecnologías de protección de datos en sus sistemas y al mismo tiempo, asegurar el cumplimiento de las leyes, fortaleciendo así la confianza del consumidor en el comercio electrónico y bancas digitales [1], [2].

El objetivo general de este estudio es analizar y evaluar las tecnologías implementadas en el comercio electrónico y las plataformas bancarias para cumplir con las leyes de protección de datos, así como sus impactos en la eficiencia operativa.

Asimismo, es importante identificar las principales tecnologías de protección de datos empleadas en plataformas de comercio electrónico y bancarias, analizar cómo estas permiten a las empresas cumplir con el GDPR y otras leyes de privacidad en distintas regiones, y evaluar los desafíos operativos, económicos y técnicos que conlleva su integración, garantizando una visión integral de su implementación y efectividad.

En este documento, la sección II se describe la metodología de Revisión Sistemática de la Literatura (RSL), detallando el uso de la estrategia PICO para la formulación de las preguntas de investigación, así como los criterios de inclusión y exclusión empleados. La sección III presenta los resultados del análisis bibliométrico y la síntesis de la literatura revisada, destacando las tecnologías predominantes, los beneficios y los desafíos en la implementación de medidas de protección de datos en el comercio digital y la banca. La sección IV presenta la Discusión donde se examina e interpreta los hallazgos en relación con la literatura existente y los objetivos de la investigación, ofreciendo una perspectiva crítica sobre los resultados obtenidos. Finalmente, la sección V expone las conclusiones del estudio, proporcionando un resumen de las mejores prácticas y sugiriendo direcciones para futuras investigaciones en el cumplimiento de la normativa de protección de datos en plataformas digitales.

II. METODOLOGIA

Para el desarrollo exitoso de la revisión sistemática de la literatura, en la cual hablamos sobre la adaptación de las empresas al nuevo reglamento general de protección de datos, se empleó una metodología estricta, basada en una investigación minuciosa, en tres plataformas de bases de datos distintas: Scopus, Redalyc y web of science.

Con ese propósito, seguimos el modelo PICO como estrategia de desarrollo de la pregunta de investigación. Este es el método recomendado para desarrollar preguntas para revisiones, asegurando que todos los componentes a tener en cuenta sean definidos correctamente [5]. A partir de ello, llegamos a la formulación de la siguiente pregunta: **"¿Cómo han adaptado las empresas de comercio electrónico y banca digital sus plataformas tecnológicas para cumplir con las normativas de protección de datos como el GDPR, mientras mantienen sus funciones operativas?"** Junto con ello, las preguntas derivadas en base a cada componente, tal cual como se presenta en la tabla I:

TABLA I
PREGUNTAS DERIVADAS DESARROLLADAS DEL MODELO PICO

P	¿Cuáles son las empresas digitales que enfrentan desafíos en cumplir con las leyes de protección de datos mientras mantienen sus operaciones?
I	¿Qué tecnologías han implementado las empresas para cumplir con normativas de protección de datos y mantener la eficiencia operativa?
C	¿Cómo han adaptado estas tecnologías para garantizar la eficiencia operativa frente a los cambios en las normativas de protección de datos en diferentes regiones?
O	¿Qué tecnologías y políticas han sido efectivas para equilibrar el cumplimiento de normativas, las operaciones eficientes y para mantenerse al día con los cambios en la legislación?

Se igual manera, rescatamos las palabras clave que ayudaron a definir la ecuación de búsqueda, mostrado en la tabla II:

TABLA II
PALABRAS CLAVE DEFINIDAS

P	e-commerce, banking, website
I	GDPR, RGPD, data privacy laws
C	Compliance, regulations, data protection, data privacy, Sensitive data
O	Technologies, encryption, politics, policies, measures

Esta búsqueda de fuentes de información se llevó a cabo mediante una aplicación cuidadosa de las normas de inclusión y exclusión, lo que facilitó la generación de una ecuación de búsqueda uniforme para todas las bases de datos. Dicha ecuación permitió filtrar los documentos relevantes al tema de investigación, siendo la siguiente:

(TITLE-ABS-KEY (“e-commerce" OR "banking" OR "website”) AND TITLE-ABS-KEY (“GDPR" OR "RGPD" OR "data privacy laws") AND TITLE-ABS-KEY ("compliance" OR "regulations" OR "data protection" OR "data privacy" OR "sensitive data") AND TITLE-ABS-KEY ("technologies" OR "encryption" OR "politic" OR "policies" OR "measures"))

Bajo esta ecuación, se optó por utilizar el diagrama PRISMA, a través de esta herramienta, se registraron las 3 bases de datos utilizadas (Scopus, Redalyc y web of science) con un total de 116 artículos. Además, se definieron los criterios de inclusión y exclusión, como se presenta en las tablas III y IV.

TABLA III
Criterios de inclusión

CI1	Los estudios incluidos deben abordar el cumplimiento de normativas de protección de datos, como el GDPR u otras leyes, en empresas de comercio electrónico o banca digital.
CI2	Los estudios incluidos deben describir o analizar la implementación de tecnologías en la protección de datos personales y financieros.
CI3	Los estudios incluidos deben reportar resultados empíricos que evalúen el impacto de estas tecnologías en la seguridad de los datos y su cumplimiento regulatorio.
CI4	Los estudios incluidos deben haber sido publicados en los últimos 5 años para asegurar que el análisis se enfoque en tecnologías y regulaciones actuales.
CI5	Los estudios deben incluir análisis de cómo las tecnologías han sido integradas identificando los desafíos y soluciones para equilibrar el cumplimiento de normativas y las actividades operativas.

TABLA IV
Criterios de exclusión

CE1	Estudios que no aborden específicamente el cumplimiento de normativas de protección de datos en plataformas de comercio electrónico o banca digital.
CE2	Estudios que no incluyan análisis o descripciones detalladas de las tecnologías implementadas o que se enfoquen solo en aspectos legales sin el componente tecnológico.
CE3	Estudios que no estén disponibles en español o inglés.

En la fase de identificación, se registraron un total de 116 artículos provenientes de 3 bases de datos. Posteriormente, se eliminó 1 artículo por duplicidad, lo que dejó 115 registros para el cribado. Tras el cribado inicial, se excluyeron 55 artículos por no cumplir con los criterios de inclusión. De los registros analizados, se recuperaron 60 publicaciones para evaluación, mientras que 15 publicaciones no pudieron ser recuperadas. En la fase de evaluación de elegibilidad, se revisaron 45 publicaciones. Durante este proceso, se excluyeron 3 publicaciones que no cumplían con el criterio de exclusión CE 1, 12 publicaciones por CE 2 y 1 publicación por CE 3.

Finalmente, se seleccionaron 29 nuevos estudios que se incorporaron a la revisión sistemática, los cuales serán utilizados en el desarrollo de la investigación. En la figura 1 se presenta el diagrama PRISMA correspondiente, desarrollado en base al modelo presentado por Smirnova y Victoriano en [5]

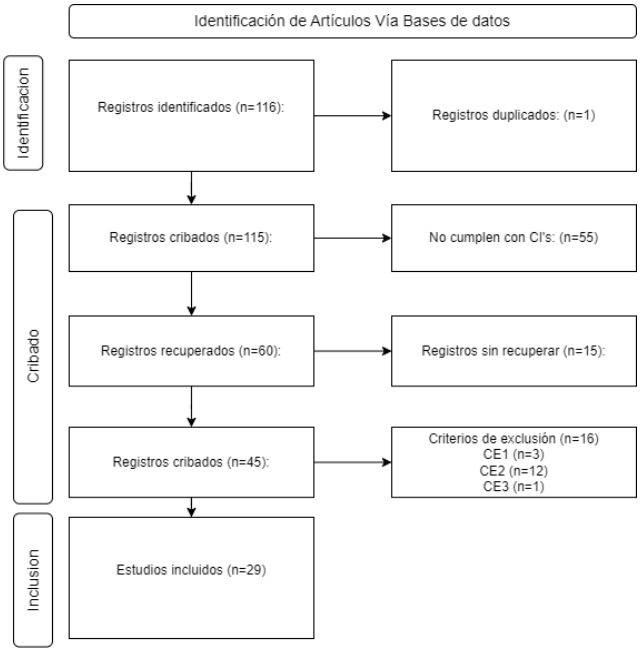

Fig. 1. Identificación de artículos vía metodología PRISMA

III. Resultados

Los resultados se estructuran en dos secciones principales para una comprensión integral del estudio: la primera, un análisis bibliométrico, que aborda la información general sobre los estudios seleccionados, así como sus características de publicación y distribución geográfica. La segunda sección se enfoca en la síntesis de los artículos seleccionados; la cual se organiza en función de las preguntas de investigación planteadas, permitiendo una integración de hallazgos clave en relación con los objetivos del estudio.

3.1. *Resultados bibliométricos.*

En el análisis bibliométrico, el estudio inició con una presentación de todas las investigaciones incluidas en la revisión sistemática. La Tabla V muestra en detalle la información de los autores junto con los títulos de cada investigación considerada en el análisis.

TABLA V
Relación de Artículos Analizados

Autores	**Titulo**
Serrado J, Pereira R, […] Scalabrin Bianchi [6]	Information security frameworks for assisting GDPR compliance in banking industry
Avendaño Carbellido O [7]	Los retos de la banca digital en México The challenges of electronic banking in Mexico
Enríquez O [8]	El derecho de protección de datos personales en los sistemas de inteligencia artificial
Belen Saglam R, Aslan C, […] Pogrebna G [9]	A Data-Driven Analysis of Blockchain Systems' Public Online Communications on GDPR
Urban T, Tatang D, […] Pohlmann N [10]	A Study on Subject Data Access in Online Advertising After the GDPR
Dorfleitner G, Hornuf L [11]	FinTech and data privacy in Germany: An empirical analysis with policy recommendations

Spalević Ž, Vićentijević K [12]	GDPR and challenges of personal data protection
Degeling M, Utz C, […] Holz T [13]	We Value Your Privacy ... Now Take Some Cookies: Measuring the GDPR's Impact on Web Privacy
Peukert C, Bechtold S, […] Kretschmer T [14]	Regulatory Spillovers and Data Governance: Evidence from the GDPR
Rahat T, Long M, Tian Y [15]	Is Your Policy Compliant? A Deep Learning-based Empirical Study of Privacy Policies Compliance with GDPR
Lakshmi K, Gupta H, Ranjan J [16]	Analysis of General Data Protection Regulation Compliance Requirements and Mobile Banking Application Security Challenges
Pikulík T, Štarchoň P [17]	Public registers with personal data under scrutiny of DPA regulators
Klein D, Rolle B, […] Johns M [18]	General Data Protection Runtime: Enforcing Transparent GDPR Compliance for Existing Applications
Bornschein R, Schmidt L, Maier E [19]	The Effect of Consumers' Perceived Power and Risk in Digital Information Privacy: The Example of Cookie Notices
Botunac I, Parlov N, Bosna J [20]	Opportunities of Gen AI in the Banking Industry with regards to the AI Act, GDPR, Data Act and DORA
Reuter C, Iacono L, Benlian A [21]	A quarter century of usable security and privacy research: transparency, tailorability, and the road ahead
Herder E, Van Maaren O [22]	Privacy Dashboards: The Impact of the Type of Personal Data and User Control on Trust and Perceived Risk
Rizou S, Alexandropoulou-Egyptiadou E, Psannis K [23]	Taxonomy about the Stages of Performing Automated Decision-Making Processing under GDPR in the Light of 6G Networks
Fabbri M [24]	Self-determination through explanation: an ethical perspective on the implementation of the transparency requirements for recommender systems set by the Digital Services Act of the European Union
Ou H, Fang Y, […] Huang C [25]	Viopolicy-Detector: An Automated Approach to Detecting GDPR Suspected Compliance Violations in Websites
Zambrano-Izurieta J, Mendoza-Barberán M, Farez-Arias M[26]	Funcionalidades de la Trazabilidad en el Desarrollo del Modelo de Comercio Electrónico B2C
Chin Y, Zhao J[27]	Governing Cross-Border Data Flows: International Trade Agreements and Their Limits
Abidi S, Essafi M, […] Ghezala H [28]	A web service security governance approach based on dedicated micro-services
Veale M, Borgesius F[29]	Adtech and Real-Time Bidding under European Data Protection Law
Batista M, Fernandes A, […] Ribeiro L [30]	Acceptance of the Cookie Notice and the creation of targeted advertising: a conscious decision or lack of information?
Pikulík T, Štarchoň P[31]	Public registers with personal data under scrutiny of DPA regulators
Gao X, Zhang W, […] Gao Y [32]	Product Authentication Technology Integrating Blockchain and Traceability Structure
Elliott K, Coopamootoo K, […] Van Moorsel A[33]	Know Your Customer: Balancing innovation and regulation for financial inclusion
Makhdoom I, Zhou I, […] Ni W [34]	PrivySharing: A Blockchain-based framework for integrity and privacy-preserving data sharing in Smart Cities

Los datos recopilados para esta Revisión Sistemática de la Literatura abarcan publicaciones de varios países, reflejando el enfoque internacional en la protección de datos y cumplimiento del GDPR [3], [11] .Como se observa en la figura 2, los países con mayor número de publicaciones incluyen Estados Unidos y Alemania, los cuales lideran en investigaciones relacionadas con la seguridad y privacidad de los datos [10], [18]. Esta tendencia indica un interés significativo en estos temas en dichos países, probablemente debido a sus estrictos marcos regulatorios y el impacto global de sus prácticas empresariales en tecnología y datos personales [19], [29].

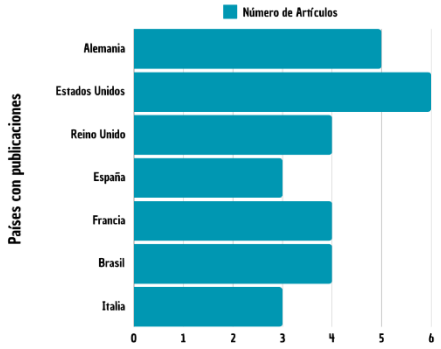

Fig. 2. Distribución cuantitativa de artículos seleccionados según país de publicación.

En la figura 3, se observa que los temas predominantes en los documentos de la RSL incluyen el cumplimiento de GDPR (27.6%), seguido por la protección de datos en empresas y la privacidad en la web, ambos representando un 20.7% [11], [29] de las publicaciones. Otros enfoques relevantes son la conversión de datos personales en datos que no se pueden utilizar para identificar a ningún individuo, también llamado anonimizar datos, con un 17.2% [10], [27] y los derechos de los usuarios con un 13.8%. Estos datos reflejan una concentración de estudios orientados hacia la implementación y cumplimiento de normativas de privacidad, así como la gestión de datos personales en diversos contextos empresariales y digitales [3], [18].

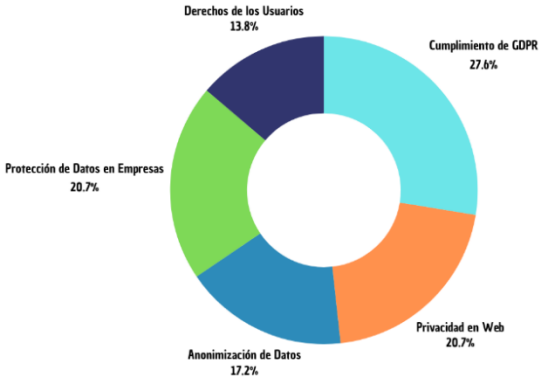

Fig. 3. Distribución cuantitativa de artículos seleccionados según tema principal.

Se llevó a cabo un análisis de las palabras clave más relevantes en los artículos seleccionados, donde "GDPR" aparece como el término central, reflejando el interés predominante en la regulación de datos en el contexto de plataformas de comercio electrónico y bancarias [12], [28], [29]. Otros términos destacados incluyen "Privacidad" y "Seguridad", resaltando la creciente preocupación por la seguridad de la información y la protección de los usuarios en operaciones digitales [11], [21].

Además, se identificaron términos como "Cumplimiento" y "Anonimización", que, aunque menos frecuentes, son cruciales para entender cómo las empresas implementan estrategias para adherirse a normativas sin comprometer la eficiencia operativa [13], [18], [29]. Estos términos alinean directamente con los objetivos de esta revisión, que busca identificar tecnologías efectivas y políticas adaptativas que permitan a las empresas digitales cumplir con las leyes de protección de datos en un entorno regulatorio en constante cambio [19], [31].

La figura 4 refleja visualmente la categorización de los temas principales abordados en la literatura revisada, brindando una perspectiva completa de las áreas prioritarias para el cumplimiento de normativas en el sector digital.

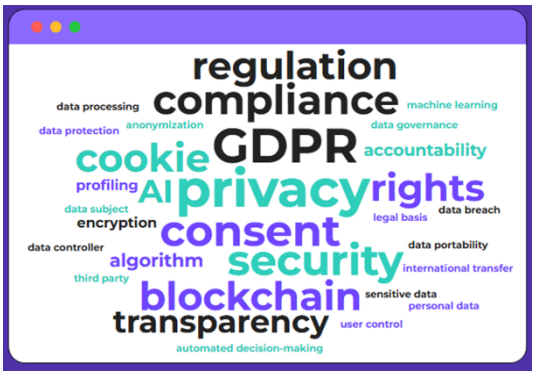

Fig. 4. Distribución cuantitativa de las palabras claves más comunes de los artículos seleccionados.

3.2. *Resultados basados en las preguntas pico.*

En esta sección se presentan los resultados del análisis y evaluación crítica de los artículos disponibles sobre tecnologías en comercio electrónico y plataformas bancarias para el cumplimiento de leyes de protección de datos, siguiendo la metodología PICO. La información se sintetiza a partir de los hallazgos más destacados, utilizando formularios de extracción que facilitan la respuesta a las preguntas de investigación formuladas en esta revisión sistemática de la literatura.

¿Cuáles son las empresas digitales que enfrentan desafíos en cumplir con las leyes de protección de datos mientras mantienen sus operaciones?

La adopción de tecnologías para cumplir con las leyes de protección de datos ha sido fundamental en varios sectores digitales, destacándose en sitios web, e-commerce y banca. En el ámbito bancario, el desarrollo de marcos de seguridad enfocados en el cumplimiento de GDPR ha permitido a las instituciones proteger la información sensible de sus clientes, aunque adaptar sistemas financieros tradicionales a estas normativas sigue siendo un reto complejo [6], [26]. Además, en contextos como el de la banca digital en México, se enfrenta el desafío de cumplir con regulaciones estrictas sin sacrificar la eficiencia operativa [7].

En el sector de e-commerce, el GDPR ha tenido un impacto directo en el uso de big data, lo cual obliga a las plataformas a buscar un equilibrio entre personalización de servicios y protección de la privacidad del usuario. Esto afecta la capacidad de las empresas para mantener su competitividad, especialmente en un entorno de comercio global donde las leyes de protección de datos varían según la región [3], [27]. Las normativas de privacidad, aunque restrictivas, también fomentan la innovación en tecnologías que aseguren la seguridad de los datos personales sin comprometer la eficacia de las operaciones [29].

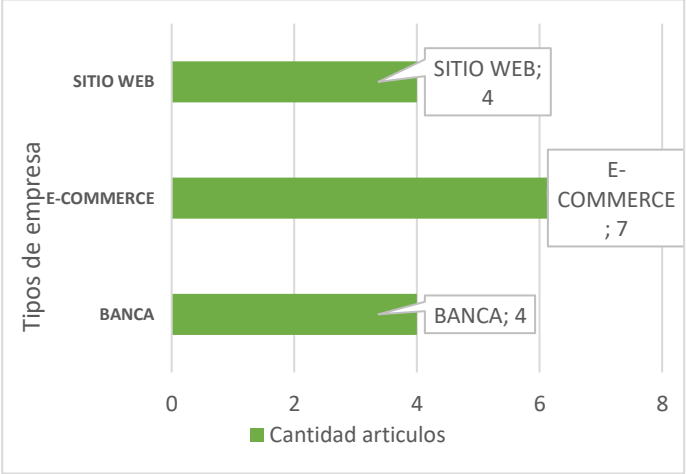

Fig. 5. Distribución cuantitativa de sectores clave para la implementación de normativas.

¿Qué tecnologías han implementado las empresas para cumplir con normativas de protección de datos y mantener la eficiencia operativa?

La adopción de diversas tecnologías ha sido clave para que las empresas logren cumplir con las normativas de protección de datos y mantengan la eficiencia operativa. Los sistemas de cumplimiento de GDPR representan una proporción significativa en las implementaciones, abordando directamente la necesidad de cumplir con la normativa a través de marcos de seguridad adaptativos en el sector bancario, como se describe en el trabajo de Serrado. [6]. Además, herramientas como el General Data Protection Runtime han sido desarrolladas para facilitar la transparencia en el cumplimiento normativo en aplicaciones existentes,

permitiendo una integración sin interrupciones en los sistemas actuales [18].

El uso de blockchain y seguridad de datos ha surgido como una tecnología innovadora para reforzar la protección de datos personales, con investigaciones que demuestran su potencial para almacenar información de forma segura y rastrear el cumplimiento de GDPR en sistemas públicos [9].

Las tecnologías de inteligencia artificial también han abierto oportunidades en el sector bancario para cumplir con regulaciones de privacidad, como muestra el trabajo de Botunac [20], que explora cómo la IA puede ayudar a mantener la eficiencia mientras se respeta el GDPR. En plataformas de comercio electrónico, el análisis de datos y su impacto en la personalización han planteado retos y oportunidades en cuanto al manejo ético y seguro de grandes volúmenes de datos, tal como lo discute [2].

Adicionalmente, el estudio sobre la automatización de redes 5G y 6G subraya cómo las futuras redes deben contemplar mecanismos de decisión automática que respeten el GDPR, demostrando que la tecnología de redes avanzadas también juega un papel en la conformidad normativa [23].

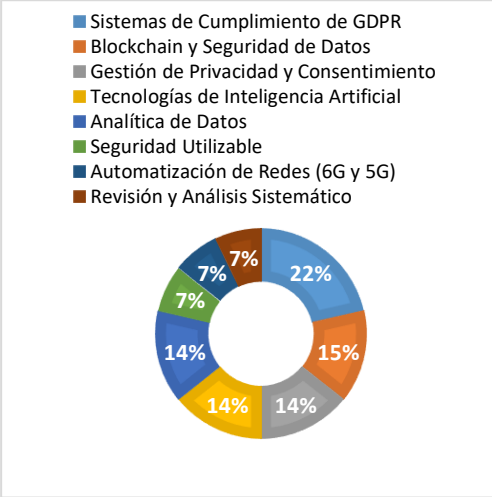

Fig. 6. Distribución cuantitativa de principales tecnologías para la protección de datos y eficiencia operativa.

¿Cómo han adaptado estas tecnologías para garantizar la eficiencia operativa frente a los cambios en las normativas de protección de datos en diferentes regiones?

En respuesta a los desafíos planteados por las normativas de protección de datos, como el GDPR en Europa, el CCPA en California y la Ley de Protección de Información Personal de Singapur (PDPA), las empresas tecnológicas y financieras han implementado diversos enfoques tecnológicos y operativos para adaptarse a estos cambios y garantizar la eficiencia en sus operaciones. Según el análisis realizado en los documentos, uno de los enfoques más comunes ha sido el de "Privacy by Design," el cual incorpora la privacidad desde la fase inicial del desarrollo de productos y sistemas, minimizando así la recopilación y almacenamiento de datos personales y limitando su procesamiento solo a lo necesario para el funcionamiento de la aplicación. Esta medida no solo reduce riesgos legales y de seguridad, sino que además optimiza recursos y promueve la confianza de los usuarios, logrando así una mayor eficiencia operativa en entornos de alta regulación como el europeo [16].

Otro aspecto destacado en los estudios es la adopción de tecnologías avanzadas como el uso de sistemas de anonimización de datos y de perfiles automatizados que cumplen con la normativa de derecho de los datos sujetos, como el derecho a ser olvidado y la rectificación de datos, sin comprometer la capacidad de análisis o la personalización de servicios [23]. En el caso de las FinTech en Alemania, por ejemplo, se implementan medidas específicas para la protección de datos sensibles como datos financieros, garantizando la seguridad sin afectar la funcionalidad, lo cual se convierte en un diferenciador competitivo [11]. De esta manera, las empresas no solo logran cumplir con las regulaciones de cada región, sino que también aprovechan estas adaptaciones para fortalecer sus modelos de negocio, ofreciendo una experiencia segura y transparente que responde a las expectativas de un consumidor cada vez más consciente y exigente en términos de privacidad.

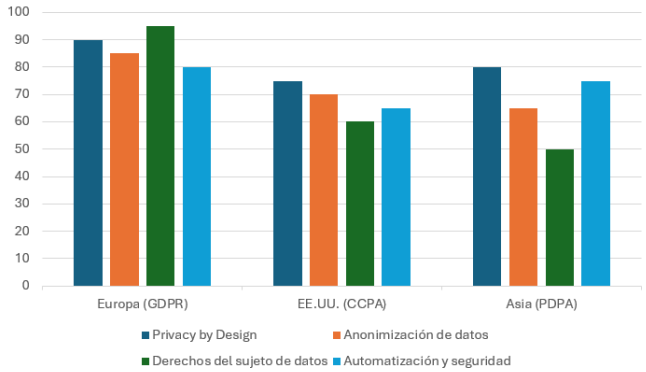

Fig. 7. Comparativa de enfoques de protección de datos en Europa, EE. UU. Y Asia

¿Qué tecnologías y políticas han sido efectivas para equilibrar el cumplimiento de normativas, las operaciones eficientes y para mantenerse al día con los cambios en la legislación?

El análisis de diversas tecnologías y políticas de cumplimiento muestra que herramientas como los dashboards de privacidad y los sistemas de rastreo de flujo de información son altamente efectivas en la categoría de cumplimiento normativo y mantienen una eficiencia operativa moderada. Por ejemplo, los dashboards de privacidad permiten a los usuarios visualizar y gestionar su información personal, promoviendo una mayor transparencia y confianza en el cumplimiento del Reglamento General de Protección de Datos, aunque su capacidad de adaptación a cambios legislativos es limitada [22]. Por otro lado, el rastreo de flujo

de información, que facilita el etiquetado y seguimiento de datos sin intervención directa en el código, destaca no solo por su alta puntuación en cumplimiento normativo, sino también por su adaptabilidad en entornos legislativos cambiantes [18], [19].

Herramientas como Viopolicy-Detector muestran una alta capacidad de adaptación al cambio legislativo, permitiendo la detección automática de posibles violaciones al GDPR en tiempo real. Este enfoque asegura que las empresas puedan realizar ajustes proactivos en sus operaciones de acuerdo con nuevas regulaciones sin comprometer la eficiencia de sus operaciones [25]. La inteligencia artificial generativa, aplicada en el sector bancario, es notable por su alta eficiencia operativa, aunque su desempeño en cumplimiento normativo es menor. Esta tecnología se encuentra en una fase de optimización para alinearse con leyes como el Acta de IA y el GDPR, equilibrando así el cumplimiento de normativas con una operación competitiva y adaptable a cambios futuros [20].

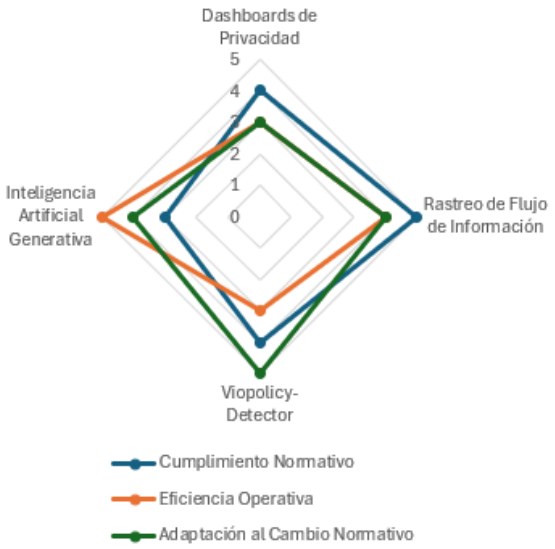

Fig. 8. Evaluación comparativa de tecnologías y políticas en cumplimiento normativo, eficiencia operativa y adaptación legislativa

IV. Discusión

En esta sección se analizará el impacto de la implementación de la ley de protección de datos y la GDPR en el e-commerce y la banca digital, basándonos en los hallazgos de nuestra revisión sistemática de la literatura (RSL). Este análisis se ha realizado mediante una metodología estructurada, asegurando una evaluación completa de los estudios existentes.

- **Innovación y Competitividad en la Banca Digital.**

La implementación de la GDPR ha tenido un impacto significativo en la competitividad de las instituciones financieras, especialmente en el ámbito de la banca digital. Las instituciones que han adoptado marcos de seguridad robustos han mejorado su capacidad para cumplir con los requisitos de la GDPR, lo que ha incrementado la confianza de los usuarios en la protección de sus datos [6], [7]. Sin embargo, varios estudios han señalado que las pequeñas instituciones bancarias y las ubicadas en mercados emergentes enfrentan dificultades en la implementación de estos marcos de seguridad debido a la falta de infraestructura adecuada y resistencia al cambio [7], [8]. Este contraste muestra que, aunque los avances en la digitalización permiten a algunas instituciones competir a nivel global, otras siguen luchando con los aspectos técnicos y regulatorios necesarios para cumplir con la GDPR [6], [9].

- **Desafíos Tecnológicos en la Implementación de la GDPR.**

La integración de tecnologías emergentes, como la inteligencia artificial (IA) y blockchain, plantea grandes desafíos en la implementación de la GDPR. Por un lado, la IA permite procesar grandes volúmenes de datos, pero también presenta dificultades para garantizar el cumplimiento de los derechos de los usuarios, especialmente en términos de transparencia y derecho al olvido [8], [9], [10]. En un análisis paralelo, los estudios de Urban [35] y Pikulík y Štarchoň [17] destacan que el uso de blockchain, aunque promueve la seguridad y la trazabilidad de los datos, entra en conflicto con los principios de la GDPR debido a la naturaleza inmutable de los datos almacenados, lo que dificulta su eliminación según los requerimientos de la normativa [9], [10]. Estos hallazgos subrayan la necesidad de adoptar enfoques más flexibles que integren tecnologías emergentes con los principios de la GDPR.

- **Herramientas Automatizadas para Detectar Incumplimientos**

El uso de herramientas automatizadas para detectar violaciones de la GDPR es clave para mejorar el cumplimiento en el e-commerce y la banca digital. Herramientas como Viopolicy-Detector han mostrado eficacia en la detección de violaciones en tiempo real, analizando políticas de privacidad y comportamientos de recolección de datos [15], [16]. Sin embargo, aunque estas herramientas son valiosas, no pueden garantizar el cumplimiento total. Veale y Borgesius [29] y Lakshmi [16] señalan que, a pesar de las mejoras en las herramientas automatizadas, sigue existiendo una brecha significativa en la implementación efectiva de la GDPR, especialmente en plataformas que no implementan mecanismos claros de consentimiento. La integración de auditorías manuales junto con las herramientas automatizadas parece ser una solución más efectiva para abordar los desafíos regulatorios [15], [16], [18].

- **Gobernanza de los Flujos de Datos Transfronterizos**

Uno de los mayores desafíos derivados de la GDPR es la gobernanza de los flujos de datos transfronterizos. Rahat [15] y Rizou [23] analizan cómo las diferencias en las regulaciones de privacidad entre la UE y otros países, como los EE. UU., dificultan la implementación uniforme de la GDPR. Las

tensiones regulatorias surgen debido a la disparidad en las normas de privacidad y el control de los datos, lo que complica las transferencias de datos a nivel global [13], [23]. A pesar de estos desafíos, estudios como el de Abidi [28] proponen que la adopción de herramientas tecnológicas avanzadas para monitorear y controlar los flujos de datos transfronterizos puede facilitar el cumplimiento global de la normativa, pero aún se necesitan acuerdos internacionales para garantizar la coherencia en las políticas de privacidad [23], [28].

V. CONCLUSIONES.

La revisión sistemática permitió analizar y evaluar las tecnologías implementadas en plataformas de comercio electrónico y bancarias para cumplir con las leyes de protección de datos y su impacto en la eficiencia operativa. Entre las principales tecnologías identificadas se encuentran la encriptación, la gestión de identidades y la anonimización, las cuales desempeñan un papel crucial en la protección de datos sensibles y el cumplimiento de normativas como el GDPR y el CCPA. El análisis evidenció que dichas tecnologías han permitido a las empresas adaptarse a las normativas internacionales, lo que facilita un equilibrio entre la protección de datos y la eficiencia operativa. No obstante, los resultados también revelan desafíos significativos en la implementación, entre ellos altos costos de integración, la necesidad de capacitación técnica y la resistencia cultural en algunos contextos.

Asimismo, se concluye que, aunque las tecnologías actuales proporcionan una base sólida para el cumplimiento normativo, su efectividad varía según las regiones y el marco regulatorio.

Por ello, se recomienda fomentar la innovación tecnológica y la cooperación intersectorial para superar las barreras económicas, operativas y culturales, garantizando así una mayor eficiencia y cumplimiento normativo en plataformas digitales.

REFERENCIAS

[1] B. Nuredini, J. Xhafaj, and V. P. Dodevska, “A Comparative Overview of Data Protection in e-Commerce in the European Union, the United States of America, the Republic of North Macedonia, and Albania: Models and Speciics | Prawnoporównawcze ujęcie zasad ochrony danych osobowych w handlu elektroniczny,” *Studia Iuridica Lublinensia*, vol. 31, no. 3, pp. 61–84, 2022, doi: 10.17951/sil.2022.31.3.61-84.

[2] M. Haddara, A. Salazar, and M. Langseth, “Exploring the impact of GDPR on big data analytics operations in the E-commerce industry,” in *Procedia Computer Science*, Elsevier B.V., 2023, pp. 767–777. doi: 10.1016/j.procs.2023.01.350.

[3] M. A. Farhad, “Consumer data protection laws and their impact on business models in the tech industry,” *Telecomm Policy*, vol. 48, no. 9, Oct. 2024, doi: 10.1016/j.telpol.2024.102836.

[4] Z. Wang, “Research on e-commerce payment security and privacy protection based on improved b2c model,” *International Journal of Circuits, Systems and Signal Processing*, vol. 14, pp. 520–525, 2020, doi: 10.46300/9106.2020.14.67.

[5] Y. Smirnova and V. Travieso-Morales, “Understanding challenges of GDPR implementation in business enterprises: a systematic literature review,” Apr. 04, 2024, *Emerald Publishing*. doi: 10.1108/IJLMA-08-2023-0170.

[6] J. Serrado, R. F. Pereira, M. Mira da Silva, and I. Scalabrin Bianchi, “Information security frameworks for assisting GDPR compliance in banking industry,” *Digital Policy, Regulation and Governance* , vol. 22, no. 3, pp. 227–244, Sep. 2020, doi: 10.1108/DPRG-02-2020-0019.

[7] O. Avendaño Carbellido, “Los retos de la banca digital en México* The challenges of electronic banking in Mexico,” 2018. [Online]. Available: http://portafolioinfo.cnbv.gob.mx/Paginas/Contenidos.aspx?ID=37&-

[8] O. A. M. Enríquez, “El derecho de protección de datos personales en los sistemas de inteligencia artificial,” *REVISTA IUS*, vol. 15, no. 48, Jun. 2021, doi: 10.35487/rius.v15i48.2021.743.

[9] R. Belen Saglam, C. B. Aslan, S. Li, L. Dickson, and G. Pogrebna, “A Data-Driven Analysis of Blockchain Systems’ Public Online Communications on GDPR,” in *Proceedings - 2020 IEEE International Conference on Decentralized Applications and Infrastructures, DAPPS 2020*, Institute of Electrical and Electronics Engineers Inc., Aug. 2020, pp. 22–31. doi: 10.1109/DAPPS49028.2020.00003.

[10] T. Urban, D. Tatang, M. Degeling, T. Holz, and N. Pohlmann, “A Study on Subject Data Access in Online Advertising After the GDPR,” in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, Springer, 2019, pp. 61–79. doi: 10.1007/978-3-030-31500-9_5.

[11] G. Dorfleitner and L. Hornuf, *FinTech and data privacy in Germany: An empirical analysis with policy recommendations*. Springer International Publishing, 2019. doi: 10.1007/978-3-030-31335-7.

[12] Ž. Spalević and K. Vićentijević, “GDPR and challenges of personal data protection,” *The European Journal of Applied Economics*, vol. 19, no. 1, pp. 55–65, 2022, doi: 10.5937/ejae19-36596.

[13] M. Degeling, C. Utz, C. Lentzsch, H. Hosseini, F. Schaub, and T. Holz, “We Value Your Privacy ... Now Take Some Cookies: Measuring the GDPR’s Impact on Web Privacy,” in *26th Annual Network and Distributed System Security Symposium, NDSS 2019*, The Internet Society, 2019. doi: 10.14722/ndss.2019.23378.

[14] C. Peukert, S. Bechtold, M. Batikas, and T. Kretschmer, “Regulatory Spillovers and Data Governance: Evidence from the GDPR,” *Marketing Science*, vol. 41, no. 4, pp. 318–340, Jul. 2022, doi: 10.1287/mksc.2021.1339.

[15] T. Al Rahat, M. Long, and Y. Tian, “Is Your Policy Compliant? A Deep Learning-based Empirical Study of Privacy Policies Compliance with GDPR,” in *WPES 2022 - Proceedings of the 21st Workshop on Privacy in the Electronic Society, co-located with CCS 2022*, Association for Computing Machinery, Inc, Nov. 2022, pp. 89–102. doi: 10.1145/3559613.3563195.

[16] K. K. Lakshmi, H. Gupta, and J. Ranjan, *Analysis of General Data Protection Regulation Compliance Requirements and Mobile Banking Application Security Challenges*. IEEE, 2020.

[17] T. Pikulík and P. Štarchoň, “Public registers with personal data under scrutiny of DPA regulators,” in *Procedia Computer Science*, Elsevier B.V., 2020, pp. 1170–1179. doi: 10.1016/j.procs.2020.03.033.

[18] D. Klein, B. Rolle, T. Barber, M. Karl, and M. Johns, “General Data Protection Runtime: Enforcing Transparent GDPR Compliance for

Existing Applications," in *CCS 2023 - Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security*, Association for Computing Machinery, Inc, Nov. 2023, pp. 3343–3357. doi: 10.1145/3576915.3616604.

[19] R. Bornschein, L. Schmidt, and E. Maier, "The Effect of Consumers' Perceived Power and Risk in Digital Information Privacy: The Example of Cookie Notices," *Journal of Public Policy and Marketing*, vol. 39, no. 2, pp. 135–154, Apr. 2020, doi: 10.1177/0743915620902143.

[20] I. Botunac, N. Parlov, and J. Bosna, "Opportunities of Gen AI in the Banking Industry with regards to the AI Act, GDPR, Data Act and DORA," in *2024 13th Mediterranean Conference on Embedded Computing, MECO 2024*, Institute of Electrical and Electronics Engineers Inc., 2024. doi: 10.1109/MECO62516.2024.10577936.

[21] C. Reuter, L. Lo Iacono, and A. Benlian, "A quarter century of usable security and privacy research: transparency, tailorability, and the road ahead," 2022, *Taylor and Francis Ltd.* doi: 10.1080/0144929X.2022.2080908.

[22] E. Herder and O. Van Maaren, "Privacy Dashboards: The Impact of the Type of Personal Data and User Control on Trust and Perceived Risk," in *UMAP 2020 Adjunct - Adjunct Publication of the 28th ACM Conference on User Modeling, Adaptation and Personalization*, Association for Computing Machinery, Inc, Jul. 2020, pp. 169–174. doi: 10.1145/3386392.3399557.

[23] S. Rizou, E. Alexandropoulou-Egyptiadou, and K. E. Psannis, "Taxonomy about the Stages of Performing Automated Decision-Making Processing under GDPR in the Light of 6G Networks," in *2020 3rd World Symposium on Communication Engineering, WSCE 2020*, Institute of Electrical and Electronics Engineers Inc., Oct. 2020, pp. 23–27. doi: 10.1109/WSCE51339.2020.9275570.

[24] M. Fabbri, "Self-determination through explanation: an ethical perspective on the implementation of the transparency requirements for recommender systems set by the Digital Services Act of the European Union," in *AIES 2023 - Proceedings of the 2023 AAAI/ACM Conference on AI, Ethics, and Society*, Association for Computing Machinery, Inc, Aug. 2023, pp. 653–661. doi: 10.1145/3600211.3604717.

[25] H. Ou, Y. Fang, Y. Guo, W. Guo, and C. Huang, "Viopolicy-Detector: An Automated Approach to Detecting GDPR Suspected Compliance Violations in Websites," in *ACM International Conference Proceeding Series*, Association for Computing Machinery, Oct. 2022, pp. 409–430. doi: 10.1145/3545948.3545952.

[26] J. P. Zambrano-Izurieta, M. G. Mendoza-Barberán, and M. del R. Farez-Arias, "Funcionalidades de la Trazabilidad en el Desarrollo del Modelo de Comercio Electrónico B2C," *Economía y Negocios*, vol. 14, no. 1, pp. 135–148, Jan. 2023, doi: 10.29019/eyn.v14i1.1057.

[27] Y. C. Chin and J. Zhao, "Governing Cross-Border Data Flows: International Trade Agreements and Their Limits," *Laws*, vol. 11, no. 4, Aug. 2022, doi: 10.3390/laws11040063.

[28] S. Abidi, M. Essafi, C. G. Guegan, M. Fakhri, H. Witti, and H. H. Ben Ghezala, "A web service security governance approach based on dedicated micro-services," in *Procedia Computer Science*, Elsevier B.V., 2019, pp. 372–386. doi: 10.1016/j.procs.2019.09.192.

[29] M. Veale and F. Z. Borgesius, "Adtech and Real-Time Bidding under European Data Protection Law," *German Law Journal*, vol. 23, no. 2, pp. 226–256, Mar. 2022, doi: 10.1017/glj.2022.18.

[30] M. Batista, A. Fernandes, A. Sabino, and L. P. Ribeiro, "Acceptance of the Cookie Notice and the creation of targeted advertising: a conscious decision or lack of information?," *RISTI - Revista Iberica de Sistemas e Tecnologias de Informacao*, vol. 2021, no. 43, pp. 75–92, Sep. 2021, doi: 10.17013/risti.43.75-92.

[31] T. Pikulík and P. Štarchoň, "Public registers with personal data under scrutiny of DPA regulators," in *Procedia Computer Science*, Elsevier B.V., 2020, pp. 1170–1179. doi: 10.1016/j.procs.2020.03.033.

[32] X. Gao, W. Zhang, B. Zhao, J. Zhang, J. Wang, and Y. Gao, "Product Authentication Technology Integrating Blockchain and Traceability Structure," *Electronics (Switzerland)*, vol. 11, no. 20, 2022, doi: 10.3390/electronics11203314.

[33] K. Elliott *et al.*, "Know Your Customer: Balancing innovation and regulation for financial inclusion," *Data Policy*, vol. 4, no. 1, Oct. 2022, doi: 10.1017/dap.2022.23.

[34] I. Makhdoom, I. Zhou, M. Abolhasan, J. Lipman, and W. Ni, "PrivySharing: A Blockchain-based framework for integrity and privacy-preserving data sharing in Smart Cities," in *ICETE 2019 - Proceedings of the 16th International Joint Conference on e-Business and Telecommunications*, SciTePress, 2019, pp. 363–371. doi: 10.5220/0007829803630371.