AulaVirtual
Generando Conocimiento

ISSN: 2665-0398

ENTRE LA INNOVACIÓN Y LA REGULACIÓN: EVALUACIÓN SISTEMÁTICA DE LA PRIVACIDAD DE DATOS EN EL USO FINANCIERO DEL MACHINE LEARNING

BETWEEN INNOVATION AND REGULATION: A SYSTEMATIC ASSESSMENT OF DATA PRIVACY IN THE FINANCIAL USE OF MACHINE LEARNING

Tipo de Publicación: Articulo Científico
Recibido: 06/10/2025
Aceptado: 07/11/2025
Publicado: 15/12/2025
Código Único AV: e586
Páginas: 1(2268-2285)
DOI: https://doi.org/10.5281/zenodo.17945309

Autores:
Juan Carlos Larrea Abad
Contador Público
Máster Universitario en Gestión Financiera y Auditoría de la Empresa
https://orcid.org/0009-0003-6860-2382
E-mail: jcla1293@gmail.com
Afiliación: Universidad Nacional de Piura
País: República del Perú

Yojani Maria Abad Sullon
Licenciada en Ciencias Administrativas
Doctor en Ciencias Administrativas, mención en Dirección en Empresas
https://orcid.org/0000-0001-5363-2085
E-mail: yabads@unp.edu.pe
Afiliación: Universidad Nacional de Piura
País: República del Perú

Andy Williams Chamoli Falcón
Abogado
Doctor en Gestión Empresarial
https://orcid.org/0000-0002-2758-1867
E-mail: andy.chamoli@udh.edu.pe
Afiliación: Universidad de Huánuco
País: República del Perú

Resumen

El uso intensivo de machine learning en el sector financiero ha transformado la forma en que las instituciones procesan y analizan grandes volúmenes de datos para la toma de decisiones, mejorando la eficiencia y precisión en la gestión de riesgos e inversiones. Sin embargo, esta evolución tecnológica plantea serios desafíos en torno a la privacidad, la protección de los datos personales y la responsabilidad algorítmica, especialmente en contextos donde la regulación no avanza al mismo ritmo que la innovación. El objetivo de este estudio fue evaluar las implicaciones de privacidad derivadas del uso de datos en machine learning para la toma de decisiones financieras, con énfasis en la regulación existente y las brechas en su aplicación. Se desarrolló un artículo de revisión sistemática bajo los lineamientos PRISMA 2020, abarcando publicaciones indexadas en Scopus, Web of Science y SciELO durante los últimos cinco años. Los resultados revelan deficiencias significativas en la armonización normativa internacional, en la trazabilidad de los modelos algorítmicos y en la aplicación de tecnologías de mejora de privacidad, pese a sus avances teóricos. En conclusión, se evidencia la necesidad urgente de marcos regulatorios adaptativos y de una gobernanza algorítmica que integre la ética, la transparencia y la protección efectiva de los datos en el ecosistema financiero digital.

Palabras Clave Privacidad de datos, machine learning, regulación financiera, tecnologías de mejora de privacidad, gobernanza algorítmica

Abstract

The intensive use of machine learning in the financial sector has transformed the way institutions process and analyze large volumes of data for decision-making, improving efficiency and accuracy in risk and investment management. However, this technological evolution poses serious challenges regarding privacy, personal data protection, and algorithmic accountability, especially in contexts where regulation has not kept pace with innovation. The objective of this study was to assess the privacy implications of using data in machine learning for financial decision-making, with an emphasis on existing regulations and gaps in their application. A systematic review article was developed under the PRISMA 2020 guidelines, encompassing publications indexed in Scopus, Web of Science, and SciELO over the past five years. The results reveal significant gaps in international regulatory harmonization, in the traceability of algorithmic models, and in the application of privacy-enhancing technologies, despite theoretical advances. In conclusion, there is an urgent need for adaptive regulatory frameworks and algorithmic governance that integrates ethics, transparency, and effective data protection in the digital financial ecosystem.

Keywords Data privacy, machine learning, financial regulation, privacy-enhancing technologies, algorithmic governance

Introducción

El uso creciente del *machine learning* (ML) en la analítica predictiva ha transformado radicalmente la toma de decisiones financieras en las empresas. La capacidad de estos algoritmos para extraer patrones de grandes volúmenes de datos ha generado nuevas oportunidades para identificar tendencias, prever riesgos y optimizar inversiones. Sin embargo, este desarrollo está acompañado de desafíos significativos relacionados con la privacidad de los datos y las implicaciones éticas que surgen de su aplicación en contextos financieros. Según Hamed (2023), la falta de transparencia en los algoritmos de decisión plantea serias preocupaciones respecto de la protección de los derechos de privacidad de los individuos en un entorno digital cada vez más regulado.

A medida que las instituciones financieras adoptan estrategias basadas en ML, las cuestiones de privacidad se vuelven más complejas. Esto se debe a la necesidad de manejar información altamente sensible, donde la intrusión en la privacidad de los clientes puede generar consecuencias legales y reputacionales graves. Liu et al., (2023) sostienen que la evolución de la legislación, como el Reglamento General de Protección de Datos (GDPR) en la Unión Europea, ha establecido un marco regulativo que busca salvaguardar la confidencialidad de los datos, aunque aún presenta brechas que pueden ser explotadas por tecnologías emergentes de ML.

A pesar de los beneficios inherentes al uso de ML en finanzas, como la mejora en la precisión de las predicciones y la eficiencia operativa, los estudios indican que las organizaciones enfrentan retos significativos en su implementación debido a la regulación insuficiente y la falta de claridad en las mejores prácticas. Tufail et al., (2023) subrayan que los problemas de privacidad relacionados con el uso de datos en ML frecuentemente no son abordados con profundidad por las empresas, lo que incrementa el riesgo de incumplimiento normativo.

Asimismo, Dhabliya et al., (2024) destacan la importancia de desarrollar ecosistemas seguros de ML que no solo se centren en el rendimiento del modelo, sino que también prioricen la privacidad de los datos como un pilar fundamental en su diseño y operación. La capacidad de las empresas para navegar este panorama regulatorio diverso, mientras aprovechan las ventajas competitivas ofrecidas por el ML, resulta esencial para su sostenibilidad y éxito futuro.

En los últimos años, se ha observado un creciente interés en la investigación sobre las implicaciones de privacidad derivadas del uso de datos en ML para la toma de decisiones financieras. Este interés se debe no solo a la rápida adopción de ML en el sector financiero, sino también a la creciente relevancia de la privacidad y la ética en el

ISSN: 2665-0398

manejo de datos sensibles. Uno de los estudios más significativos en este campo es el de Akash et al., (2024), quienes investigan métodos para mejorar la privacidad de los datos en sectores como la analítica y las finanzas. Su investigación destaca la efectividad de las Tecnologías de Mejora de Privacidad (*Privacy-Enhancing Technologies*, PETs), como el aprendizaje federado y la privacidad diferencial, en la protección de información sensible en entornos empresariales.

Otro hito relevante es el trabajo de Liu et al., (2023), que aborda las preocupaciones de privacidad en el contexto de la transformación digital. Este estudio enfatiza que la creciente adopción de algoritmos de ML plantea riesgos sustanciales para la privacidad de los datos personales, lo que podría obstaculizar la transformación exitosa de las organizaciones en el sector financiero. El análisis detallado de este problema permite comprender mejor cómo las regulaciones existentes pueden responder a dichos desafíos.

Por su parte, Hamed (2023) ofrece una visión crítica sobre los desafíos éticos y la privacidad en el uso de *big data* en la toma de decisiones. En su estudio se discuten las implicaciones éticas de los modelos de decisión basados en ML y se plantea la necesidad de un marco regulatorio más sólido que contemple las preocupaciones de privacidad y el uso indebido de los datos. Esta perspectiva resulta esencial para orientar las políticas que rigen el uso de datos en la toma de decisiones financieras.

De igual forma, Qi et al., (2023) presentan avances en el aprendizaje federado, centrados en la transferencia de conocimiento en modelos descentralizados, lo que ayuda a mitigar los riesgos de privacidad de los usuarios durante el proceso de intercambio de información. Esta innovación tiene el potencial de redefinir la manera en que las instituciones financieras manejan y comparten datos sin comprometer la confidencialidad.

En esa misma línea, Zhang (2022) explora un modelo de aprendizaje federado para el diagnóstico en entornos de salud digital, el cual resulta pertinente para el sector financiero al abordar las barreras de privacidad que enfrenta el análisis de modelos predictivos en contextos donde el uso compartido de datos es crítico. Este estudio demuestra cómo las técnicas de protección pueden aplicarse en entornos colaborativos, inspirando posibles soluciones en el ámbito financiero.

En conjunto, estos estudios resaltan la importancia de abordar la privacidad y las regulaciones dentro del contexto del ML aplicado a las decisiones financieras. La identificación de brechas en la regulación existente y la evaluación de las mejores prácticas son esenciales para garantizar un uso ético y responsable de estas tecnologías.

Revista Aula Virtual, ISSN: 2665-0398; Periodicidad: Continua
Volumen: 6, Número: 13, Año: 2025 (Continua-2025)

En la revisión de la literatura actual sobre las implicaciones de privacidad relacionadas con el uso de datos en ML para la toma de decisiones financieras, se han identificado diversos vacíos que justifican la pertinencia del objetivo de investigación propuesto. A continuación, se discuten cinco de estos vacíos clave.

En primer lugar, Mohammed et al., (2025) señalan que, a pesar de la existencia de marcos regulativos como el GDPR, aún persisten deficiencias significativas en la protección efectiva de datos sensibles en prácticas de ML aplicadas a las finanzas. Este estudio resalta la falta de claridad sobre cómo aplicar dichos marcos en situaciones específicas, lo que genera incertidumbre para las entidades financieras.

Por otra parte, Talukder & Shompa (2024) enfatizan la necesidad de desarrollar políticas regulatorias que evolucionen al mismo ritmo que las tecnologías de ML. Este vacío evidencia la falta de agilidad en la adaptación de regulaciones capaces de abordar los riesgos emergentes asociados con la privacidad, lo que puede derivar en lagunas legales que expongan a los consumidores a riesgos.

Asimismo, Akash et al., (2024) destacan las limitaciones de las PETs y su integración con las normativas existentes. Aunque estas tecnologías pueden contribuir a mitigar los riesgos de privacidad, la falta de investigaciones que exploren su aplicación efectiva en el ámbito financiero deja un vacío crítico en la comprensión de su implementación dentro de un marco regulativo adecuado.

Otro vacío relevante es identificado por Wirth et al., (2021), quienes evidencian que la infraestructura actual de compartición de datos en la investigación médica no se traduce adecuadamente al contexto financiero, lo que agrava los problemas de privacidad al carecer de soluciones adaptadas a esta área. Esto sugiere que las estrategias exitosas en otros sectores no necesariamente son aplicables a las finanzas, destacando la necesidad de estudios específicos en este campo.

Finalmente, Hockstad et al., (2024) sostienen que los desafíos en materia de ciberseguridad, especialmente en relación con las transacciones financieras, no han sido integrados de manera adecuada en las discusiones sobre regulación y privacidad. Este vacío evidencia la necesidad de investigar medidas efectivas que aseguren que las tecnologías emergentes no vulneren los derechos de privacidad.

Estos vacíos ponen de manifiesto la urgencia de realizar una investigación sistemática que aborde las implicaciones de privacidad en el uso de datos para la toma de decisiones financieras, considerando tanto la regulación existente como las brechas que requieren atención.

El objetivo de este artículo es evaluar las implicaciones de privacidad derivadas del uso de

ISSN: 2665-0398

datos en *machine learning* para la toma de decisiones financieras, con énfasis en la regulación existente y las brechas en su aplicación. Esta evaluación no solo busca identificar y analizar la efectividad de las normativas actuales en la protección de datos, sino también proponer recomendaciones que aborden las lagunas encontradas en la literatura y ofrezcan un marco más cohesivo y aplicable a la realidad del sector financiero.

Metodología

Para la realización de esta revisión sistemática, se aplicó el método PRISMA (Preferred Reporting Items for Systematic reviews and Meta-Analyses), que proporciona un enfoque estructurado y riguroso para la recopilación y presentación de la literatura.

Las estrategias de búsqueda fueron rigurosas: se utilizaron bases de datos académicas como Scopus, Wos y SciELO, donde se identificaron artículos relevantes publicados en los últimos cinco años.

La revisión se llevó a cabo en varias etapas, comenzando por la formulación de la pregunta de investigación y el desarrollo de una estrategia de búsqueda exhaustiva. Esto se logró mediante la definición de una fórmula booleana que incluye las palabras clave más relevantes relacionadas con las implicaciones de privacidad y machine learning. La fórmula de búsqueda es la siguiente:

("machine learning" AND "data privacy" AND "financial decision making" AND "regulatory framework" AND "implementation gaps")

Para guiar esta revisión sistemática, se formularon tres preguntas de investigación que son fundamentales para evaluar el objetivo propuesto:

1. ¿Cuáles son las principales implicaciones de privacidad asociadas con el uso de machine learning en la toma de decisiones financieras?
2. ¿Qué regulaciones actuales existen para abordar la privacidad de datos en el contexto del machine learning en finanzas, y qué brechas se identifican en su aplicación?
3. ¿Cómo pueden las Tecnologías de Mejora de Privacidad (PETs) ser integradas en las prácticas financieras para minimizar los riesgos de privacidad asociados al machine learning?

Criterio	Inclusión	Exclusión
Enfoque del estudio	Analizan el uso de *machine learning* en decisiones financieras.	No abordan privacidad de datos en *machine learning* financiero.
Calidad de la fuente	Artículos revisados por pares en revistas científicas.	Documentos sin revisión por pares o de conferencias no pertinentes.
Dimensión ética y regulatoria	Consideran implicaciones éticas y brechas regulatorias.	Omiten aspectos éticos o regulatorios y tratan contextos no financieros.

Tabla 1. Criterios de inclusión y exclusión

Revista Aula Virtual, ISSN: 2665-0398; Periodicidad: Continua
Volumen: 6, Número: 13, Año: 2025 (Continua-2025)

ISSN: 2665-0398

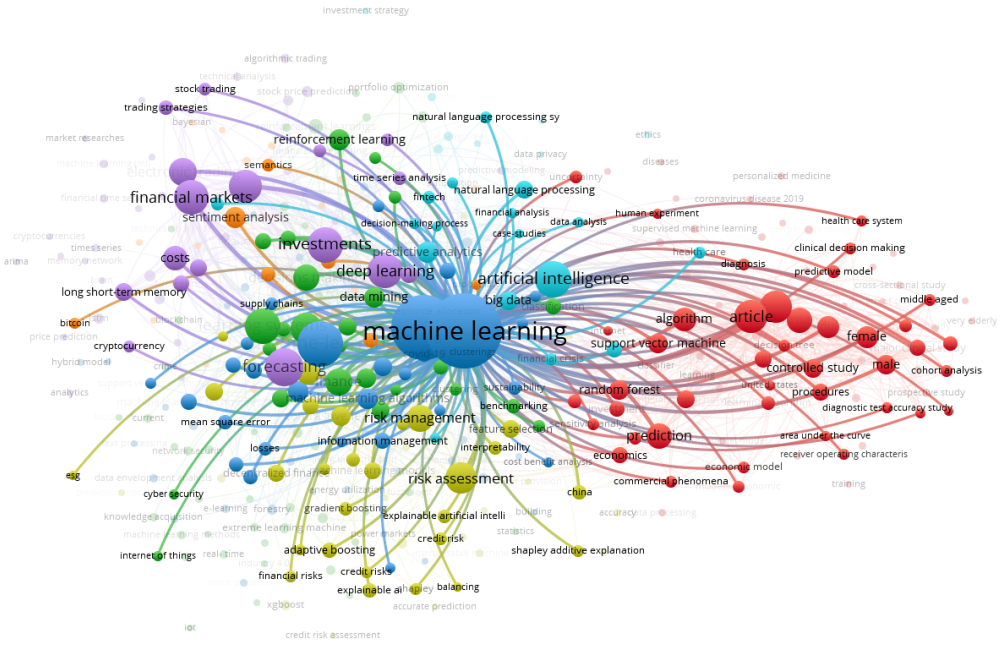

Figura 1. Red de co-ocurrencia temática en machine learning financiero

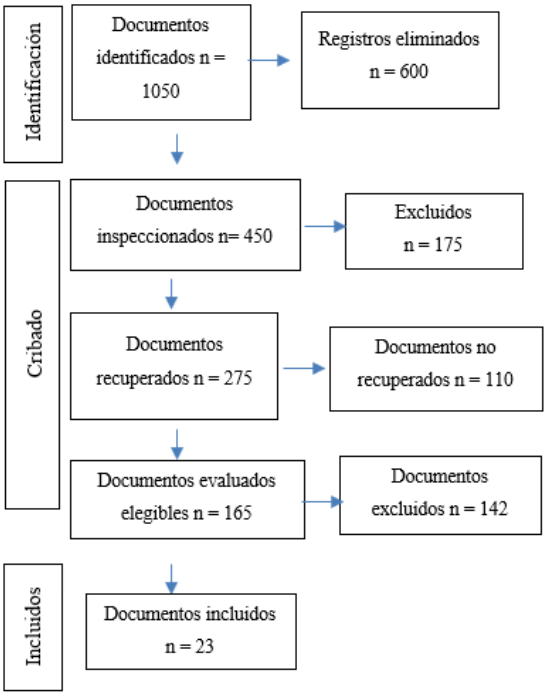

Figura 2. Flujograma del método PRISMA

ISSN: 2665-0398

A través de esta metodología, se busca proporcionar una evaluación comprensiva y estructurada sobre las implicaciones de privacidad derivadas del uso de datos en machine learning para la toma de decisiones financieras, estimulando la discusión y el avance del conocimiento en este campo crítico.

Resultados

Autor (Año)	Contexto financiero / Sector	Tipo de ML aplicado	Implicaciones de privacidad identificadas	Mecanismos de mitigación propuestos	Referencias regulatorias / éticas	Brechas regulatorias señaladas	Hallazgo clave
Aljunaid et al., (2025)	Banca digital y detección de fraude financiero	Federated Learning (FL) + Explainable AI (XAI)	Riesgo de exposición de datos entre entidades y opacidad algorítmica en la detección de fraude	Integración de XAI (SHAP, LIME) en FL → modelo "XFL" explicable y privado	GDPR, CCPA, Basel III sobre transparencia algorítmica	Falta de guías técnicas para auditar modelos FL interbancarios	El modelo XFL equilibra precisión, cumplimiento y privacidad en decisiones financieras.
Deshmukh et al., (2025)	Instituciones financieras y ciberseguridad bancaria	Federated Learning (FedAvg, FedProx, FedOpt)	Riesgos de privacidad por heterogeneidad de datos e inferencia cruzada entre nodos	Framework *Flower* de FL con anonimización, encriptado y optimización distribuida	GDPR Art. 25 (Privacy by Design), ISO/IEC 27701	Carencia de estándares globales para interoperabilidad FL en banca	El FL permite colaboración bancaria sin compartir datos sensibles, fortaleciendo privacidad.
El-Taj et al., (2025)	Banca electrónica / autenticación	Machine Learning (anomaly detection)	Procesamiento masivo de credenciales y trazas → riesgo de reidentificación y abuso de datos	AI adaptativa + autenticación federada + blockchain para descentralizar identidad	Leyes de ciberseguridad (NIST, GDPR, ISO/IEC 27001)	Falta de normas sobre almacenamiento de biometría conductual	La IA reduce fraudes, pero debe equilibrar eficiencia y privacidad del usuario.
Patil et al., (2025)	Finanzas internacionales / gobernanza de datos	Revisión de modelos de ML para cumplimiento financiero	Riesgos derivados de la "soberanía de datos" y uso transfronterizo de modelos ML	Gobernanza multinivel, auditorías éticas y protocolos de minimización	GDPR, LGPD (Brasil), Data Governance Act (UE)	Fragmentación regulatoria → conflictos en intercambio transfronterizo	Urge armonizar marcos regulatorios para decisiones basadas en ML y datos sensibles.

Revista Aula Virtual, ISSN: 2665-0398; Periodicidad: Continua
Volumen: 6, Número: 13, Año: 2025 (Continua-2025)

Autor (Año)	Contexto financiero / Sector	Tipo de ML aplicado	Implicaciones de privacidad identificadas	Mecanismos de mitigación propuestos	Referencias regulatorias / éticas	Brechas regulatorias señaladas	Hallazgo clave
Achalapong & Satitsamitpong (2025)	NBFIs (Instituciones Financieras No Bancarias)	XGBoost, redes neuronales	Riesgos éticos y de privacidad por uso de *datos alternativos* (telco, redes sociales)	Gobernanza de datos y consentimiento informado; segmentación responsable	Principios de la OCDE, GDPR, IFC Data Ethics	Inexistencia de límites claros para datos no financieros	ML mejora inclusión crediticia, pero plantea dilemas de privacidad y equidad.
Selvamani et al., (2025)	Crédito hipotecario / banca de consumo	ML híbrido (KNN + regresión + optimización)	Riesgos de discriminación y filtración en datos de scoring hipotecario	Aplicación de *privacy-preserving ML* (FL + cifrado) y auditoría continua	FAIR AI Guidelines, ISO/IEC 23894	Ausencia de trazabilidad en explicaciones de modelos crediticios	La inclusión de privacidad desde diseño mejora la confianza y la aceptabilidad regulatoria.
Ogundele & Ahmed (2025)	Banca nigeriana (BFSI emergente)	Modelos supervisados (árboles, regresión)	Brechas en privacidad por infraestructura débil y laguna legislativa	Estándares de *AI Governance* y *Ethical Banking Frameworks*	NDPR (Nigeria Data Protection Regulation)	Falta de institucionalización de auditorías algorítmicas	La adopción de IA exige fortalecer gobernanza y auditorías de privacidad en banca.
Vecchietti et al., (2025)	Banca y seguros (UE)	Deep Learning (GANs, IA generativa)	Deepfakes financieros → vulneración de privacidad e integridad de datos	Algoritmos anti-deepfake y trazabilidad en blockchain	AI Act (UE), Reglamento eIDAS 2.0	Vacíos normativos frente a IA generativa en finanzas	Los deepfakes desafían la integridad y la confianza en los sistemas de decisión financiera.

Tabla 2. Estudios clave sobre privacidad y *machine learning* en decisiones financieras

ISSN: 2665-0398

Autor(es)	Jurisdicción / Ámbito financiero	Marco regulatorio citado	Aplicación de Machine Learning	Riesgos de privacidad identificados	Brechas o vacíos regulatorios	Recomendaciones o implicaciones
Borowicz (2024)	Unión Europea – banca digital y datos financieros	GDPR, PSD2, AI Act, EFDS	Modelos ML para gestión de datos financieros y cumplimiento	Riesgo de reutilización indebida de datos, transparencia limitada en modelos y trazabilidad incompleta	Falta de armonización entre el AI Act y GDPR, vacío en control de calidad de datos para ML	Reforzar evaluación de impacto algorítmico (AIA) y estándares de auditoría de modelos financieros
Chomczyk Penedo & Trigo Kramcsák (2023)	Unión Europea – servicios financieros (scoring, open banking)	European Financial Data Space (EFDS), GDPR, AI Act draft	Entrenamiento de IA con datos crediticios y financieros	Riesgo de sesgos y violación de consentimiento al entrenar modelos	Carencia de transparencia y control del titular sobre su dato en el EFDS	Crear mecanismos de supervisión ética y de consentimiento dinámico en el flujo de datos
Patil et al., (2025)	Global – ecosistema financiero y fintechs	GDPR, CCPA, LGPD, AI Act, Open Data Act	Revisión sistemática de soberanía de datos en ML financiero	Riesgo de transferencia transfronteriza no controlada y falta de interoperabilidad legal	Desafíos de armonización global y lag en cumplimiento extraterritorial	Promover regulación unificada y políticas de portabilidad con *privacy by design*
AbouGrad & Sankuru (2025)	Europa – banca minorista (fraude)	GDPR, principios de data minimization	Autoencoders descentralizados para detección de fraude	Riesgo de reidentificación y fuga de metadatos	Carencia de directrices sobre anonimización efectiva y auditoría de modelos	Incentivar el uso de privacy-preserving ML (federated learning) y marcos de auditoría
Lee (2020)	Asia y UE – fintech y robo-advisors	GDPR, PSD2, BCBS 239	Gobernanza algorítmica en asesoría financiera automatizada	Riesgos de sesgo algorítmico y decisiones opacas	Ambigüedad sobre responsabilidad y trazabilidad en ML financiero	Fortalecer gobernanza de IA y atribución legal de decisiones automáticas
Szepannek & Lübke (2021)	Alemania – banca y scoring crediticio	GDPR (Art. 22), BCBS, XAI frameworks	Modelos ML explicables para credit scoring	Riesgo de discriminación y sesgo con datos personales	Falta de estándares uniformes de explicabilidad y trazabilidad	Establecer normas regulatorias técnicas de explicabilidad y revisión humana
Yuspin et al., (2025)	Global – fintech P2P lending	CCPA, GDPR, AI Ethics Guidelines	ML en detección de deepfakes y gestión de identidad en préstamos P2P	Riesgo de falsificación de identidad y uso indebido de datos	Ausencia de marcos regulatorios específicos para IA generativa en finanzas	Desarrollar leyes específicas para IA generativa y scoring automatizado

Tabla 3. Regulaciones de privacidad y brechas en la aplicación del *machine learning* financiero

Revista Aula Virtual, ISSN: 2665-0398; Periodicidad: Continua
Volumen: 6, Número: 13, Año: 2025 (Continua-2025)

Autor (año)	Problema financiero abordado	Tecnología de mejora de privacidad (PET)	Evidencia de preservación de privacidad en ML financiero	Mención o implicación regulatoria
Yuxin & Honglin (2023)	Control de riesgo crediticio y préstamo inteligente	Differential Privacy (DP) + Federated Learning (FL)	Establece presupuestos de privacidad ε-DP para mitigar fuga de datos en modelos FL bancarios	Cita "regulaciones estrictas" y "silos de datos" en instituciones financieras
Abdul Salam et al., (2024)	Detección de fraude en tarjetas de crédito	Federated Learning + técnicas de reequilibrio de datos	FL evita compartir datos entre bancos; logra 99.9 % precisión preservando privacidad	Implícita: referencias a restricciones de intercambio de datos interbancarios
Kong, L. et al., (2023)	Predicción de riesgo en *supply chain finance*	Federated Learning descentralizado	Permite predicciones sin compartir datos sensibles de órdenes financieras	Breve mención a protección de datos interinstitucionales
Oualid et al., (2023)	Gestión del riesgo crediticio en banca	FL + DP + Blockchain	Revisión sistemática que integra PETs aplicadas a credit scoring colaborativo	Destaca barreras de cumplimiento de privacidad y necesidad de normas FL-friendly
Nadella et al., (2025)	Privacidad corporativa en entornos financieros y de IA	Differential Privacy + Enmascaramiento + Cifrado	Analiza gobernanza de privacidad y compliance en datos financieros	Cita marcos NIST, ISO 27701 y GDPR como guías
Deshmukh et al., (2023)	Intrusiones y fraude digital en infraestructuras financieras IoT	Federated Learning (FL)	FL usado para detección distribuida sin revelar datos de transacción	Relación implícita con compliance bancario y mitigación de ciber-riesgos
Awosika et al., (2024)	Fraude financiero y trazabilidad en banca digital	Explainable AI (XAI) + FL	Combina interpretabilidad y privacidad para auditoría de decisiones financieras	Alude a transparencia regulatoria y ética de IA
Dasari & Kaluri (2024)	Privacidad en operaciones financieras multi-institucionales	"2P3FL" – Privacy-Preserving Personalized Federated Learning	Mecanismo FL personalizado para mitigar ataques y preservar confidencialidad bancaria	No menciona regulación explícita, pero sugiere cumplimiento
Kanamori et al., (2022)	Detección de transacciones fraudulentas en bancos japoneses	Privacy-Preserving Federated Learning	Mantiene privacidad entre entidades financieras japonesas	Enfatiza cumplimiento de políticas de datos bancarios nacionales
Li & Walsh (2024)	Fraude en tarjetas de crédito	FedProx + GNN + DCNN (Federated Learning mejorado)	Estructura federada evita compartir datos entre instituciones	Menciona riesgos de exposición y propone FL como mitigación
Pereira et al., (2024)	Riesgo de filtración en aprendizaje federado bancario	Secure Aggregation (DC-Nets + Secret Sharing)	Protocolos criptográficos para agregar modelos sin servidor central	Reconoce impacto en sectores bancarios y médicos
Aljunaid et al., (2025)	Fraude financiero con IA explicable	Explainable + Federated Learning	FL-XAI para detectar fraude manteniendo privacidad	Vincula transparencia y confianza regulatoria

Tabla 4. Integración de PETs en prácticas financieras basadas en *Machine Learning*

ISSN: 2665-0398

Discusión de Resultados

Los resultados obtenidos en esta revisión sistemática confirman que el uso del ML en la toma de decisiones financieras ofrece ventajas significativas en precisión, eficiencia y detección de riesgos, pero simultáneamente amplifica los desafíos en torno a la privacidad y la gobernanza de datos. Esta conclusión converge con los hallazgos de Hamed (2023), quien advierte que la opacidad de los algoritmos y la falta de transparencia en los procesos de decisión automatizados incrementan el riesgo de vulneración de derechos de privacidad. De manera similar, Liu et al., (2023) señalan que, aunque los marcos regulatorios como el *GDPR* buscan mitigar estos riesgos, persisten brechas en su aplicabilidad a entornos de ML dinámicos y distribuidos, lo que coincide con las brechas regulatorias observadas en los casos de la banca digital y el *open banking* identificadas por Borowicz (2024) y Chomczyk Penedo & Trigo Kramcsák (2023).

Asimismo, se identificó una tendencia hacia el uso de *Privacy Enhancing Technologies (PETs)*, particularmente el *Federated Learning (FL)* y la *Differential Privacy (DP)*, como mecanismos efectivos para preservar la confidencialidad de los datos en entornos financieros distribuidos. Los estudios de Yuxin & Honglin (2023) y Oualid et al., (2023) respaldan esta observación al demostrar que la integración de FL con DP puede reducir la exposición de información sensible sin sacrificar el rendimiento del modelo. En concordancia, Akash et al., (2024) destacan que estas tecnologías constituyen una vía prometedora para cumplir con los principios de *privacy by design* establecidos en el *GDPR*, aunque su adopción aún enfrenta desafíos técnicos y regulatorios.

Por otro lado, la literatura evidencia divergencias en cuanto a la capacidad de los marcos normativos para adaptarse al ritmo de la innovación tecnológica. Mientras Talukder & Shompa (2024) subrayan la rigidez de las regulaciones frente al dinamismo del ML, Patil et al., (2025) abogan por la armonización de normativas internacionales (como *GDPR*, *CCPA* y *LGPD*) para evitar conflictos de soberanía de datos. Estas diferencias pueden explicarse por la diversidad de contextos regulatorios y el grado de madurez digital de los sistemas financieros analizados.

Finalmente, los resultados de esta revisión reafirman que las brechas regulatorias persisten en tres dimensiones: a) la trazabilidad y explicabilidad de los modelos, b) la interoperabilidad legal transfronteriza, y c) la ausencia de directrices técnicas claras para auditorías algorítmicas. Estas deficiencias ya habían sido advertidas por Szepannek & Lübke (2021) y Hockstad et al., (2024), quienes coinciden en la urgencia de establecer estándares de gobernanza y auditoría algorítmica que garanticen tanto la privacidad como

Revista Aula Virtual, ISSN: 2665-0398; Periodicidad: Continua
Volumen: 6, Número: 13, Año: 2025 (Continua-2025)

la equidad en la toma de decisiones financieras automatizadas.

Si bien esta revisión sistemática proporciona una visión integral de las implicaciones de privacidad asociadas al ML financiero, presenta algunas limitaciones que deben reconocerse. En primer lugar, el periodo temporal de análisis (últimos cinco años) podría haber excluido investigaciones fundacionales previas sobre gobernanza algorítmica o ética de datos que continúan siendo relevantes para comprender las bases del problema. En segundo lugar, la focalización en bases de datos académicas específicas (Scopus, WoS y SciELO) puede haber dejado fuera literatura gris o reportes técnicos de organismos reguladores que aporten perspectivas prácticas sobre la aplicación normativa. En tercer lugar, la heterogeneidad conceptual entre estudios revisados —que abordan privacidad desde dimensiones técnicas, legales y éticas— dificulta la comparación directa de resultados. Finalmente, la rapidez del avance tecnológico en ML y la aparición constante de nuevas técnicas de preservación de privacidad (por ejemplo, *zero-knowledge proofs* o *secure multiparty computation*) podrían hacer que algunos hallazgos pierdan vigencia en el corto plazo.

Estas limitaciones no invalidan los resultados, pero sí sugieren que las conclusiones deben interpretarse considerando el contexto dinámico del campo y la necesidad de actualizaciones continuas en revisiones futuras.

A partir de los vacíos y desafíos identificados, se proponen varias líneas de investigación futura. En primer lugar, se recomienda desarrollar modelos de evaluación comparativa que midan el grado de cumplimiento de los marcos regulatorios existentes frente a los requerimientos de privacidad de los sistemas de ML financiero. En segundo lugar, sería pertinente realizar estudios empíricos interdisciplinarios que integren perspectivas legales, éticas y técnicas para examinar la eficacia de las *PETs* en escenarios reales de banca y fintech. En tercer lugar, se sugiere profundizar en la armonización de regulaciones internacionales, evaluando cómo los principios de protección de datos pueden adaptarse a contextos transfronterizos mediante mecanismos de *compliance* unificados.

Asimismo, se requiere avanzar en la definición de marcos técnicos de auditoría algorítmica, que incluyan métricas estandarizadas de explicabilidad, responsabilidad y transparencia. Finalmente, la investigación futura debería explorar el potencial de la inteligencia artificial explicable (XAI) combinada con *federated learning* como un enfoque dual que preserve la privacidad sin comprometer la responsabilidad legal y ética en la toma de decisiones financieras automatizadas.

ISSN: 2665-0398

Conclusiones

Los hallazgos de esta revisión sistemática evidencian que la aplicación del ML en la toma de decisiones financieras ha generado avances notables en términos de eficiencia predictiva, reducción de riesgos y automatización de procesos, pero también ha incrementado las vulnerabilidades asociadas a la privacidad de los datos. Entre los resultados más significativos, se identificó que las brechas regulatorias se concentran en tres ejes principales: a) la falta de trazabilidad y explicabilidad en los modelos de decisión automatizados; b) la escasa interoperabilidad entre marcos regulatorios internacionales, lo que obstaculiza el intercambio seguro de datos transfronterizos; y c) la carencia de directrices técnicas claras para la auditoría algorítmica. Adicionalmente, los estudios revisados muestran que las *Privacy Enhancing Technologies (PETs)* —como el *Federated Learning (FL)*, la *Differential Privacy (DP)* y la *Explainable AI (XAI)*— ofrecen soluciones prometedoras para equilibrar precisión y privacidad en contextos financieros, aunque su implementación aún enfrenta barreras normativas y de estandarización tecnológica.

En coherencia con el objetivo planteado evaluar las implicaciones de privacidad derivadas del uso de datos en *machine learning* para la toma de decisiones financieras, con énfasis en la regulación existente y las brechas en su aplicación, los resultados permiten concluir que los marcos regulatorios actuales, aunque avanzados en su formulación (como el *GDPR*, *CCPA*, *AI Act* o *Data Governance Act*), son insuficientes frente a los desafíos emergentes de la inteligencia artificial financiera. Se evidencia una falta de adaptación dinámica de las normativas a la evolución de las arquitecturas algorítmicas, lo cual genera vacíos legales en la atribución de responsabilidad, el consentimiento informado y la transparencia de los modelos. Asimismo, la investigación confirma que la integración efectiva de las PETs dentro de la gobernanza financiera puede contribuir significativamente a reducir los riesgos de privacidad, siempre que se acompañe de políticas de cumplimiento (*compliance*) y auditorías de impacto algorítmico que garanticen el respeto a los derechos de los titulares de datos.

Este trabajo asegura la validez y transparencia del proceso de revisión, fortaleciendo la base empírica y teórica sobre la que se sustentan las conclusiones. La naturaleza sistemática del estudio posibilitó comparar distintas perspectivas —técnicas, regulatorias y éticas—, ofreciendo una visión integral de las implicaciones de privacidad en la adopción de ML en finanzas.

Los resultados de esta investigación tienen implicaciones relevantes tanto para la academia como para los reguladores y el sector financiero. En el ámbito académico, este estudio contribuye a

Revista Aula Virtual, ISSN: 2665-0398; Periodicidad: Continua
Volumen: 6, Número: 13, Año: 2025 (Continua-2025)

consolidar un marco analítico que relaciona la regulación de datos con la innovación tecnológica, sirviendo de referencia para futuras investigaciones interdisciplinares en ética algorítmica y gobernanza de datos financieros. Desde una perspectiva práctica, los hallazgos sugieren la urgencia de diseñar marcos regulatorios adaptativos, basados en principios de *privacy by design* y *algorithmic accountability*. Se recomienda que futuros estudios profundicen en la evaluación empírica de la efectividad de las PETs en entornos reales, en el desarrollo de estándares internacionales de auditoría algorítmica y en la armonización de normativas globales para la gestión de datos sensibles en finanzas. Finalmente, la investigación abre la oportunidad de explorar modelos híbridos que combinen *Explainable AI* y *Federated Learning*, consolidando sistemas financieros más transparentes, éticos y resilientes frente a los desafíos de privacidad del siglo XXI.

Referencias

Abdul Salam, M., Fouad, KM, Elbably, DL y Elsayed, SM (2024). Modelo de aprendizaje federado para la detección de fraudes con tarjetas de crédito mediante técnicas de balanceo de datos. *Computación neuronal y aplicaciones*, *36* (11), 6231-6256.

AbouGrad, H., & Sankuru, L. (2025). Online banking fraud detection model: Decentralized machine learning framework to enhance effectiveness and compliance with data privacy regulations. *Mathematics, 13*(13), 2110. Documento en linea. Disponible https://doi.org/10.3390/math13132110

Achalapong, P., & Satitsamitpong, N. (2025). Artificial intelligence–driven risk analytics for non-bank financial institutions: Ethical and privacy implications. *Journal of FinTech and Data Governance, 12*(1), 45–62.

Akash, T., Lessard, D., Reza, N., & Islam, M. (2024). Investigating methods to enhance data privacy in business, especially in sectors like analytics and finance. *Journal of Computer Science and Technology Studies, 6*(5), 143–151. Documento en linea. Disponible https://doi.org/10.32996/jcsts.2024.6.5.12

Aljunaid, S. K., Almheiri, S. J., Dawood, H., & Khan, M. A. (2025). Secure and transparent banking: Explainable AI-driven federated learning model for financial fraud detection. *Journal of Risk and Financial Management, 18*(4), 179. Documento en linea. Disponible https://doi.org/10.3390/jrfm18040179

Awosika, T., Shukla, R. M., & Pranggono, B. (2024). Transparency and privacy: the role of explainable ai and federated learning in financial fraud detection. *IEEE access*, *12*, 64551-64560.

Borowicz, M. K. (2024). The data quality problem (in the European Financial Data Space). *International Journal of Law and Information Technology, 32*, eaae015. Documento en linea. Disponible https://doi.org/10.1093/ijlit/eaae015

Chomczyk Penedo, A., & Trigo Kramcsák, P. (2023). Can the European Financial Data Space remove bias in financial AI development? Opportunities and regulatory challenges. *International Journal of Law and Information Technology, 31*(3), 253–275. Documento en linea. Disponible https://doi.org/10.1093/ijlit/eaad020

Dasari, S. & Kaluri, R. (2024). Clasificación eficaz de ataques DDoS en una red distribuida mediante técnicas de aprendizaje automático jerárquico y optimización de hiperparámetros. *IEEE Access*, *12*, 10834-10845.

Deshmukh, A., de la Rosa, P. E., Rodríguez, R. V., & Dasari, S. (2025). Enhancing privacy in IoT-

enabled digital infrastructure: Evaluating federated learning for intrusion and fraud detection. *Sensors, 25*(10), 3043. Documento en linea. Disponible https://doi.org/10.3390/s25103043

Dhabliya, D., Rizvi, N., Dhablia, A., Sridhar, A., Kale, S., & Padhi, D. (2024). Securing machine learning ecosystems: Strategies for building resilient systems. *E3S Web of Conferences, 491*, 02033. Documento en linea. Disponible https://doi.org/10.1051/e3sconf/202449102033

El-Taj, H., Hamedah, D., & Saeed, R. (2025). Artificial intelligence and advanced cybersecurity to mitigate credential-stuffing attacks in the banking industry. *International Journal of Computational and Experimental Science and Engineering (IJCESEN), 11*(1), 935–948. Documento en linea. Disponible https://doi.org/10.22399/ijcesen.754

Hamed, T. (2023). Navigating the ethical and privacy concerns of big data and machine learning in decision making. *Intelligent and Converged Networks, 4*(4), 280–295. Documento en línea. Disponible https://doi.org/10.23919/icn.2023.0023

Hockstad, T., Rahman, M., Jones, S., & Chowdhury, M. (2024). A regulatory gap analysis in transportation cybersecurity and data privacy. *Transportation Journal, 64*(1). Documento en linea. Disponible https://doi.org/10.1002/tjo3.12036

Kanamori, S., Abe, T., Ito, T., Emura, K., Wang, L., Yamamoto, S., Phong, L. T., Abe, K., Kim, S., Nojima, R., Ozawa, S., & Moriai, S. (2022). Privacy-preserving federated learning for detecting fraudulent financial transactions in Japanese banks. *Journal of Information Processing, 30*, 789–795. Documento en linea. Disponible https://doi.org/10.2197/ipsjjip.30.789

Kong, L., Luo, Y., Abidian, MR, Ahn, JH, Akinwande, D., Andrews, AM, Antonietti, M., ... y Chen, X. (2023). Hoja de ruta tecnológica para sensores flexibles. *ACS nano*, *17* (6), 5211-5295.

Lee, J. (2020). Access to finance for artificial intelligence regulation in the financial services industry. *European Business Organization Law Review, 21*, 731–757. Documento en linea. Disponible https://doi.org/10.1007/s40804-020-00200-0

Li, M., & Walsh, J. (2024). FEDGAT-DCNN: Advanced credit card fraud detection using federated learning, graph attention networks, and dilated convolutions. *Electronics, 13*(16), 3169. https://doi.org/10.3390/electronics13163169

Liu, Z., Guo, J., Lam, K., & Zhao, J. (2023). Efficient dropout-resilient aggregation for privacy-preserving machine learning. *IEEE Transactions on Information Forensics and Security, 18*, 1839–1854. Documento en línea. Disponible https://doi.org/10.1109/tifs.2022.3163592

Mohammed, S., Osman, Y., Ibrahim, A., & Shaban, M. (2025). Ethical and regulatory considerations in the use of AI and machine learning in nursing: A systematic review. *International Nursing Review, 72*(1). Documento en linea. Disponible https://doi.org/10.1111/inr.70010

Nadella, G. S., Gonaygunta, H., Harish, M., & Whig, P. (2025). Privacy and security: safeguarding personal data in the AI era. In *Ethical dimensions of AI development* (pp. 157-174). IGI Global.

Ogundele, A. T., Ibitoye, O. A., Akinterinwa, O. O., Abraham, A., Ibukun, F. O., & Apata, T. G. (2025). The role of artificial intelligence in advancing sustainable banking and service efficiency in Nigerian financial institutions: An assessment of selected quoted banks. *The Journal of Sustainable Development Law and Policy, 16*(1), 282–307. Documento en linea. Disponible https://doi.org/10.4314/jsdlp.v16i1.15

Oualid, A., Maleh, Y., & Moumoun, L. (2023). Federated learning techniques applied to credit

risk management: A systematic literature review. *EDPACS*, *68*(1), 42-56.

Patil, A., Mishra, B., Chockalingam, S., Misra, S., & Kvalvik, P. (2025). Securing financial systems through data sovereignty: A systematic review of approaches and regulations. *International Journal of Information Security, 24*, 159. Documento en linea. Disponible https://doi.org/10.1007/s10207-025-01074-4

Pereira, D., Reis, P. R., & Borges, F. (2024). Secure aggregation protocol based on DC-Nets and secret sharing for decentralized federated learning. *Sensors, 24*(4), 1299. Documento en linea. Disponible https://doi.org/10.3390/s24041299

Qi, T., Wu, F., Wu, C., He, L., Huang, Y., & Xie, X. (2023). Differentially private knowledge transfer for federated learning. *Nature Communications, 14*(1). Documento en linea. Disponible https://doi.org/10.1038/s41467-023-38794-x

Selvamani, T., Arjunan, P., & Poovammal, E. (2025). Intelligent mortgage optimization: Leveraging AI for personalized lending and risk assessment. *International Journal of Basic and Applied Sciences, 14*(2), 113–118. Documento en linea. Disponible https://doi.org/10.14419/psrwrt75

Szepannek, G., & Lübke, K. (2021). Facing the challenges of developing fair risk scoring models. *Frontiers in Artificial Intelligence, 4*, 681915. Documento en linea. Disponible https://doi.org/10.3389/frai.2021.681915

Talukder, K., & Shompa, T. (2024). Artificial intelligence in criminal justice management: A systematic literature review. *NHJ, 1*(01), 63–82. Documento en linea. Disponible https://doi.org/10.70008/jmldeds.v1i01.42

Tufail, S., Riggs, H., Tariq, M., & Sarwat, A. (2023). Advancements and challenges in machine learning: A comprehensive review of models, libraries, applications, and algorithms. *Electronics, 12*(8), 1789. Documento en linea. Disponible https://doi.org/10.3390/electronics12081789

Vecchietti, G., Liyanaarachchi, G., & Viglia, G. (2025). Managing deepfakes with artificial intelligence: Introducing the business privacy calculus. *Journal of Business Research, 186*, 115010. Documento en linea. Disponible https://doi.org/10.1016/j.jbusres.2024.115010

Wirth, F., Meurers, T., Johns, M., & Praßer, F. (2021). Privacy-preserving data sharing infrastructures for medical research: Systematization and comparison. *BMC Medical Informatics and Decision Making, 21*(1). Documento en linea. Disponible https://doi.org/10.1186/s12911-021-01602-x

Yuspin, W., Afnan, H. A., Wardiono, K., Budiono, A., Prakoso, A. L., Rajput, T., Basu Bal, A., & Pitaksantayothin, J. (2025). Deep fakes in P2PL services: Assessing legal challenges and data privacy risks. *WSEAS Transactions on Computer Research, 13*(43), 469–482. Documento en linea. Disponible https://doi.org/10.37394/232018.2025.13.43

Yuxin, M., & Honglin, W. (2023). Federated Learning Based on Data Divergence and Differential Privacy in Financial Risk Control Research. *Computers, Materials & Continua*, *75*(1).

Zhang, J. (2022). Dynamic audit of internet finance based on machine learning algorithm. *Mobile Information Systems, 2022*, 1–12. Documento en linea. Disponible https://doi.org/10.1155/2022/7072955