

Data Brokers: Dinámicas, riesgos y desafíos para la seguridad digital

Data Brokers: Dynamics, Risks and Challenges for Digital Security

 **Guliana María Fernanda Lulichac Ramos:** Universidad Nacional de Trujillo, Ingeniera en Sistemas, <https://orcid.org/0009-0006-5503-7451>

 **Aldo Jean Marcos Sánchez Chiclayo:** Universidad Nacional de Trujillo, Ingeniero en Sistemas, <https://orcid.org/0009-0000-4429-714X>

Alberto Carlos Mendoza de los Santos: Universidad Nacional de Trujillo, Doctor en Ingeniería de Sistemas e Informática,

 <https://orcid.org/0000-0002-0469-915X>

Autor de correspondencia: t033300220@unitru.edu.pe



DOI: <https://doi.org/10.64424/rcu51202699>

Recibido: 24 de octubre 2025

Aprobado: 18 de diciembre 2026

Publicado: 19 de junio 2026

Resumen:

Los datos personales se han establecido como un elemento clave en la economía digital, con los corredores de datos desempeñando un papel fundamental en la recopilación, análisis y venta de información. Este artículo de revisión examina cómo las dinámicas económicas, tecnológicas, sociales y éticas de estos intermediarios afectan los riesgos de ciberseguridad y protección de datos, enfatizando los desafíos regulatorios en el entorno digital. Se realizó una revisión sistemática siguiendo la declaración PRISMA 2020; de 2078 registros iniciales identificados en Scopus, ScienceDirect y Springer Nature (2022-2025), se seleccionaron 12 estudios tras eliminar duplicados y aplicar criterios de inclusión y exclusión rigurosos. Los estudios fueron evaluados independientemente por dos revisores ($Kappa=0.85$) y analizados cualitativamente mediante síntesis temática en cuatro dimensiones: económica, tecnológica, social-ética y regulatoria. Complementariamente, se realizó análisis bibliométrico con VOSviewer y Bibliometrix de R sobre 1051 documentos de Scopus y ScienceDirect. Los hallazgos revelan que los data brokers operan en mercados con deficiencias estructurales que propician discriminación de precios y barreras de entrada. Tecnológicamente, el modelo centralizado acumula riesgos de seguridad, mientras las alternativas descentralizadas presentan oportunidades, pero desafíos de gobernanza. En lo social-ético, se identificó comercialización de información sensible en salud y educación, además de prácticas de consentimiento engañoso. Regulatoriamente, la dispersión normativa y ausencia de definiciones claras dificultan la supervisión efectiva, evidenciando la necesidad urgente de marcos regulatorios armonizados que equilibren innovación y protección de derechos fundamentales.

Palabras clave: Ciberseguridad; economía de la información; privacidad digital; regulación tecnológica.

Abstract:

Personal data has become a key element in the digital economy, with data brokers playing a fundamental role in collecting, analysing and selling information. This review article examined how the economic, technological, social and ethical dynamics of these intermediaries affect cybersecurity and data protection risks, emphasising regulatory challenges in the digital environment. A systematic review following PRISMA 2020 was conducted. From 2,078 initial records identified in Scopus, ScienceDirect and Springer Nature (2022–2025), 12 studies were selected after removing duplicates and applying rigorous inclusion and exclusion criteria. Studies were independently evaluated by two reviewers ($Kappa=0.85$) and qualitatively analysed through thematic synthesis across four dimensions: economic, technological, social-ethical and regulatory. Complementarily, bibliometric analysis was performed using VOSviewer and Bibliometrix in R on 1,051 documents from Scopus and ScienceDirect. Findings reveal that data brokers operate in markets with structural deficiencies fostering price discrimination and entry barriers. Technologically, the centralised model accumulates security risks, while decentralised alternatives offer opportunities but governance challenges. Social-ethically, commercialisation of sensitive health and education information was identified, alongside deceptive consent practices. Regulatorily, normative dispersion and absence of clear definitions hinder effective oversight, evidencing urgent need for harmonised regulatory frameworks balancing innovation and fundamental rights protection.

Keywords: Cybersecurity; data surveillance; digital privacy; information economy; technological regulation.

UNANCHAY Revista de Ciencias de la Ingeniería Volumen 5. Número 1. Año 2026, p. 122-138

ISSN 2953-6707 enero - junio 2026

<https://publicacionestecnocuatoriano.edu.ec/index.php/RCU/index>

Como citar la obra: Lulichac-Ramos, G., M., F., Sánchez-Chiclayo, A., J., M. y Mendoza-de los Santos, A., C. (2026). Data Brokers: Riesgos y desafíos para la seguridad digital. *Revista Científica Unanchay*, 5(1), 122-138
doi: <https://doi.org/10.64424/rcu51202699>



Introducción

En la actualidad, la información personal se ha convertido en uno de los recursos más valiosos del ámbito digital. Cada interacción en redes sociales, aplicaciones móviles, compras en línea o simples búsquedas en internet deja un rastro que puede ser recolectado, analizado y comercializado. Los principales actores en este proceso son los data brokers o corredores de datos: organizaciones que captan grandes volúmenes de información de variadas fuentes para luego venderla o intercambiarla con terceros, generando un mercado millonario basado en la explotación de datos personales (Abrardi, Cambini & Pino, 2025). Su actividad no se limita únicamente a la publicidad digital, sino que se vincula estrechamente con el fenómeno del capitalismo de vigilancia, donde los datos se utilizan para predecir y modelar comportamientos futuros. Empresas como Oracle afirman tener información de más de dos mil millones de personas y decenas de miles de atributos por individuo, lo que refleja la dimensión de esta industria y la amenaza que representa para la privacidad y la seguridad digital (Reviglio, 2022).

Los data brokers emplean técnicas de rastreo que permiten construir perfiles detallados sobre consumo, ubicación y otros intereses. Este seguimiento ocurre de manera invisible para la mayoría de los usuarios, quienes desconocen la magnitud de la información recolectada y su potencial uso en publicidad dirigida, evaluación crediticia o procesos de selección laboral (González Guerrero, 2019). En Estados Unidos, se ha documentado cómo algunas empresas han economizado información sensible de ciudadanos, incluyendo registros financieros y de salud, lo que genera riesgos de discriminación y exposición indebida (Sherman, 2021). Más grave aún, investigaciones recientes han demostrado la oferta de datos relacionados con condiciones de salud mental, sin garantías de anonimización ni medidas regulatorias efectivas sobre sus compradores (Kim, 2023).

Este escenario se ve agravado por un marco normativo insuficiente. Mientras que en la Unión Europea se promueve un modelo de protección a través del Reglamento General de Protección de Datos, en Estados Unidos la ausencia de una legislación integral permite que la compraventa de información ocurra sin consentimiento informado ni supervisión adecuada (DiPersio, 2024). De esta forma, los data brokers no solo plantean desafíos en materia de privacidad individual, sino también en términos de seguridad digital y equilibrio social. Por ello, el objetivo de este artículo de revisión es explicar cómo las dinámicas económicas, tecnológicas, sociales y éticas en la intermediación de datos generan riesgos para la privacidad y la ciberseguridad; además, identificar a través de co-ocurrencias los mecanismos que vinculan esos riesgos con los vacíos regulatorios.

Metodología

Se utilizó la declaración PRISMA (Preferred Reporting Items for Systematic reviews and Meta-Analyses) para desarrollar esta revisión sistemática que abordó la siguiente pregunta de investigación: ¿De qué manera las dinámicas económicas, tecnológicas, y sociales y éticas de los data brokers influyen críticamente en los riesgos de ciberseguridad y protección de datos en el ecosistema digital?

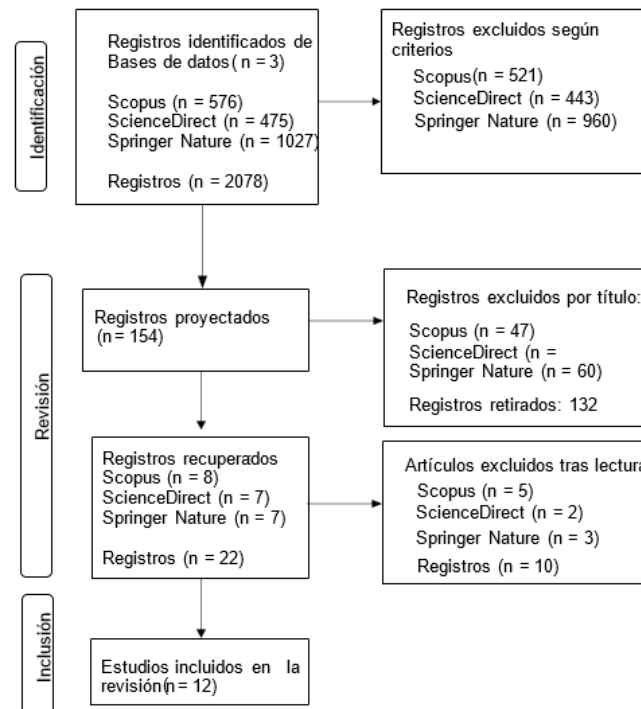
En consecuencia, se aplicaron los lineamientos de la metodología PRISMA 2020 (Page et al., 2021) para evaluar la idoneidad y fiabilidad de los estudios, garantizando así un proceso riguroso, transparente y reproducible. Asimismo, se consideraron los principios de síntesis investigativa de Gurevitch et al. (2018) para fortalecer la integración sistemática de la evidencia científica.

A continuación, se realizó una búsqueda avanzada en tres bases de datos científicas reconocidas: Scopus, ScienceDirect y Springer Nature, seleccionadas por su cobertura multidisciplinaria, indexación de revistas de alto impacto en ciberseguridad y políticas tecnológicas, y acceso a producción científica reciente. Se emplearon términos clave combinados con operadores booleanos, como se detalla en la Tabla 01. Todas las búsquedas se limitaron a publicaciones entre enero de 2022 y diciembre de 2025. Seguidamente, tras el filtrado por idioma y período, se ejecutó una selección manual evaluando la pertinencia temática y calidad técnica de los artículos que cumplieron los criterios establecidos previamente.

Para garantizar la calidad de los estudios incluidos, se aplicó una evaluación sistemática considerando claridad metodológica, relevancia temática, actualidad y revisión por pares, además de originalidad conceptual. Dos revisores evaluaron independientemente cada estudio, resolviendo discrepancias mediante consenso.

Los criterios de inclusión requirieron que los artículos fueran: (a) investigaciones originales o revisiones sistemáticas publicadas entre 2022 y 2025; (b) revisados por pares en revistas indexadas; (c) disponibles en texto completo con DOI; (d) redactados en inglés o español; y (e) enfocados directamente en data brokers y su relación con privacidad, ciberseguridad, protección de datos o mercados de datos.

Se excluyeron: (a) documentos duplicados entre bases de datos; (b) artículos cuyos títulos o resúmenes no abordarán explícitamente la relación entre intermediarios de datos y riesgos de seguridad o privacidad; y (c) estudios sin acceso completo o con calidad metodológica insuficiente, según los criterios PRISMA establecidos.

Figura 1*Proceso de recolección de estudios PRISMA 2020 de datos*

Nota. Autores, (2026)

Para responder a la pregunta de investigación, se diseñaron estrategias de búsqueda específicas para cada base de datos consultada.

En Sciencedirect se utilizaron las combinaciones: "data brokers" AND "digital security" OR "information security" y "data brokers" AND "data privacy" OR "personal data" OR "data protection" AND "risks" OR "threats". En Scopus se aplicaron: "data broker*" OR "information broker*" OR "data harvesting" y "data broker" OR "information broker*" OR "data trading" OR "data marketplace". Para Springer Nature se emplearon ecuaciones que combinaron términos relacionados con intermediarios de datos, seguridad digital e impactos o riesgos.

Tabla 1

La adquisición de las investigaciones se llevó a cabo a través de la exploración en buscadores académicos y sus herramientas de búsqueda correspondientes

Base de búsqueda	Términos de Búsqueda	Resultados	Seleccionados
Science Direct	("data brokers") AND ("digital security" OR "information security") ("data brokers") AND ("data privacy" OR "personal data" OR "data protection") AND ("risks" OR "threats")	475	5
Scopus	(TITLE-ABS-KEY ("data broker*" OR "information broker*" OR "data harvesting")) AND (TITLE-ABS-KEY ("privacy risk" OR "cyber risk" OR "security threat*" OR "identity theft" OR "data breach")) AND PUBYEAR > 2021 AND PUBYEAR < 2026 AND (LIMIT-TO (DOCTYPE, "ar")) AND (LIMIT-TO (OA, "all")) (TITLE-ABS-KEY ("data broker*" OR "information broker*" OR "data trading" OR "data marketplace")) AND (TITLE-ABS-KEY ("information security" OR "digital security" OR "cybersecurity" OR "data protection" OR "privacy")) AND PUBYEAR > 2021 AND PUBYEAR < 2026 AND (LIMIT-TO (OA, "all")) AND (LIMIT-TO (DOCTYPE, "ar"))	576	3
Springer Nature	("data broker" OR "data brokers" OR "information broker" OR "data intermediary") AND ("digital security" OR "information security" OR "cybersecurity" OR "data protection") AND (impact OR effect OR risk* OR threat* OR challenge*) ("data broker" OR "information broker") AND ("privacy" OR "data privacy" OR "personal data") AND ("security" OR "breach" OR "leak" OR "unauthorized access")	1027	4

Nota. Autores, (2026)

Tras la aplicación de la ecuación de búsqueda en las bases de datos Scopus, Sciencedirect y SpringerNature, se identificaron inicialmente un total de 2078 registros. Durante la fase de identificación, se obtuvieron 576 documentos de Scopus, 475 de Sciencedirect y 1027 registros de SpringerNature, los cuales fueron sometidos a un proceso sistemático de cribado siguiendo el protocolo PRISMA (Preferred Reporting Items for Systematic reviews and Meta-Analyses).

En la primera etapa de cribado, se procedió a la eliminación de duplicados mediante el uso de gestores bibliográficos, y posteriormente se aplicaron los criterios de inclusión y exclusión específicos establecidos para el estudio. Durante esta fase, se excluyeron 1924 registros que no cumplían con los criterios específicos y eran duplicados, resultando en 154 documentos pre-seleccionados para la evaluación detallada. Luego, se retiraron 132 documentos, los cuales no tenían un título relevante y relacionado con el tema de investigación.

En la fase de elegibilidad, los 22 artículos restantes fueron sometidos a una lectura completa y evaluación exhaustiva. Como resultado de este proceso, se excluyeron 10 artículos tras su lectura completa por no ajustarse completamente a los objetivos de la investigación, resultando en una muestra final de 12 registros incluidos en la revisión.

En los 12 artículos seleccionados, se aplicó un análisis de contenido temático siguiendo las directrices de Kiger y Varpio (2020). Dos revisores extrajeron independientemente los metadatos críticos de cada estudio: objetivos, diseño metodológico, hallazgos principales y riesgos identificados, sistematizándolos en una matriz de extracción estandarizada.

Mediante codificación inductiva y deductiva, se identificaron unidades de significado emergentes y se establecieron cuatro categorías analíticas: (a) dinámicas económicas de los data brokers; (b) dinámicas tecnológicas y de infraestructura; (c) dinámicas sociales y consideraciones éticas; y (d) desafíos de gobernanza y regulación. Las discrepancias se resolvieron por consenso, alcanzando un índice Kappa de 0.85. Este proceso permitió una síntesis narrativa estructurada de la evidencia.

Análisis Bibliométrico

De los 2078 registros inicialmente identificados (576 de Scopus, 475 de ScienceDirect y 1027 de Springer Nature), se importaron 1051 documentos obtenidos de Scopus y Sciencedirect en VOSviewer (versión 1.6.20), ya que los registros restantes procedentes de Springer Nature se utilizaron solo en la revisión cualitativa debido a limitaciones técnicas de exportación masiva.

Este software permite la creación y examen detallado de mapas bibliométricos, incluyendo información sobre año de publicación, idioma, revista, título, autor, institución, palabras clave, tipo de documento, resumen y recuento de citas. VOSviewer es una herramienta de software diseñada para crear, explorar y visualizar mapas derivados de datos de redes bibliométricas, permitiendo construir redes de publicaciones científicas, revistas, investigadores, instituciones, países, palabras clave o términos conectados a través de coautoría, co-publicación, citas o enlaces bibliográficos (Van Eck & Waltman, 2022).

Adicionalmente, se utilizó el software R con su aplicación RStudio, específicamente el paquete Bibliometrix, desarrollado por Massimo Aria y Corrado Cuccurullo. Esta herramienta proporcionó funcionalidades complementarias para realizar un análisis bibliométrico completo, siguiendo el flujo de trabajo de mapeo científico establecido (Gregorio-Chaviano, 2024).

Resultados y Discusión

La presente investigación buscó responder de qué manera las dinámicas económicas, tecnológicas, sociales y éticas de los data brokers influyen críticamente en los riesgos de ciberseguridad y protección de datos. El análisis de los estudios revela que los data brokers son actores centrales en un ecosistema digital complejo, cuyas operaciones generan tensiones fundamentales entre la eficiencia del mercado, la innovación y los derechos de los individuos. La dinámica observada en los mercados de datos no es lineal y es inherentemente compleja, un fenómeno que surge de la transformación de la información personal en capital, dando lugar a sistemas como el "capitalismo de vigilancia" (Baik & Famularo, 2024; Deng & Shi, 2025). Esta búsqueda de valor económico crea intrínsecamente riesgos sistémicos a través de externalidades negativas, como la vigilancia no deseada y la elaboración de perfiles coercitivos (Baik & Famularo, 2024).

Dinámicas Económicas: Fallas de Mercado y Creación de Barreras

Las dinámicas económicas de los data brokers se encuentran intrínsecamente ligadas a las fallas del mercado de datos. Deng y Shi (2025) describen estas fallas como la incapacidad de los mecanismos del mercado para asignar eficientemente los recursos de datos, resultando en una baja eficiencia de asignación y la imposibilidad de maximizar el bienestar social. Debido a las características únicas de los datos como mercancía —son no rivales y su valor aumenta con el uso (efectos de red)—, lo que genera un desajuste fundamental con los mecanismos de compensación monetaria tradicionales. En este contexto, los data brokers actúan como intermediarios monopolísticos u oligopólicos que, lejos de resolver estas fallas, a menudo las explotan para maximizar sus beneficios.

Un mecanismo central identificado es la discriminación de precios. Clavorà Braulin (2021) sostiene que los data brokers venden información del consumidor a empresas competidoras, permitiéndoles implementar estrategias de precios personalizados. Curiosamente, la información parcial sobre los consumidores resulta ser más rentable para la industria que la información completa, creando una relación en forma de "U" invertida entre la cantidad de datos y los beneficios, por lo tanto, los consumidores resultan perjudicados en escenarios de privacidad intermedia.

Esta dinámica se agrava por el "efecto de barrera de entrada", como lo analizan Abrardi et al. (2024, 2025). Estos autores demuestran que tanto un data broker monopolista como los brokers en competencia pueden ajustar estratégicamente la cantidad de datos que venden para moderar la competencia en los mercados descendentes. Al vender datos, crean una barrera que reduce la entrada de nuevas empresas, perjudicando a los consumidores a través de una mayor concentración del mercado. El mecanismo de venta utilizado es crucial, ya que este define el poder de negociación del broker y, por ende, la cantidad de datos transaccionados y el perjuicio al consumidor.

Abrardi et al. (2024) analizan el impacto de tres mecanismos que representan niveles decrecientes de poder de negociación del DB monopolista:

Subasta con Precio de Reserva (AR - Auction with Reserve Prices), este mecanismo otorga el mayor poder al broker. En este caso, el DB maximiza la extracción de rentas vendiendo a empresas alternas y restringe estratégicamente la cantidad de datos, lo que resulta en la menor cantidad de datos vendidos y el mayor perjuicio para el consumidor.

Subasta sin Precio de Reserva (AU - Auction without Reserve Prices), con poder intermedio, el DB también opta por la venta a empresas alternas para maximizar el efecto barrera de entrada, ofreciendo un tamaño de partición lo suficientemente grande ($\geq 3/2n$) para minimizar la entrada de empresas.

Oferta Tómalo o Déjalo (TIOLI - Take-It-Or-Leave-It): Este mecanismo representa el menor poder de negociación para el broker. Al no poder usar la amenaza de la subasta, el DB opta por vender a todas las empresas, lo que lleva a la mayor cantidad de datos vendidos y el menor perjuicio para el consumidor en comparación con los mecanismos de subasta.

Este conjunto de hallazgos subraya que, desde una perspectiva económica, el modelo de negocio de los data brokers tiende a priorizar la extracción de rentas sobre el bienestar del consumidor y la competencia justa.

Dinámicas Tecnológicas: Entre la Centralización Riesgosa y la Descentralización Emergente

El modelo operativo tradicional de los data brokers se basa en una infraestructura tecnológica centralizada que, si bien es eficiente para la agregación de datos, presenta riesgos inherentes de seguridad y privacidad. Bokolo Anthony Jr. (2023) señala que los mercados de datos centralizados introducen serias preocupaciones de confianza, ya que una autoridad central tiene acceso a los datos y puede beneficiarse ilegalmente de ellos, además de crear puntos únicos de fallo. Esta vulnerabilidad se magnifica en entornos como las ciudades inteligentes, donde la fragmentación de datos en silos tecnológicos también compromete la interoperabilidad y la seguridad.

Como respuesta a estos riesgos, surgen dinámicas tecnológicas alternativas basadas en la descentralización. Bokolo Anthony Jr. (2023) propone un ecosistema descentralizado que utiliza tecnologías de registro distribuido (DLT) como IOTA y un intermediario de mensajes (MQTT) para automatizar el intercambio de datos de forma segura, sin la necesidad de un tercero de confianza. Este enfoque busca mejorar la seguridad, mitigar problemas de rendimiento y eliminar puntos únicos de fallo. De manera similar, Deng y Shi (2025) apuntan a tecnologías como el aprendizaje federado y blockchain como vías futuras de gobernanza para proteger la privacidad mientras se habilita el uso de datos. Scheider et al. (2023) exploran la diversidad de diseños de mercados de datos personales (PDMs), identificando arquetipos que a menudo se basan en blockchain y tokenomics para gestionar el consentimiento y la propiedad de los datos. Sin embargo, estos autores advierten que incluso los PDMs descentralizados enfrentan desafíos interdisciplinarios (legales, económicos y éticos) que ponen en riesgo tanto su viabilidad como la protección de los individuos, especialmente en lo que respecta a la mercantilización de los "rastros de datos" de la vida humana. Por lo tanto, aunque la tecnología descentralizada ofrece una solución prometedora a los riesgos de los sistemas centralizados, su diseño e implementación deben abordar cuidadosamente los mismos dilemas éticos y de gobernanza.

Dinámicas Sociales y Éticas: Mercantilización de Datos Sensibles y Consentimiento Ilusorio

Las prácticas de los data brokers tienen profundas implicaciones sociales y éticas, particularmente en la recopilación y comercialización de datos sensibles. El estudio de Baik y Famularo (2024) sobre los programas de lealtad (LPs) revela cómo se recopilan y comercializan datos de salud de los consumidores fuera del alcance de regulaciones como la ley HIPAA en Estados Unidos.

Estos programas crean redes de múltiples actores que intercambian datos de salud, llevando a una mercantilización de información íntima sin un consentimiento informado y significativo por parte de los consumidores, lo que puede resultar en vigilancia no deseada y perfiles coercitivos.

Este problema se extiende a otros sectores. Spithoff y Grundy (2023) analizan cómo los data brokers comercializan bases de datos de atención primaria a la industria farmacéutica, describiendo información detallada e íntima a nivel de paciente. A pesar de las afirmaciones de que los datos están des-identificados, los autores advierten sobre el riesgo persistente de re-identificación, especialmente para personas con diagnósticos inusuales. Friedman et al. (2023) complementan esta visión al demostrar que el 98.6% de los sitios web de hospitales en EE. UU. instalan código de seguimiento de terceros, transfiriendo datos de navegación de los visitantes a data brokers y otras empresas tecnológicas, lo cual puede revelar información de salud sensible y generar serios riesgos de privacidad.

La cuestión del consentimiento es central en este debate. Deng y Shi (2025) describen la "paradoja de la privacidad", donde los consumidores, a menudo por conveniencia, comparten más datos de los que desearían, subvalorando su información personal. Baik y Famularo (2024) critican lo que denominan un "empoderamiento superficial del consumidor", en el que las empresas ofrecen opciones de exclusión limitadas en lugar de una protección genuina, mientras minimizan su responsabilidad por los riesgos de privacidad. Esta dinámica transforma la privacidad en una mercancía de lujo, accesible solo para quienes pueden permitirse no participar en estos ecosistemas de datos. La mercantilización de la información personal, especialmente la relacionada con la salud, la educación (Isus et al., 2024) o la ubicación, plantea un desafío ético fundamental que los marcos regulatorios actuales luchan por abordar.

Desafíos para la Ciberseguridad y la Protección de Datos: Fragmentación Regulatoria y Gobernanza

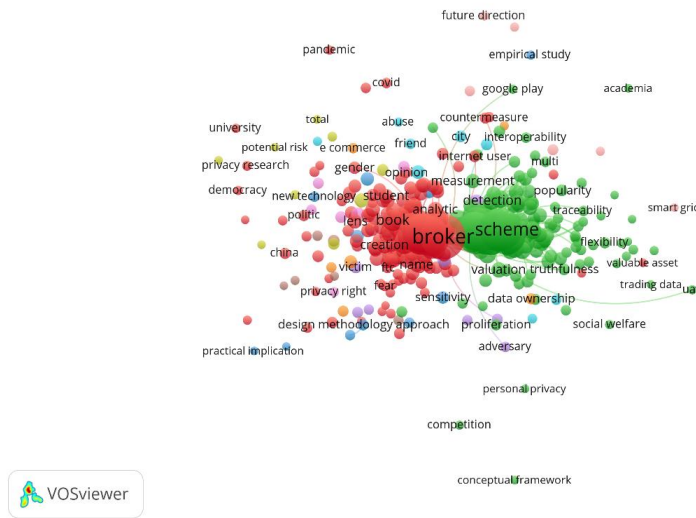
Los riesgos para la ciberseguridad y la protección de datos se ven exacerbados por la fragmentación y las insuficiencias de los marcos regulatorios. La Ley de Gobernanza de Datos (DGA) de la Unión Europea, por ejemplo, intenta regular a los intermediarios de datos como actores neutrales, pero, como señalan Carovano y Finck (2023), sus requisitos pueden hacer que estos intermediarios no sean económicamente viables, especialmente frente a las grandes tecnológicas no sujetas a las mismas reglas. Esta incoherencia dentro del marco legal de la UE (DGA, GDPR, DMA) crea incertidumbre y puede sofocar la innovación en lugar de fomentarla.

En el ámbito educativo, Isus et al. (2024) identifican que la intermediación a través de un data broker aumenta los riesgos de pérdida de datos personales en múltiples etapas: durante la transferencia, en el almacenamiento del broker y, crucialmente, cuando éste distribuye los datos a terceros sin el control de la institución educativa. Su propuesta de anonimizar los datos en origen resalta la necesidad de soluciones tecnológicas que complementen la regulación.

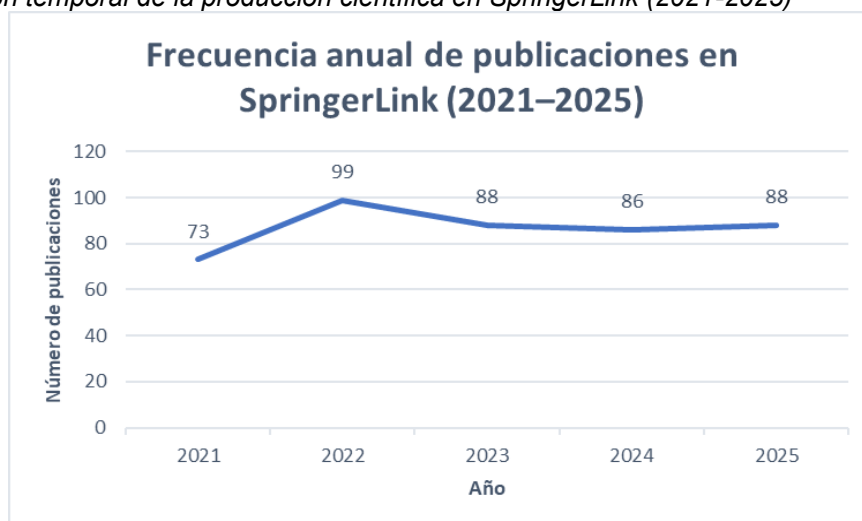
La falta de una conceptualización clara de los intermediarios de datos también es un desafío. Schweihoff et al. (2024) argumentan que la "confusión conceptual" sobre qué son los intermediarios de datos y qué servicios ofrecen crea un riesgo regulatorio, ya que las empresas pueden no cumplir con las normativas simplemente porque no se reconocen a sí mismas como tales. Esta situación subraya la necesidad de una gobernanza de datos más robusta e interempresarial, que aborde las externalidades negativas a nivel de sistema y exija mayor transparencia y auditoría, especialmente considerando que los data brokers a menudo operan en una "zona gris" legal, explotando excepciones y la falta de una supervisión rigurosa.

Análisis Bibliométrico: Estructura Temática, Tendencias Temporales y Colaboración Internacional

El análisis de co-ocurrencia de palabras clave realizado mediante VOSviewer como se muestra en la Figura 2 reveló la estructura temática central del campo de estudio, identificando dos clústeres principales de investigación basados en 237 términos con frecuencia mínima de aparición. El cluster 1 (rojo), compuesto por 20 ítems, se articula en torno a términos relacionados con aspectos regulatorios y de gestión, donde destacan "broker" (237 ocurrencias), "consumer" (168), "company" (159) y "personal information" (137). Este cluster aborda principalmente las dimensiones legales, empresariales y de protección de datos en el ecosistema digital. Por el contrario, el cluster 2 (verde), constituido por 21 elementos, concentra aspectos técnicos y tecnológicos del campo, liderado por "blockchain" (208 ocurrencias), "mechanism" (200), "data trading" (178) y "internet" (165). La fortaleza de los vínculos temáticos se evidencia en la alta conectividad entre términos, siendo "broker" el nodo con mayor fuerza de enlace total (3,131), seguido por "blockchain" (2,767) y "mechanism" (2,701), lo que confirma la centralidad de estos conceptos en la literatura analizada.

Figura 2*Mapa de coocurrencias de palabras clave**Nota. Autores, (2026)*

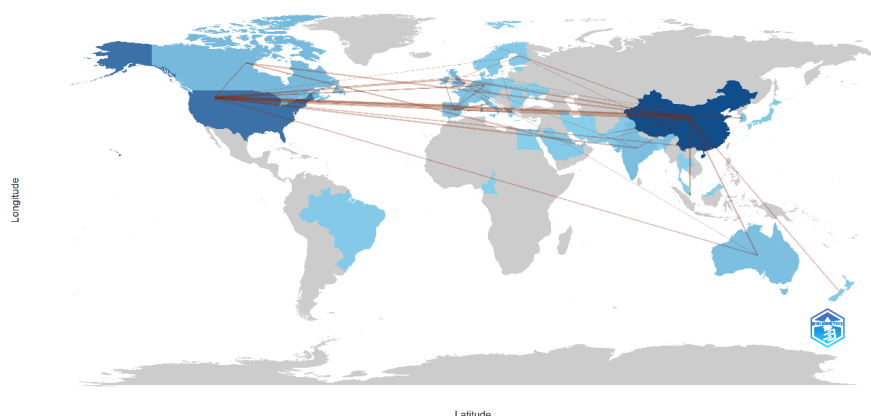
La Figura 3 ilustra la evolución temporal de la producción científica en SpringerLink, el análisis reveló una tendencia fluctuante con un pico máximo en 2022, registrando 99 publicaciones. Posteriormente, se observó una disminución gradual, con 88 publicaciones en 2023 y 86 en 2024, estabilizándose en 88 publicaciones proyectadas para 2025. Esta tendencia sugiere una fase de consolidación tras el período de crecimiento inicial, posiblemente influenciada por la maduración del campo de estudio y la especialización temática de las investigaciones.

Figura 3*Evolución temporal de la producción científica en SpringerLink (2021-2025)**Nota. Autores, (2026)*

El mapa de colaboración internacional desarrollado con Biblioshiny evidenció patrones significativos de cooperación científica global como se observa en la Figura 4. La colaboración más intensa se registró entre China y Estados Unidos con 41 publicaciones conjuntas, posicionándose como el eje principal de cooperación internacional. Asimismo, China estableció vínculos importantes con Singapur (8), Hong Kong (7), Reino Unido (7) y Australia (6), mientras que Estados Unidos desarrolló colaboraciones destacadas con Reino Unido (7), Francia (5) e India (5). En el contexto europeo, la colaboración entre Italia y España alcanzó 5 publicaciones conjuntas, y España mantuvo conexiones con Grecia (4) e Irlanda (3). Los datos revelan que China participó en 104 colaboraciones internacionales, seguida por Estados Unidos con 87, Reino Unido con 37, y España con 32, consolidando estos países como los principales actores en la red de cooperación científica internacional del campo de estudio.

Figura 4

Mapa mundial de colaboración científica por países
Country Collaboration Map



Nota. Autores, (2026)

Conclusiones

Esta revisión sistemática cumplió su objetivo de examinar cómo las dinámicas económicas, tecnológicas, sociales y éticas de los data brokers generan riesgos para la privacidad y la ciberseguridad. El análisis de 12 estudios reveló que estos intermediarios operan en un ecosistema donde las fallas estructurales del mercado —discriminación de precios y barreras estratégicas de entrada— se amplifican tecnológicamente mediante modelos centralizados que concentran vulnerabilidades de seguridad. Esta dualidad genera una tensión permanente: mientras facilitan nuevas formas de negocio e innovación, exponen a las personas a mayores riesgos de privacidad, seguridad y pérdida de control sobre sus datos.

El análisis de coocurrencias mediante VOSviewer identificó dos clusters temáticos principales que evidencian los mecanismos que vinculan riesgos con vacíos regulatorios. El cluster regulatorio (centrado en "broker", "consumer", "personal information") y el cluster tecnológico (articulado en "blockchain", "mechanism", "data trading") revelan una desconexión estructural: mientras la investigación técnica avanza hacia soluciones descentralizadas, los marcos normativos permanecen fragmentados y carentes de definiciones operativas precisas. Esta desarticulación permite que, en la publicidad digital, múltiples intermediarios operen sin responsabilidad clara; en la intermediación de ubicación, se almacenen datos sin garantías de anonimización; y en mercados descentralizados, se comercialicen datos sensibles sin trazabilidad ni auditoría.

Desde la perspectiva social y regulatoria, la literatura revisada demuestra que el paradigma del consentimiento individual ha sido superado por la necesidad de responsabilidad demostrable (accountability). Las empresas deben evidenciar trazabilidad de datos, aplicar principios de minimización y garantizar transparencia operativa mediante marcos verificables y auditables. El análisis bibliométrico reveló una concentración de investigación en colaboraciones China-Estados Unidos (41 publicaciones conjuntas), evidenciando una brecha significativa en América Latina que implica dependencia regulatoria, adopciones acríticas de marcos externos y brechas de protección adaptadas al contexto regional.

Como limitaciones, se reconoce que la concentración de estudios en países desarrollados restringe la generalización de hallazgos a contextos latinoamericanos, la exclusión de literatura gris puede haber omitido perspectivas regulatorias relevantes, y el período analizado (2021-2025) captura únicamente tendencias recientes. Para investigaciones futuras, se propone desarrollar estudios empíricos comparativos sobre efectos diferenciados de data brokers en sectores críticos latinoamericanos, examinar la viabilidad de modelos de protección desde el diseño (privacy by design) con auditoría continua, y construir marcos normativos con criterios operativos verificables que aborden las interconexiones sistémicas identificadas en esta revisión.

Referencias

- Abrardi, L., Cambini, C., & Pino, F. (2024). Regulating data sales: The role of data selling mechanisms. *Telecommunications Policy*, 48(8), 102813. <https://doi.org/10.1016/j.telpol.2024.102813>
- Abrardi, L., Cambini, C., & Pino, F. (2025). Data brokers competition, synergic datasets, and endogenous information value. *International Journal of Industrial Organization*, 103146. <https://doi.org/10.1016/j.ijindorg.2025.103146>
- Anthony, B. (2023). Decentralized brokered enabled ecosystem for data marketplace in smart cities towards a data sharing economy. *Environment Systems and Decisions*, 43(3), 453-471. <https://doi.org/10.1007/s10669-023-09907-0>
- Baik, J. S., & Famularo, J. (2024). Contextual integrity of loyalty programs, compromised? Interrogating consumer health data practices and networked actors in the U.S. retail sector. *Telecommunications Policy*, 48(7), 102780. <https://doi.org/10.1016/j.telpol.2024.102780>
- Carovano, G., & Finck, M. (2023). Regulating data intermediaries: The impact of the Data Governance Act on the EU's data economy. *Computer Law & Security Review*, 50, 105830. <https://doi.org/10.1016/j.clsr.2023.105830>
- Clavorà Braulin, F. (2023). The effects of personal information on competition: Consumer privacy and partial price discrimination. *International Journal of Industrial Organization*, 87, 102923. <https://doi.org/10.1016/j.ijindorg.2023.102923>
- Deng, X., & Shi, Y. (2025). A study on the causes and regulation of data market failure. *The 12th International Conference on Information Technology and Quantitative Management (ITQM 2025)*, 266, 1220-1225. <https://doi.org/10.1016/j.procs.2025.08.150>
- DiPersio, D. (2024). Selling personal information: Data brokers and the limits of US regulation. En I. Siegert & K. Choukri (Eds.), *Proceedings of the Workshop on Legal and Ethical Issues in Human Language Technologies @ LREC-COLING 2024* (pp. 39–46). ELRA and ICCL. <https://aclanthology.org/2024.legal-1.7/>
- Friedman, A. B., Merchant, R. M., Maley, A., Farhat, K., Smith, K., Felkins, J., Gonzales, R. E., Bauer, L., & McCoy, M. S. (2023). Widespread third-party tracking on hospital websites poses privacy risks for patients and legal liability for hospitals. *Health Affairs*, 42(4), 508-515. <https://doi.org/10.1377/hlthaff.2022.01205>

- González, L. D. (2019). Control de nuestros datos personales en la era del big data: El caso del rastreo web de terceros. *Estudios Socio-Jurídicos*, 21(1).
<https://doi.org/10.12804/revistas.urosario.edu.co/sociojuridicos/a.6941>
- Gregorio-Chaviano, O. (2024). *Guía de trabajo con Biblioshiny*.
<https://zenodo.org/records/11078477/files/Biblioshiny%20Manual01.pdf>
- Isus, R., Kolesnikova, K., Khlevna, I., Oleksandr, T., & Liubov, K. (2024). Development of a model of personal data protection in the context of digitalization of the educational sphere using information technology tools. *14th International Conference on Emerging Ubiquitous Systems and Pervasive Networks / 13th International Conference on Current and Future Trends of Information and Communication Technologies in Healthcare (EUSPN/ICTH 2023)*, 231, 347-352.
<https://doi.org/10.1016/j.procs.2023.12.215>
- Kiger, M. E., & Varpio, L. (2020). Thematic analysis of qualitative data: AMEE Guide No. 131. *Medical Teacher*, 42(8), 846-854.
<https://doi.org/10.1080/0142159X.2020.1755030>
- Kim, J. (2023). *Data brokers and the sale of Americans' mental health data*. [Documento técnico]. Duke Sanford School of Public Policy.
<https://donestech.net/files/kim-2023-data-brokers-and-the-sale-of-americans-mental-health-data.pdf>
- Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., Shamseer, L., Tetzlaff, J. M., Akl, E. A., Brennan, S. E., Chou, R., Glanville, J., Grimshaw, J. M., Hróbjartsson, A., Lalu, M. M., Li, T., Loder, E. W., Mayo-Wilson, E., McDonald, S., ... Alonso-Fernández, S. (2021). Declaración PRISMA 2020: Una guía actualizada para la publicación de revisiones sistemáticas. *Revista Española de Cardiología*, 74(9), 790-799.
<https://doi.org/10.1016/j.recesp.2021.06.016>
- Reviglio, U. (2022). The untamed and discreet role of data brokers in surveillance capitalism: A transnational and interdisciplinary overview. *Internet Policy Review*, 11(3).
<https://doi.org/10.14763/2022.3.1670>
- Scheider, S., Lauf, F., Geller, S., Möller, F., & Otto, B. (2023). Exploring design elements of personal data markets. *Electronic Markets*, 33(1), 28.
<https://doi.org/10.1007/s12525-023-00646-3>
- Schweihoff, J., Lipovetskaja, A., Jussen-Lengersdorf, I., & Möller, F. (2024). Stuck in the middle with you: Conceptualizing data intermediaries and data intermediation services. *Electronic Markets*, 34(1), 48.
<https://doi.org/10.1007/s12525-024-00729-9>

- Sherman, J. (2021). *Data brokers and sensitive data on US individuals*. [Documento técnico]. Duke University Sanford Cyber Policy Program. <https://techpolicy.sanford.duke.edu/wp-content/uploads/2021/08/Data-Brokers-and-Sensitive-Data-on-US-Individuals-Sherman-2021.pdf>
- Spithoff, S., & Grundy, Q. (2023). Commercializing personal health information: A critical qualitative content analysis of documents describing proprietary primary care databases in Canada. *International Journal of Health Policy and Management*, 12(1). <https://doi.org/10.34172/ijhpm.2023.6938>
- Van Eck, N. J., & Waltman, L. (2022). *VOSviewer manual* (Versión 1.6.20) [Manual de software]. Universiteit Leiden. https://www.vosviewer.com/documentation/Manual_VOSviewer_1.6.20.pdf