Programa sobre
Sistemas Financieros Internacionales

Localización de Datos, Adopción de la Nube y el Sector Financiero

[Traducido del Inglés]

JULIO 2024

El Programa sobre Sistemas Financieros Internacionales (PIFS) es una organización 501(c)(3) que realiza investigaciones sobre temas que afectan al sistema financiero global. PIFS también organiza simposios internacionales, programas de educación ejecutiva y eventos especiales que fomentan el diálogo y promueven la educación sobre estos temas. PIFS fue fundado en 1986 por Hal S. Scott, actualmente Profesor Emérito de la Facultad de Derecho de Harvard. Más de treinta años después, Hal Scott sigue liderando PIFS.

Este informe fue preparado por Hal Scott (Presidente de PIFS), John Gulliver (Director Ejecutivo), Hillel Nadler (Investigador Principal), y Jon Ondrejko (Vicepresidente Senior de Programas).

Amazon Web Services, Inc. es un patrocinador financiero de PIFS.

[El informe original fue redactado en Inglés.
Esta versión ha sido traducida al Español.]

© Programa sobre Sistemas Financieros Internacionales 2024. Todos los derechos reservados. Se pueden reproducir o traducir extractos limitados siempre que se indique la fuente.

Localización de Datos, Adopción de la Nube y el Sector Financiero

JULIO 2024

Índice

RESUMEN EJECUTIVO

En un mundo cada vez más conectado, la capacidad de las instituciones financieras para transferir datos a través de fronteras es crucial para su éxito y para atender a sus clientes. No obstante, cada vez más jurisdicciones están implementando requisitos de "localización de datos" que restringen o incluso prohíben la transferencia de datos fuera de sus fronteras. Este informe explora cómo estos requisitos impactan al sector financiero a medida que aumenta la adopción de la computación en la nube. Los requisitos de localización de datos, aunque a menudo son motivados por preocupaciones políticas legítimas, imponen costos significativos a las instituciones financieras y sus clientes, impidiendo el uso completo de la computación en la nube. Los reguladores pueden abordar estas preocupaciones sin restringir el libre flujo de datos, que es vital para aprovechar los beneficios de la nube en el sector financiero.

La Promesa de la Tecnología en la Nube para el Sector Financiero

La pandemia de COVID-19 aceleró una tendencia que ya estaba en marcha: la adopción de la computación en la nube por parte de las instituciones financieras. La tecnología en la nube ofrece beneficios significativos, incluyendo eficiencia en costos, mejor ciberseguridad y resiliencia operativa. Al permitir que las instituciones financieras escalen automáticamente sus recursos de computación, la tecnología en la nube les permite manejar eventos de estrés en el mercado, como aumentos inesperados en los volúmenes de transacciones o ciberataques, que podrían abrumar la infraestructura tecnológica (IT) tradicional. Además, los extensos recursos de computación disponibles en la nube facilitan el acceso a tecnologías avanzadas como el análisis de datos y la inteligencia artificial (IA), que prometen transformar cómo las instituciones financieras satisfacen las necesidades de sus clientes y gestionan el riesgo.

El Rol Crítico de los Flujos de Datos Transfronterizos en las Finanzas

Las transferencias de datos transfronterizos son esenciales para el sector financiero global. Son necesarias para procesar pagos internacionales, proporcionar servicios financieros a clientes que viven o hacen negocios en múltiples jurisdicciones y facilitar la supervisión regulatoria. Incluso las instituciones financieras locales dependen de los flujos de datos transfronterizos cuando conectan a sus clientes con redes financieras globales. Al obstaculizar estos flujos, los requisitos de localización de datos limitan la capacidad de las instituciones financieras para satisfacer las necesidades de sus clientes e incluso la capacidad de los reguladores financieros para llevar a cabo una supervisión efectiva.

Requisitos de Localización de Datos y Adopción de la Nube

Los defensores de la localización de datos a menudo argumentan que mejora la privacidad de los datos, asegura la disponibilidad de los datos en caso de una interrupción y facilita la supervisión regulatoria y la aplicación de la ley. Sin embargo, estos argumentos son erróneos. La ubicación física de los datos no es ni necesaria ni suficiente para su seguridad; los datos que no se gestionan de forma segura pueden ser comprometidos sin importar dónde se almacenan. Además, los principales proveedores de nube, debido a las economías de escala, pueden invertir mucho más en ciberseguridad y resiliencia

que los proveedores locales de tecnología. Y el almacenamiento local de datos no garantiza el acceso regulatorio; los reguladores pueden asegurar el acceso a los datos almacenados en el extranjero a través de acuerdos bilaterales o multilaterales.

Los requisitos de localización de datos también amenazan con cortar a las instituciones financieras de los beneficios de la adopción de la nube, que dependen críticamente de la capacidad de mover datos a través de fronteras. Los principales proveedores de nube no mantienen centros de datos en cada jurisdicción. En su lugar, aprovechan las economías de escala operando una red global de centros de datos. Esta infraestructura distribuida es clave para las ventajas de resiliencia y ciberseguridad de la nube: los datos y procesos pueden ser distribuidos en diferentes centros de datos, haciéndolos menos vulnerables a interrupciones o ataques localizados. Esa infraestructura distribuida también proporciona los recursos de computación masivos que permiten el análisis avanzado y la IA.

Recomendaciones de Política para los Reguladores Financieros

Para equilibrar las preocupaciones políticas legítimas con el imperativo de facilitar los flujos de datos transfronterizos para permitir la adopción de la nube, el informe recomienda que los reguladores financieros:

- Adopten un enfoque basado en principios para la protección de datos que se enfoque en asegurar que los datos se almacenen de manera segura, en lugar de dónde se almacenan.
- Trabajen juntos con las entidades reguladas y los proveedores de servicios en la nube para aprovechar la infraestructura global en la nube fuera de la jurisdicción de una manera que mejore la ciberseguridad y la resiliencia operativa.
- Aseguren el acceso a los datos para la supervisión regulatoria y la aplicación de la ley a través de acuerdos con otras jurisdicciones, no mediante la localización de datos.
- Aumenten la coordinación con otras autoridades locales y contrapartes extranjeras para desarrollar políticas coherentes para la transferencia de datos.

Conclusión

Los requisitos de localización de datos, aunque a menudo se basan en preocupaciones legítimas, imponen costos significativos a las instituciones financieras y a sus clientes. Estos requisitos limitan la capacidad de las instituciones para aprovechar la tecnología en la nube, lo que afecta la seguridad, la resiliencia y la innovación. Al implementar políticas que faciliten los flujos de datos transfronterizos seguros, los reguladores financieros pueden abordar sus preocupaciones sin obstaculizar el sector financiero global. En un mundo cada vez más interconectado, el libre flujo de datos no solo es beneficioso, sino esencial.

INTRODUCCIÓN

El sector financiero depende de la información: el éxito de las instituciones financieras depende de su capacidad para obtener, proteger y utilizar información para su beneficio y el beneficio de sus clientes. Los datos financieros incluyen información sobre los clientes, como su nombre y número de cuenta, así como información sobre las empresas y sus empleados clave. La creciente dependencia de las instituciones financieras en los servicios en la nube para almacenar, procesar y transmitir información de manera segura y eficiente ha planteado desafíos sobre cómo las jurisdicciones regulan los datos financieros.

En un mercado global, como el mercado de servicios financieros, el libre flujo de datos a través de las fronteras genera un valor significativo. El movimiento transfronterizo de datos es esencial para procesar pagos internacionales, proporcionar servicios financieros a clientes individuales y empresariales, y mejorar la gestión de riesgos a nivel de las instituciones financieras. Sin embargo, en los últimos años se han impuesto requisitos de "localización de datos": restricciones que requieren directamente, o que tienen como consecuencia, que los datos originados en una jurisdicción permanezcan en esa jurisdicción.[1]

Este informe analiza los requisitos de localización de datos y su impacto en el sector financiero. La Parte I del informe proporciona antecedentes sobre la adopción de la nube en el sector financiero y el papel crítico de los flujos de datos transfronterizos para el sector financiero. La Parte II profundiza en los diferentes tipos de requisitos de localización de datos, las motivaciones declaradas para adoptar estos requisitos y sus posibles desventajas. La Parte III se enfoca en cómo los requisitos de localización de datos afectan a las instituciones financieras y su capacidad para beneficiarse de la adopción de la nube.

La Parte IV concluye con recomendaciones de políticas para los reguladores financieros respecto a la transferencia de datos transfronterizos en el contexto de la adopción de la nube que aborden las preocupaciones que los gobiernos nacionales y los reguladores financieros han utilizado para justificar los requisitos de localización de datos. Los reguladores deben adoptar un enfoque basado en principios para la protección de datos que permita la transferencia segura de datos a otras jurisdicciones, siempre que se ofrezcan niveles suficientes de protección para los datos privados. También deben reconocer que la infraestructura tecnológica global fuera de la jurisdicción puede mejorar la ciberseguridad y la resiliencia operativa. En lugar de enfocarse en la ubicación de los datos, los reguladores pueden abordar las preocupaciones sobre la supervisión regulatoria y la aplicación de la ley asegurando el acceso a los datos. Además, deben trabajar para alinear las políticas de transferencia de datos con otras autoridades locales y reguladores en otras jurisdicciones.

[1] David McCabe y Adam Satariano, *La Era de los Datos Sin Fronteras Está Terminando*, NEW YORK TIMES (23 de mayo de 2022), https://www.nytimes.com/2022/05/23/technology/data-privacy-laws.html.

PARTE I: ADOPCIÓN DE LA NUBE Y TRANSFERENCIAS INTERNACIONALES DE DATOS EN EL SECTOR FINANCIERO

La computación en la nube permite que los datos se almacenen en servidores remotos mantenidos por un proveedor externo y se recuperen a través de una red, como Internet, en lugar de en infraestructura propia y local.[2] Aunque la computación en la nube no es nueva para el sector financiero, la pandemia de COVID-19 aceleró la adopción de la nube por parte de las instituciones financieras. La adopción de la nube ofrece una promesa significativa de eficiencia en costos, resiliencia operativa, ciberseguridad e innovación para las instituciones financieras. También ayuda a facilitar flujos de datos transfronterizos seguros, que desempeñan un papel crítico en el mercado global de servicios financieros. Sin embargo, los requisitos de localización de datos perjudican la capacidad de las instituciones financieras para aprovechar la tecnología en la nube en beneficio propio y de sus clientes.

a. Adopción de la nube en el sector financiero

Las instituciones financieras han estado utilizando la tecnología en la nube, de una forma u otra, durante casi dos décadas.[3] La adopción de servicios en la nube en el sector financiero ya estaba en marcha antes de la pandemia de COVID-19.[4] La pandemia aceleró la demanda de servicios en la nube, ya que las instituciones financieras se vieron obligadas a alejarse del servicio al cliente en persona y a apoyar una fuerza laboral remota. La adopción de la nube permitió a las instituciones financieras escalar los servicios remotos en cuestión de días.[5]

Según una encuesta reciente de instituciones financieras globales, el 98 por ciento de los encuestados mantenía al menos algunos datos, aplicaciones u operaciones en la nube.[6] Banco Santander, uno de los bancos más grandes del mundo, planea migrar la mayoría de sus servicios bancarios centrales a la nube para finales de 2024.[7] El banco más grande de América Latina, Itau Unibanco, trasladará la mayoría de sus sistemas a la nube en un período de diez años. [8] Algunos bancos han ido aún más lejos: Capital One, uno de los bancos más grandes de los Estados Unidos, anunció en 2021 que había cerrado sus centros de datos privados y había trasladado todos sus servicios centrales a la nube.[9] Otras instituciones financieras, incluidas empresas de inversión, corredores de bolsa, asesores de inversión y compañías de seguros, también han migrado algunas

[2] Peter Mell y Tim Grance, *La Definición de Computación en la Nube del NIST*, INSTITUTO NACIONAL DE ESTÁNDARES Y TECNOLOGÍA (sep. 2011), https://csrc.nist.gov/pubs/sp/800/145/final.
[3] Lisa Valentine, *Perspectiva Nublada*, 104 ABA BANKING JOURNAL 22 (sep. 2012).
[4] Jerry Silva, *Apostando por la Nube: Resultados de la Encuesta CloudPath 2020*, IDC PERSPECTIVE 7-8 (nov. 2020).
[5] Daniel Pujazon y Brad Carr, *Computación en la Nube: Un Facilitador Vital en Tiempos de Disrupción*, INSTITUTE OF INTERNATIONAL FINANCE 4-5 (jun. 2020), https://www.iif.com/portals/0/Files/content/32370132_iif_cloud_computing_resilience.pdf.
[6] CLOUD SECURITY ALLIANCE, *ESTADO DE LOS SERVICIOS FINANCIEROS EN LA NUBE (2023)*. LOS ENCUESTADOS INCLUYERON BANCOS Y COOPERATIVAS DE CRÉDITO, FINTECHS Y OTRAS INSTITUCIONES FINANCIERAS EN LAS AMÉRICAS (52%), EMEA (28%) Y LA REGIÓN ASIA-PACÍFICO (20%).
[7] BANCO SANTANDER, *SANTANDER ALCANZA UN HITO CLAVE EN SU TRANSFORMACIÓN TRAS MIGRAR SU PLATAFORMA BANCARIA CIB A LA NUBE* (11 DE DICIEMBRE DE 2023), https://www.santander.com/en/press-room/press-releases/2023/12/santander-passes-key-milestone-in-its-transformation-after-migrating-its-cib-banking-platform-to-the-cloud.
[8] Samantha Lipana y Marissa Ramos, *Los 30 Bancos Más Grandes de América Latina por Activos, 2024, S&P GLOBAL MARKET INTELLIGENCE* (30 de abril de 2024), https://www.spglobal.com/marketintelligence/en/news-insights/research/latin-americas-30-largest-banks-by-assets-2024.
[9] Adrian Jimenea et al., *Los Bancos Más Grandes del Mundo por Activos, 2024, S&P GLOBAL MARKET INTELLIGENCE* (30 de abril de 2024), https://www.spglobal.com/marketintelligence/en/news-insights/research/the-worlds-largest-banks-by-assets-2024; Lananh Nguyen, *Banks Tiptoe Toward Their Cloud-Based Future*, NEW YORK TIMES (Jan. 3, 2022), https://www.nytimes.com/2022/01/03/business/wall-street-cloud-computing.html.

operaciones a la nube.[10] Y varias utilidades del mercado financiero, incluidas las cámaras de compensación y las bolsas, han realizado la transición a la nube en alguna capacidad.[11]

Aunque instituciones financieras como Banco Santander y Capital One han apostado por completo (o casi por completo) a la computación en la nube, la adopción en el sector financiero todavía está en sus primeras etapas. La misma encuesta de la industria que informó sobre la adopción del 98 por ciento en la nube también informó que casi la mitad de los encuestados mantiene menos del diez por ciento de sus cargas de trabajo críticas para el negocio en la nube. De manera similar, casi la mitad de los encuestados informa que menos del diez por ciento de sus cargas de trabajo reguladas han sido migradas a entornos de nube pública.[12] Las instituciones financieras han utilizado principalmente la nube para aplicaciones empresariales como recursos humanos y herramientas de colaboración. La mayoría de las operaciones centrales todavía se realizan en su mayoría utilizando sistemas de TI heredados.[13]

b. Los beneficios de la tecnología en la nube para las instituciones financieras y sus clientes

Aun así, se espera que la adopción de la nube en el sector financiero, incluidas las operaciones centrales, aumente en los próximos años. El modelo de la nube, que hace que los recursos informáticos estén disponibles bajo demanda y permite a los clientes pagar solo por los recursos que realmente utilizan, permite a las instituciones financieras convertir grandes gastos de TI iniciales en costos operativos continuos más pequeños.[14] Según algunas estimaciones, la adopción de la nube puede reducir los costos de TI entre un 20 y un 50 por ciento, lo que equivale a cientos de millones de dólares en ahorros a nivel económico.[15] Transformar grandes gastos de capital en costos operativos continuos también hace que las instituciones financieras sean más ágiles tecnológicamente: pueden probar nuevos escenarios, herramientas de software y configuraciones alternativas sin un largo proceso de compra y provisión. Menores costos y mayor agilidad tecnológica se traducen en mejores productos y servicios para los clientes, especialmente productos financieros digitales con características y datos robustos. La computación en la nube también balancea el acceso tecnológico entre instituciones financieras de diferentes tamaños, ofreciendo a las instituciones más pequeñas y a las startups fintech recursos de

[10] AMAZON WEB SERVICES, *VANGUARD AUMENTA EL VALOR PARA LOS INVERSORES USANDO AMAZON ECS Y AWS FARGATE* (2021), https://aws.amazon.com/solutions/case-studies/vanguard-ecs-fargate-case-study/.
[11] CME GROUP, *CME GROUP FIRMA UNA ASOCIACIÓN DE 10 AÑOS CON GOOGLE CLOUD PARA TRANSFORMAR LOS MERCADOS GLOBALES DE DERIVADOS A TRAVÉS DE LA ADOPCIÓN DE LA NUBE* (4 DE NOVIEMBRE DE 2021), https://www.cmegroup.com/media-room/press-releases/2021/11/04/cme_group_signs_10-yearpartnershipwithgooglecloudtotransformglob.html; NASDAQ, *NASDAQ Y AWS SE ASOCIAN PARA TRANSFORMAR LOS MERCADOS DE CAPITAL* (30 DE NOVIEMBRE DE 2021), https://www.nasdaq.com/press-release/nasdaq-and-aws-partner-to-transform-capital-markets-2021-12-01; NEW YORK STOCK EXCHANGE, *DATOS DEL MERCADO NYSE A TRAVÉS DE AMAZON WEB SERVICES (AWS),* https://www.nyse.com/nyse-cloud.
[12] CLOUD SECURITY ALLIANCE, *ESTADO DE LOS SERVICIOS FINANCIEROS EN LA NUBE (2023)*.
[13] Id.
[14] DEPOSITORY TRUST & CLEARING CORPORATION, *MOVIENDO LA INFRAESTRUCTURA DEL MERCADO FINANCIERO A LA NUBE*, 5-6 (MAYO DE 2017).
[15] Patrick Wauters, et al., *Midiendo el Impacto Económico de la Computación en la Nube en Europa*, DELOITTE (2016), https://ec.europa.eu/newsroom/dae/redirection/document/41184.

computación que previamente solo estaban al alcance de grandes instituciones con capacidad para dedicar importantes recursos a la infraestructura tecnológica.[16]

Al facilitar la innovación de bajo costo y aumentar la competencia, la migración a la nube ayuda a expandir el acceso y la inclusión financiera, particularmente para clientes en mercados en desarrollo o desatendidos.[17] A nivel global, la proporción de adultos con una cuenta en una institución financiera o servicio de dinero móvil aumentó del 51 al 76 por ciento en la década comprendida entre 2011 y 2021.[18] Las plataformas financieras basadas en la nube han desempeñado un papel fundamental en llegar a empresas e individuos anteriormente desatendidos. En China, por ejemplo, el enfoque nativo en la nube de WeBank ha permitido que su plataforma de préstamos llegue a millones de individuos y empresas con poca o ninguna historia crediticia.[19] Nubank, un banco brasileño solo móvil, utiliza infraestructura basada en la nube para ofrecer tarjetas de crédito y préstamos personales a clientes que no podían obtener préstamos de bancos tradicionales debido a su falta de historial crediticio.[20] En el sudeste asiático, aplicaciones de transporte como Grab y Go-Jek (ahora GoTo) han aprovechado la infraestructura en la nube para proporcionar pagos y otros servicios financieros a usuarios minoristas.[21] Mercado Libre, el proveedor de comercio en línea y pagos más grande de América Latina, ofrece servicios de pago y crédito basados en la nube a clientes que de otro modo no tendrían acceso a ellos.[22]

La computación en la nube también puede ser más segura y resiliente que la infraestructura tradicional. A diferencia de todas menos las instituciones financieras más grandes, los principales proveedores de la nube están a la vanguardia de la investigación y la implementación de seguridad.[23] Las plataformas de los principales proveedores de la nube también están diseñadas para ofrecer a los clientes herramientas para implementar requisitos de seguridad estrictos, como monitoreo y registro de todas las actividades y cifrado de datos incorporado.[24] La escalabilidad de los servicios en la nube permite a las instituciones financieras manejar requisitos de capacidad inesperados, ya sea debido a un aumento imprevisto en la actividad del mercado o un ciberataque malicioso, que podrían abrumar la infraestructura de TI de una institución financiera.[25] Además, dado que la infraestructura en la nube está más distribuida geográficamente a través de centros de

[16] Wang Jin y Kristina McElheran, *Economías antes de la Escala: Estrategia IT y Dinámicas de Rendimiento de los Nuevos Negocios en EE. UU.*, ROTMAN SCHOOL OF MANAGEMENT WORKING PAPER NO. 3112901 (2018), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3112901. Los proveedores de la nube pueden permitir el cumplimiento del Estándar de Seguridad de Datos del Sector de Tarjetas de Pago (PCI DSS) al ofrecer un entorno seguro para almacenar, procesar y transmitir información de tarjetas de crédito. Ver en general, CLOUD SPECIAL INTEREST GROUP AND PAYMENT CARD INDUSTRY SECURITY STANDARDS COUNCIL, *PCI SSC Cloud Computing Guidelines (Abril, 2018)*, https://www.pcisecuritystandards.org/pdfs/PCI_SSC_Cloud_Guidelines_v3.pdf.

[17] BANCO MUNDIAL Y FONDO MONETARIO INTERNACIONAL, AGENDA FINTECH DE BALI (2018); MAX CHUARD, *LA TECNOLOGÍA EN LA NUBE Y SAAS PUEDE IMPULSAR LA BANCA INCLUSIVA. AQUÍ ESTÁN 3 RAZONES DE CÓMO*, *FORO ECONÓMICO MUNDIAL* (10 DE DICIEMBRE DE 2020), https://www.weforum.org/agenda/2020/12/cloud-and-saas-technology-can-drive-inclusive-banking/.

[18] BANCO MUNDIAL, *LA BASE DE DATOS GLOBAL FINDEX: MIDIENDO LA INCLUSIÓN FINANCIERA Y LA REVOLUCIÓN FINTECH* (2024), https://www.worldbank.org/en/publication/globalfindex.

[19] Sally Chen et al., *Banca Virtual y Más Allá*, 120 BIS PAPERS (Enero 2022), https://www.bis.org/publ/bppdf/bispap120.pdf.

[20] Debopriyo Bhattacharyya et al., *Global Banking Annual Review 2023*: La Gran Transición Bancaria, MCKINSEY & COMPANY (10 de octubre de 2023), https://www.mckinsey.com/industries/financial-services/our-insights/global-banking-annual-review.

[21] GRAB, *GRAB FORJA UNA ASOCIACIÓN ESTRATÉGICA EN LA NUBE CON MICROSOFT PARA IMPULSAR LA INNOVACIÓN Y LA ADOPCIÓN DE SERVICIOS DIGITALES EN EL SUDESTE ASIÁTICO* (9 DE OCTUBRE DE 2018), https://www.grab.com/sg/press/business/grab-forges-strategic-cloud-partnership-with-microsoft-to-drive-innovation-and-adoption-of-digital-services-across-southeast-asia/; Leon Spencer, *El Grupo GoTo de Indonesia Opta por Google Cloud para la Próxima Fase de su Expansión en Asia*, CHANNEL ASIA (27 de julio de 2021), https://www.channelasia.tech/article/1269704/indonesias-goto-group-goes-with-google-cloud-for-next-phase-of-asian-attack-2.html.

[22] Frost et al., BigTech y la Estructura Cambiante de la Intermediación Financiera, 34(100) ECONOMIC POLICY 761-799 (2019).

[23] Los principales proveedores de la nube, por ejemplo, detectaron y mitigaron rápidamente vulnerabilidades significativas a nivel de chip que habían sido descubiertas por uno de los proveedores. Jordan Novet, *Amazon, Microsoft y Google Responden a la Vulnerabilidad del Chip de Intel*, CNBC (3 de enero de 2018), https://www.cnbc.com/2018/01/03/microsoft-google-respond-to-intel-chip-vulnerability.html.

[24] DEPOSITORY TRUST & CLEARING CORPORATION, *MOVER LA INFRAESTRUCTURA DEL MERCADO FINANCIERO A LA NUBE* (MAYO DE 2017).

[25] AMAZON WEB SERVICES, *MEJORES PRÁCTICAS DE AWS PARA LA RESILIENCIA ANTE DDOS*, 6-15 (2021), https://d1.awsstatic.com/whitepapers/Security/DDoS_White_Paper.pdf.

datos y regiones que la infraestructura de TI tradicional, la adopción de la nube facilita una mayor resiliencia en caso de una interrupción local.[26]

Los extensos recursos informáticos y la escalabilidad automática de la nube también la hacen especialmente adecuada para transformar la forma en que las instituciones financieras manejan los datos. Los entornos basados en la nube permiten a las instituciones financieras ingerir datos a velocidades mucho mayores que las disponibles con la infraestructura de TI tradicional. También facilitan un análisis y manipulación de datos sin precedentes una vez que se ingieren.[27] Ese nivel sofisticado de análisis de datos puede ayudar a las instituciones financieras a obtener ventajas competitivas, mejorar su gestión de riesgos y mejorar funciones existentes como la detección de fraude y lavado de dinero. Los avances recientes en el entrenamiento y despliegue de grandes modelos de lenguaje y otras herramientas de aprendizaje automático e inteligencia artificial serían imposibles sin los recursos informáticos masivos disponibles en los entornos de la nube.[28] Cualquier institución financiera que busque aprovechar el aprendizaje automático o la inteligencia artificial en el futuro necesitará confiar en la infraestructura en la nube.

c. La importancia de los flujos de datos transfronterizos en el sector de servicios financieros globales

En el sector financiero, los datos son un activo esencial que facilita la toma de decisiones financieras informadas. En un mercado de servicios financieros cada vez más globalizado, el flujo seguro de datos a través de las fronteras es crítico para que las instituciones financieras tengan éxito. Por ejemplo, una institución financiera que opera sucursales o afiliadas en múltiples jurisdicciones podría querer compartir información sobre sus clientes en una jurisdicción con una afiliada en otra jurisdicción para servir a un cliente que se ha trasladado de una jurisdicción a otra.[29] Las instituciones financieras se benefician del análisis de mercado o las actividades de diligencia debida en las que la transferencia de datos a través de fronteras es de importancia material.[30] Además, las instituciones financieras pueden depender de la transferencia internacional de datos de crédito de consumidores o empresas para determinaciones de solvencia crediticia.[31]

---

[26] DEPOSITORY TRUST & CLEARING CORPORATION, *Mover la Infraestructura del Mercado Financiero a la Nube* (mayo de 2017). Ver también Glen Robinson et al., Uso de Amazon Web Services para la Recuperación ante Desastres, AMAZON WEB SERVICES (octubre de 2014), https://d1.awsstatic.com/whitepapers/aws-disaster-recovery.121b65092f931567af5370b47dd12cb18866089c.pdf.

[27] Davies, *Nuevas Herramientas Ofrecen una Mejor Imagen, Literalmente, del Riesgo del Sistema Financiero*, WALL STREET JOURNAL (2017), https://www.wsj.com/articles/new-tools-give-better-picture-literally-of-financial-system-risk1493086260?mod=article_inline; John Ashley y Jochen Papenbrock, *Plataformas de Computación Moderna como Tecnología Clave para Bancos Centrales, Supervisores Financieros y Reguladores*, IRVING FISHER COMMITTEE ON CENTRAL BANK STATISTICS (2022), https://www.bis.org/ifc/publ/ifcb59_04.pdf; Joshua P. Meltzer y Peter Lovelock, *Regulando para una Economía Digital: Comprendiendo la Importancia de los Flujos de Datos Transfronterizos en Asia*, GLOBAL ECONOMY AND DEVELOPMENT (marzo de 2018).

[28] Id.

[29] Peter P. Swire y Robert E. Litan, *Ningún Asunto Tuyo: Flujos de Datos Mundiales, Comercio Electrónico y la Directiva Europea de Privacidad*, BROOKINGS INSTITUTION PRESS (1998).

[30] Id.

[31] Id.

En esencia, las transacciones vitales para el sistema financiero internacional, incluyendo los sistemas de pago transfronterizos, dependen del flujo de datos a nivel mundial.[32] Con el aumento de la movilidad internacional de bienes, servicios, capital y personas, la importancia de las transacciones transfronterizas ha crecido tanto en volumen como en valor.[33] En 2022, los pagos transfronterizos anuales llegaron a unos 150 billones de dólares.[34] Y durante 2023, las reclamaciones financieras transfronterizas pendientes aumentaron en más de 2 billones de dólares.[35]

La llegada y adopción generalizada de la tecnología en la nube ha creado nuevas oportunidades para que las instituciones financieras se beneficien de los flujos de datos transfronterizos. Aunque la infraestructura de los principales proveedores de nube está ampliamente distribuida a través de regiones geográficas, no mantienen centros de datos en todas las jurisdicciones.[36] Para explotar los beneficios de la tecnología en la nube, las instituciones financieras pueden necesitar transferir datos a otra jurisdicción. Por ejemplo, los recientes avances de gran relevancia en los campos del análisis de datos y la IA tienen un gran potencial para el sector financiero. Los bancos multinacionales recopilan información detallada sobre cómo se comportan sus clientes y utilizan análisis de grandes datos o IA para desarrollar servicios personalizados, como alertas personalizadas y una mejor detección de fraudes.[37] Estos campos dependen del procesamiento de volúmenes masivos de datos para el entrenamiento y la producción de conocimientos útiles, lo cual requiere acceso a recursos informáticos que solo están disponibles en los mayores proveedores de nube, y que pueden no estar ubicados en la jurisdicción de origen de una institución financiera.[38]

Las restricciones a las transferencias de datos transfronterizas, que han aumentado significativamente en los últimos años, dificultan la capacidad de las instituciones financieras para competir en el mercado global de servicios financieros y aprovecharlo. Los requisitos de localización de datos limitan su capacidad para servir mejor a sus clientes. Y si limitan sus oportunidades de aprovechar la tecnología en la nube, esos requisitos impiden su acceso a tecnologías —como el análisis de datos y la IA— que prometen transformar el sector financiero. Por lo tanto, es crítico que los reguladores, incluyendo a los

[32] Id.; BANCO DE INGLANDERA, *Pagos Transfronterizos* (31 de enero de 2023), https://www.bankofengland.co.uk/payment-and-settlement/cross-border-payments.
[33] BANCO DE INGLANDERA, *Trabajando juntos para mejorar los pagos transfronterizos - discurso de Victoria Cleland* (22 de noviembre de 2021), https://www.bankofengland.co.uk/speech/2021/november/victoria-cleland-keynote-presentation-the-cbpc-international-payments-on-the-move.
[34] Luca Bionducci et al., *En el umbral de la próxima era de pagos: Oportunidades futuras para los bancos*, MCKINSEY & COMPANY (18 de septiembre de 2023), https://www.mckinsey.com/industries/financial-services/our-insights/the-2023-mckinsey-global-payments-report#/.
[35] BANCO DE PAGOS INTERNACIONALES, *Estadísticas bancarias por ubicación, BIS WS_LBS_D_PUB 1.0* (conjunto de datos) (2024), https://data.bis.org/topics/LBS/BIS%2CWS_LBS_D_PUB%2C1.0/Q.S.C.A.TO1.A.5J.A.5A.A.5J.N?view=observations.
[36] Daniel Castro y Alan McQuinn, *Los Flujos de Datos Transfronterizos Facilitan el Crecimiento en Todas las Industrias*, FUNDACIÓN DE TECNOLOGÍA E INNOVACIÓN (febrero de 2015), https://www2.itif.org/2015-cross-border-data-flows.pdf.
[37] Id.
[38] John Ashley y Jochen Papenbrock, *Plataformas de Computación Moderna como Tecnología Clave para Bancos Centrales, Supervisores Financieros y Reguladores*, IRVING FISHER COMMITTEE ON CENTRAL BANK STATISTICS (2022), https://www.bis.org/ifc/publ/ifcb59_04.pdf; Joshua P. Meltzer y Peter Lovelock, *Regulando para una Economía Digital: Comprendiendo la Importancia de los Flujos de Datos Transfronterizos en Asia*, GLOBAL ECONOMY AND DEVELOPMENT (marzo de 2018).

reguladores financieros, sopesen las justificaciones para las restricciones sobre la transferencia transfronteriza de datos financieros frente a sus significativos costos.

PARTE II: COMPRENSIÓN DE LOS REQUISITOS DE LOCALIZACIÓN DE DATOS

Desde que las empresas utilizan la tecnología para transferir datos a través de las fronteras, los reguladores han impuesto reglas sobre cómo pueden hacerlo. A medida que el flujo internacional de datos ha aumentado, también han aumentado los esfuerzos para regularlo. Las restricciones sobre la transferencia de datos fuera de la jurisdicción de origen toman diferentes formas, desde reglas que requieren que los datos se ubiquen físicamente donde se originan hasta requisitos de almacenamiento local "de facto" que imponen condiciones estrictas para transferir datos fuera de la jurisdicción. Los reguladores han citado varios motivos para imponer requisitos de localización de datos, incluyendo privacidad, desarrollo económico, aplicación regulatoria y preocupaciones geopolíticas. Sin embargo, los requisitos de localización de datos tienen significativas desventajas conceptuales y prácticas, lo que subraya la importancia de lograr estos objetivos de otras maneras.

a. Diferentes tipos de requisitos de localización de datos

Los requisitos de localización de datos preceden a la nube. Las primeras leyes nacionales de protección de datos, introducidas a fines de la década de 1970 y principios de la de 1980, requerían la localización de las operaciones de procesamiento de datos o la autorización previa para la exportación de datos sensibles.[39] Sin embargo, en la última década, a medida que tecnologías como la computación en la nube han transformado la forma en que se almacenan, procesan y comparten los datos, las restricciones sobre la transferencia transfronteriza de datos se han multiplicado.[40] Según un estudio, el número de países que imponen restricciones al flujo transfronterizo de datos casi se duplicó entre 2017 y 2021.[41]

Estas restricciones varían según el país tanto en términos de su alcance como en la forma en que limitan las transferencias transfronterizas de datos. Algunas restricciones se aplican a cualquier dato generado dentro de un país; otras se aplican solo a ciertas categorías de datos, como datos financieros, o a sectores económicos o entidades específicas. En algunas jurisdicciones, por ejemplo, los reguladores financieros han impuesto requisitos de localización de datos a las instituciones financieras en ausencia de restricciones generales sobre la transferencia de datos en esas jurisdicciones.[42]

En cuanto al contenido, los requisitos de localización de datos se pueden dividir en tres categorías amplias: (1) reglas explícitas de almacenamiento o procesamiento local de

[39] Christopher J. Millard, Protección Legal de los Programas Informáticos y los Datos, 14(1-2) INTERNATIONAL JOURNAL OF LEGAL INFORMATION 74-75 (1985).
[40] CENTRO EUROPEO DE ECONOMÍA POLÍTICA INTERNACIONAL, *RESTRICCIONES EN LOS FLUJOS DE DATOS TRANSFRONTERIZOS: UNA TAXONOMÍA* (2017); FUNDACIÓN DE TECNOLOGÍA E INNOVACIÓN (2021).
[41] Id.
[42] Javier López González, Francesca Casalini y Juan Porras, *Un Mapeo Preliminar de las Medidas de Localización de Datos*, ORGANIZACIÓN PARA LA COOPERACIÓN Y EL DESARROLLO ECONÓMICO, DOCUMENTOS DE POLÍTICA COMERCIAL, NO. 262 (2022), https://www.oecd-ilibrary.org/trade/a-preliminary-mapping-of-data-localisation-measures_c5ca3fed-en.

datos, que mandatan que los datos originados en un país se almacenen o procesen en esa jurisdicción; (2) reglas de "espejo de datos", que permiten la transferencia de datos al extranjero siempre que una copia de esos datos se almacene localmente; y (3) reglas que imponen restricciones condicionales a la transferencia de datos al extranjero. Dependiendo de la rigurosidad de esas condiciones, cuando el costo de cumplimiento es prohibitivo, equivalen a requisitos de almacenamiento local de facto.

Las reglas de almacenamiento o procesamiento local de datos son la forma más estricta de requisito de localización de datos. La República Popular China, por ejemplo, requiere que los "operadores de infraestructura de información crítica" deben almacenar localmente en China continental la información personal y otros "datos importantes" que se recopilan y generan en China (aunque los datos pueden transferirse al extranjero bajo ciertas circunstancias). [43] Las restricciones más estrictas se aplican a los datos financieros: el Banco Popular de China manda que prácticamente todos los datos personales recopilados como parte de la provisión de servicios financieros se almacenen, procesen y analicen en China continental.[44] Turquía requiere que una amplia variedad de empresas y organizaciones, incluyendo empresas que cotizan en bolsa, fondos de pensiones, bancos y reguladores e infraestructuras del mercado financiero, ubiquen sus sistemas informáticos en vivo y de respaldo dentro del país.[45] Otras jurisdicciones imponen requisitos de localización de datos a tipos específicos de entidades o infraestructura: Venezuela, por ejemplo, requiere que la infraestructura tecnológica para el procesamiento de pagos se ubique en el país.[46] Y el Banco Central de Nigeria requiere que las transacciones de pago domésticas, incluidas las transacciones en puntos de venta y cajeros automáticos, se enruten localmente para su conmutación entre emisores y adquirentes nigerianos.[47]

Los requisitos de "espejo de datos" son menos restrictivos que las reglas de almacenamiento local, ya que solo mandan que una copia de los datos se mantenga en servidores o centros de datos locales para asegurar la resiliencia operativa en caso de una interrupción. Esto significa que los datos pueden transferirse y procesarse en el extranjero, siempre que se mantenga una copia de los datos localmente. Sin embargo, el requisito de que se mantenga una copia redundante de los datos localmente eleva el costo relativo de almacenar datos en el extranjero, y por lo tanto, en la práctica, puede tener el mismo efecto que las reglas de almacenamiento local.[48] México requiere que ciertas instituciones financieras, como bancos y empresas fintech, que almacenan datos en centros de datos ubicados fuera de México mantengan copias de los registros contables y

[43] Ley de Ciberseguridad, Artículo 37; Ley de Protección de Información Personal.
[44] Artículo 6, Aviso No. 17 (2011).
[45] JUNTA DE MERCADOS DE CAPITALES, *Comunicado sobre la Gestión de los Sistemas de Información*, VII-128.9 (2018) (EMPRESAS QUE COTIZAN EN BOLSA Y REGULADORES E INFRAESTRUCTURAS DE MERCADOS FINANCIEROS); AUTORIDAD REGULADORA Y SUPERVISORA BANCARIA, *Reglamento sobre los Sistemas de Información y Servicios Bancarios Electrónicos de los Bancos* (2020) (BANCOS).
[46] Nigel Cory y Luke Dascoli, *Cómo las Barreras a los Flujos de Datos Transfronterizos se Están Expandiendo a Nivel Global, Sus Costos y Cómo Abordarlos*, FUNDACIÓN PARA LA TECNOLOGÍA DE LA INFORMACIÓN Y LA INNOVACIÓN (jul. 2021).
[47] BANCO CENTRAL DE NIGERIA, *Directrices sobre Servicios de Aceptación de Tarjetas en Puntos de Venta* 4.4.8.
[48] Id.

transaccionales localmente para asegurar la continuidad operativa.[49] De igual manera, Chile manda que los bancos que subcontratan cargas de trabajo críticas en el extranjero, incluyendo a través del uso de servicios en la nube, mantengan un centro de procesamiento de datos local para propósitos de contingencia.[50]

Otras jurisdicciones imponen restricciones condicionales a las transferencias internacionales de datos. Estas restricciones condicionales adoptan una variedad de formas diferentes. Algunos países mandan que los datos solo se transfieran a otra jurisdicción que tenga en vigor reglas de protección de datos equivalentes o que la protección de datos esté garantizada por contrato. Por ejemplo, la ley de protección de datos de Brasil solo permite transferencias internacionales de datos personales donde el país receptor proporciona un nivel "adecuado" de protección de datos o donde se establecen ciertas disposiciones contractuales.[51] Otras jurisdicciones requieren que las empresas obtengan el consentimiento de los reguladores o clientes antes de transferir datos al extranjero. Arabia Saudita, por ejemplo, requiere que los datos personales se almacenen y procesen localmente a menos que se obtenga una aprobación por escrito de la autoridad reguladora correspondiente.[52] Los reguladores de bancos y mercados de capitales de Panamá, por ejemplo, requieren que las entidades reguladas obtengan una aprobación previa para el uso de servicios en la nube extranjeros proporcionados por un tercero.[53] Las instituciones financieras mexicanas están sujetas a requisitos similares.[54]

b. Razones para los requisitos de localización de datos

Existen diversas motivaciones para las políticas de localización de datos. Una preocupación comúnmente mencionada es que los datos transferidos al extranjero, especialmente los datos personales sensibles como los financieros, no estén adecuadamente protegidos contra posibles brechas de seguridad o el acceso de gobiernos extranjeros.[55] Alternativamente, los reguladores temen que los datos almacenados en el extranjero no estén disponibles en caso de una interrupción.[56] Según el argumento, el almacenamiento local de datos es necesario para protegerlos contra intrusiones no deseadas e interrupciones imprevistas.

Además de las supuestas preocupaciones de privacidad y disponibilidad, los países vinculan los requisitos de localización de datos con el amplio concepto de "soberanía digital". En el contexto europeo, la soberanía digital se ha definido como la "capacidad de

[49] Instituciones de fondos de pago electrónico (Fintechs), Artículo 49, IV; Bancos (Anexo 52(I)(e)); Casas de bolsa, Anexo 12(I)(e). Además, las instituciones financieras mexicanas que utilizan servicios en la nube solo pueden conectarse al Sistema de Pagos Electrónicos Interbancarios (SPEI) utilizando centros de datos locales.
[50] Circular Bancaria 2409/Financiera 798 Capítulo 20-7. Los bancos solo pueden subcontratar servicios de procesamiento de datos a jurisdicciones que tengan una calificación de riesgo país de grado de inversión y una protección legal adecuada para la seguridad de los datos personales.
[51] Ley de Protección General de Datos, Capítulo V – Transferencia Internacional de Datos. Véase también el borrador del reglamento de protección de datos de Perú.
[52] Reglamento Provisional de Gobernanza de Datos Nacionales, Sección 5.4 (2020).
[53] Acuerdo No. 003-2012; Acuerdo No. 005-2018.
[54] Ver, por ejemplo, Instituciones de fondos de pago electrónico (Fintechs), Artículo 49, VIII.
[55] Christopher Millard, *Localización Forzada de Servicios en la Nube: ¿Es la Privacidad el Motor Real?*, NUBE Y LA LEY (2015).
[56] Id.

actuar de manera independiente en el mundo digital", en relación tanto con "mecanismos de protección como con herramientas ofensivas para fomentar la innovación digital"[57]

En consecuencia, algunos países han justificado los requisitos de localización de datos con el argumento de que el acceso directo a las empresas puede facilitar la aplicación de leyes, como los estatutos fiscales y contra el lavado de dinero.[58] Cuando los datos están ubicados en el extranjero, las autoridades legales temen que su capacidad para acceder a los datos pueda verse obstaculizada. Este argumento es particularmente relevante para sectores, como el de servicios financieros, que están sujetos a requisitos de divulgación y mantienen datos que son altamente solicitados por las autoridades de aplicación de la ley. El almacenamiento local de datos podría facilitar la vigilancia y otras divulgaciones involuntarias de información por parte de entidades reguladas. Sin embargo, esta justificación podría socavar la razón de privacidad para la localización de datos.[59]

Los países también introducen requisitos de localización de datos con el objetivo de incentivar la inversión en sus sectores locales de tecnología de la información, otro objetivo vinculado a la noción de soberanía digital. Si las empresas están obligadas a almacenar y procesar datos localmente, se verán forzadas a invertir en servidores y centros de datos locales. Esa inversión, en teoría, podría crear beneficios indirectos para el sector local de alta tecnología.[60] Más allá de los beneficios económicos de la inversión nacional en infraestructura tecnológica como los centros de datos, algunos gobiernos ven los centros de procesamiento de datos locales como infraestructura crítica necesaria para su seguridad y soberanía nacionales.[61] Además, la interrupción de ciertos servicios críticos, como los servicios financieros, podría perjudicar gravemente el funcionamiento básico del país, lo que justifica requisitos especiales para garantizar la resiliencia y disponibilidad de esos servicios.[62]

c. Costos de la localización de datos en general

Aunque estos objetivos de política son legítimos (si bien potencialmente contradictorios), el uso de requisitos de localización de datos para lograrlos probablemente sea ineficaz. La ubicación física de los datos puede ser un factor en su privacidad, pero no es el más importante. Desde una perspectiva técnica, el acceso físico a un servidor u otro dispositivo de almacenamiento de datos no es ni necesario ni suficiente para acceder a la información almacenada en él. Los datos que no se gestionan de forma segura pueden ser

---

[57] SERVICIO DE INVESTIGACIÓN DEL PARLAMENTO EUROPEO, *SOBERANÍA DIGITAL PARA EUROPA* (JUL., 2020),, https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651992/EPRS_BRI(2020)651992_EN.pdf.

[58] INSTITUTO DE FINANZAS INTERNACIONALES, *FLUJOS DE DATOS A TRAVÉS DE FRONTERAS: SUPERANDO LAS RESTRICCIONES DE LOCALIZACIÓN DE DATOS* (MAR. 2019).

[59] Christopher Millard, *Localización Forzada de Servicios en la Nube: ¿Es la Privacidad el Motor Real?*, NUBE Y LA LEY (2015).

[60] INSTITUTO DE FINANZAS INTERNACIONALES, *FLUJOS DE DATOS A TRAVÉS DE FRONTERAS: SUPERANDO LAS RESTRICCIONES DE LOCALIZACIÓN DE DATOS* (MAR. 2019).

[61] CENTRO DE ESTUDIOS ESTRATÉGICOS E INTERNACIONALES, *LAS VERDADERAS PREOCUPACIONES DE SEGURIDAD NACIONAL SOBRE LA LOCALIZACIÓN DE DATOS* (2021); ASOCIACIÓN DE MERCADOS FINANCIEROS EN EUROPA, *ESQUEMA DE CERTIFICACIÓN DE CIBERSEGURIDAD EUROPEO PARA SERVICIOS EN LA NUBE (EUCS) – SOLUCIONES SOBRE EL PROBLEMA DE LA INDEPENDENCIA A LA LEY NO-UE* (13 DE MARZO DE 2023), https://www.afme.eu/Portals/0/DispatchFeaturedImages/230310_AFME%20Comments%20on%20EUCS_FINAL.pdf; ORGANIZACIÓN INTERNACIONAL DE COMISIONES DE VALORES, *MEMORANDO MULTILATERAL DE ENTENDIMIENTO SOBRE CONSULTA Y COOPERACIÓN Y EL INTERCAMBIO DE INFORMACIÓN* (MAYO 2012), https://www.iosco.org/library/pubdocs/pdf/IOSCOPD386.pdf.

[62] Id.

accedidos incluso si un usuario no tiene acceso físico a un servidor. Y si los datos están cifrados de manera segura, el acceso físico por sí solo no los hará accesibles en una forma inteligible. Además, si los datos están cifrados de manera segura, el acceso físico a los datos no dará lugar a riesgos de privacidad independientemente de dónde se almacenen físicamente.[63]

El almacenamiento local de datos no necesariamente mejora la seguridad o disponibilidad de los datos. El almacenamiento de datos utilizando la infraestructura extranjera de un importante proveedor de servicios en la nube puede ofrecer una mejor seguridad y disponibilidad. Las economías de escala permiten a los principales proveedores de servicios en la nube realizar inversiones en capacidades de resiliencia y ciberseguridad que superan con creces las disponibles solo con la infraestructura tecnológica local.[64] Además, los principales proveedores de servicios en la nube garantizan la seguridad y disponibilidad de los datos distribuyéndolos y procesándolos entre múltiples sistemas y ubicaciones, haciéndolos menos vulnerables a una brecha o interrupción.[65] Al exigir que los datos permanezcan en una jurisdicción en particular, los requisitos de localización inhiben el uso de esa infraestructura distribuida. Además, al aumentar el número y las ubicaciones de centros de datos que deben ser atendidos y mantenidos por empresas que operan en diferentes jurisdicciones, los requisitos de localización de datos también añaden riesgo y complejidad a sus operaciones de ciberseguridad. Requerir que cualquier empresa multinacional cree y defienda múltiples versiones de sus sistemas en diferentes lugares significa más hardware, más empleados y más proveedores, aumentando la superficie para posibles interrupciones o ciberataques.[66]

Exigir el almacenamiento local de datos tampoco elimina el riesgo de acceso de gobiernos extranjeros. La ley estadounidense, por ejemplo, establece que los proveedores de servicios en la nube sujetos a la jurisdicción de EE. UU. no pueden evitar cumplir con una solicitud de acceso de las autoridades de aplicación de la ley simplemente porque los datos están ubicados en una jurisdicción no estadounidense.[67] Tampoco garantiza el almacenamiento local de datos la supervisión regulatoria local o el acceso para la aplicación de la ley local. Los proveedores de servicios en la nube con sede en EE. UU., por ejemplo, generalmente tienen prohibido compartir datos con gobiernos extranjeros, independientemente de dónde se encuentren los datos. Desde la perspectiva de la ley estadounidense, no importa si los datos se almacenan en un centro de datos estadounidense o en uno ubicado en otro país. La mejor manera para que los reguladores y las autoridades de aplicación de la ley garanticen el acceso a los datos no es la localización, sino a través de acuerdos bilaterales o multilaterales de intercambio de datos. Algunas jurisdicciones han trabajado con gobiernos extranjeros para facilitar el acceso a los datos de sus propios ciudadanos almacenados en el extranjero. Varios países, por ejemplo, han firmado acuerdos bilaterales con los Estados Unidos para que los proveedores de servicios en la nube de EE. UU. puedan cumplir con las solicitudes legales de datos electrónicos

[63] Christopher Millard, *Ley de Computación en la Nube*, OXFORD UNIVERSITY PRESS (2013).
[64] Véase arriba, Parte I.b.
[65] Id.
[66] Anupam Chander, *¿Es la Localización de Datos una Solución para Schrems II?*, 23 REVISTA DE DERECHO ECONÓMICO INTERNACIONAL 771-784 (2020), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3662626; BLANCCO, El Alto Costo de los Centros de Datos Saturados (2019).
[67] Ley CLOUD.

emitidas por el otro país sin una orden directamente al proveedor de servicios en la nube.[68]

Aunque la localización de datos puede ofrecer algunos beneficios económicos directos, esos beneficios son limitados. Aunque la localización de datos puede atraer inversión en infraestructura tecnológica nacional, como los centros de datos, los beneficios indirectos son mínimos porque los centros de datos son altamente automatizados y tienen relativamente pocos empleados permanentes.[69] Más fundamentalmente, la competencia por la ubicación de la infraestructura de los principales proveedores de servicios en la nube es un juego de suma cero: no es económicamente viable que los proveedores de servicios en la nube construyan centros de datos, que cuestan cientos de millones de dólares o más,[70] en *cada jurisdicción*. Los principales proveedores de servicios en la nube pueden optar por no construir infraestructura local. En ese caso, los requisitos de localización de datos perjudicarán la economía local, al desconectar a las empresas nacionales de los beneficios que ofrece la infraestructura tecnológica de clase mundial de los principales proveedores de servicios en la nube. Esto se traduce en mayores costos tecnológicos: según un estudio, los requisitos de localización de datos pueden aumentar los costos de alojamiento de datos entre un 30% y un 60%.[71] Los costos aumentados significan una reducción en la capacidad de las empresas locales para competir a nivel global y menos innovación para los clientes locales. También, el endurecimiento de las normas de transferencia de datos en un país se ha relacionado con una considerable disminución en la productividad y un alza en los precios de las industrias afectadas.[72]

Algunas jurisdicciones han reconocido que la confidencialidad, integridad y disponibilidad de los datos se pueden lograr mejor mediante el uso de servidores en la nube ubicados en el extranjero.[73] Estonia, por ejemplo, ha establecido una "embajada de datos" virtual utilizando servicios en la nube extranjeros para garantizar la continuidad de los datos que se consideran críticos para el funcionamiento del estado. Otros gobiernos han revisado los requisitos de localización de datos existentes a la luz de los costos asociados con ellos. Indonesia, por ejemplo, redujo sus estrictos requisitos de localización de datos, que

---

[68] Id.

[69] Nigel Cory, *El Falso Encanto del Nacionalismo de Datos: Por Qué el Valor de los Datos Proviene de Cómo se Usan, No de Dónde se Almacenan*, FUNDACIÓN PARA LA TECNOLOGÍA DE LA INFORMACIÓN E INNOVACIÓN (abr. 2019).

[70] Matt Vincent, *Los Mega Acuerdos de los Gigantes de la Nube Hiperescala en Centros de Datos Siguen Multiplicándose,* DATA CENTER FRONTIER (1 de abr. 2024), https://www.datacenterfrontier.com/hyperscale/article/55001427/hyperscale-cloud-giants-data-center-mega-deals-keep-sprouting-zeroes; AMAZON WEB SERVICES, AWS LANZARÁ UNA REGIÓN DE INFRAESTRUCTURA EN MÉXICO (26 DE FEB. 2024), https://press.aboutamazon.com/2024/2/aws-to-launch-an-infrastructure-region-in-mexico.

[71] LEVIATHAN SECURITY GROUP, *CUANTIFICANDO EL COSTO DE LA LOCALIZACIÓN FORZADA* (2015), https://static1.squarespace.com/static/6128b1eb2eb2cf15b7a35a2f/t/65af6b484ec970386fd56386/1705995081389/Quantifying%2Bthe%2BCost%2Bof%2BForced%2BLocalization.pdf.

[72] FUNDACIÓN PARA LA TECNOLOGÍA DE LA INFORMACIÓN E INNOVACIÓN (2021); CENTRO EUROPEO DE ECONOMÍA POLÍTICA INTERNACIONAL (2014); MARTINA F. FERRACANE, *LOS COSTOS DEL PROTECCIONISMO DE DATOS, BIG DATA Y LEY COMERCIAL GLOBAL* (9 DE JUL. 2021). LA ADOPCIÓN DE LA NUBE TAMBIÉN SE HA VINCULADO A LA REDUCCIÓN DE EMISIONES, YA QUE LA ACTIVIDAD DE LOS CENTROS DE DATOS SE TRASLADA DE SERVIDORES LOCALES MENOS EFICIENTES A SERVIDORES PÚBLICOS EN LA NUBE MÁS EFICIENTES Y NUEVOS. FTI CONSULTING, *IMPACTO ECONÓMICO DE LA ADOPCIÓN DE LA NUBE EN SEIS PAÍSES DE AMÉRICA LATINA* (20 DE OCT. 2023), https://fticommunications.com/economic-impact-of-cloud-adoption-in-six-latin-american-countries/?utm_source=web_linkedin&utm_medium=aws_social&utm_campaign=latam_awr_cloud_adoption_economic_impact_10-25-2023&utm_content=aws-cloud-adoption-economic-impact-report.

[73] E-ESTONIA, *E-GOBERNANZA*, https://e-estonia.com/solutions/e-governance/data-embassy/.

anteriormente se aplicaban a cualquier proveedor de "servicios públicos" electrónicos, para aplicarse solo a entidades gubernamentales.[74] Y Ucrania levantó los requisitos de localización de datos para transferir datos críticos del gobierno y del sector privado, incluidos los datos de su banco privado más grande, a servidores en la nube seguros en el extranjero antes de la invasión rusa.[75]

Parte III: Requisitos De Localización De Datos Y El Sector Financiero

La proliferación de requisitos de localización de datos, que impiden el flujo de datos a través de fronteras, plantea problemas particulares para los servicios financieros. La transferencia transfronteriza de datos dentro de entidades multinacionales y entre entidades en diferentes jurisdicciones es fundamental para el funcionamiento del sector financiero global. Las instituciones financieras más grandes dependen del libre flujo de datos para operar sin problemas en diferentes jurisdicciones alrededor del mundo. Y las instituciones financieras más pequeñas y locales dependen de esas instituciones más grandes para proporcionar servicios internacionales a sus propios clientes, quienes, en un mundo donde el comercio global es la norma, pueden requerir servicios financieros en lugares donde la institución local no opera.

Un ciudadano francés de vacaciones en la República Dominicana puede necesitar retirar dinero utilizando un cajero automático local; o un vendedor peruano que vende productos en Japón a través de internet puede querer recibir el pago en una moneda extranjera. En ambos casos, la transacción solo se puede procesar y el dinero transferir si los datos se mueven a través de fronteras internacionales. La autorización para el retiro del cajero automático debe provenir de un sistema informático en Francia, lo que requiere la transferencia de los datos del cliente al extranjero. La venta en línea implica la transferencia de datos tanto del cliente como del vendedor entre bancos y procesadores de pago ubicados en ambas jurisdicciones.

Estas son solo algunas de las maneras en que los flujos de datos transfronterizos son cruciales para el funcionamiento del sector financiero. Los requisitos de localización de datos limitan la capacidad de las instituciones financieras para operar a través de fronteras, inhibiendo su capacidad para satisfacer las necesidades de sus clientes e incluso la capacidad de los reguladores financieros para supervisar. También impiden que las instituciones financieras aprovechen nuevas oportunidades, como el análisis de datos a gran escala y la inteligencia artificial, que ofrece la tecnología en la nube.

a. Las regulaciones complejas de datos aumentan los costos y sofocan la competencia

Además de sus restricciones sustantivas sobre la transferencia transfronteriza de datos, las reglas de localización de datos también pueden ser difíciles de implementar y cumplir. Por un lado, puede haber una considerable incertidumbre sobre el alcance de las reglas

[74] Regulación Gubernamental No. 71 (2019).
[75] Ryan White, *Cómo la nube salvó los datos de Ucrania de los ataques rusos*, C4ISRNET (22 de jun. 2022), https://www.c4isrnet.com/2022/06/22/how-the-cloud-saved-ukraines-data-from-russian-attacks/; David E. Sanger, *La Nueva Estrategia de Ciberseguridad de Biden Asigna Responsabilidad a las Empresas Tecnológicas,* NEW YORK TIMES (2 de mar. 2023), https://www.nytimes.com/2023/03/02/us/politics/biden-cybersecurity-strategy.html.

de privacidad de datos. Puede no estar claro qué entidades están sujetas a ellas y a qué datos se aplican.[76] Aunque las reglas de localización de datos a menudo distinguen entre datos personales y no personales, la línea entre ellos no siempre es clara.[77] La información sobre individuos particulares, como empleados clave (datos personales), a veces está incrustada en la información sobre empresas (datos no personales).[78] Además, las herramientas sofisticadas de análisis de datos facilitan más que nunca inferir información personal de datos supuestamente no personales.[79] Como resultado, los requisitos de localización que ostensiblemente se aplican solo a datos personales pueden, en la práctica, limitar la transferencia de todos los datos, sean personales o no. Otra fuente de complejidad es que las instituciones financieras pueden estar sujetas a reglas específicas de localización de datos que complementan las leyes generales de protección de datos en una jurisdicción particular.[80] La combinación de reglas generales de protección de datos con reglas específicas aplicables a los servicios financieros puede dar lugar a costos significativos de cumplimiento.

Consideremos una institución financiera global que está evaluando la posibilidad de abrir una sucursal o afiliada en una jurisdicción que requiere almacenamiento local (o copias) de ciertos datos. Para abrir la sucursal, la institución financiera tendría que implementar una solución operativa, como el uso de un proveedor de software local o un centro de datos para procesar y almacenar datos en esa jurisdicción. Establecer y mantener esta solución local requerirá tiempo y dinero, tanto operativamente como en términos de asegurar el cumplimiento de los requisitos de localización de datos aplicables.[81] Esos costos adicionales serán trasladados a los clientes locales de la institución financiera, dejándolos en peor situación que sus clientes en otras jurisdicciones.

Alternativamente, la institución financiera puede decidir que el costo de establecer una solución local es prohibitivo y renunciar a la sucursal o afiliada por completo.[82] Incluso si el costo de la solución local no lo descarta, la institución financiera puede encontrar que no existe una solución local que cumpla con sus propios estándares —o estándares impuestos por su país de origen— para la seguridad o resiliencia de los datos.[83] O la institución financiera puede decidir que es demasiado complicado desarrollar políticas de cumplimiento y gestión de riesgos que estén adaptadas a los requisitos específicos de

[76] Dmitry Kurochkin, Marat Agabalyan y Saglara Ildzhirinova, *La Nueva Ley de Localización de Servidores de Rusia: Implicaciones para Empresas Extranjeras*, BLOOMBERG BNA WORLD DATA PROTECTION REPORT (feb. 2015), https://news.bloomberglaw.com/privacy-and-data-security/russias-new-server-localization-law-implications-for-foreign-companies.

[77] Michèle Finck y Frank Pallas, *Aquellos que No Deben Ser Identificados: Diferenciar Datos Personales de No Personales Bajo el GDPR*, 10(1) INTERNATIONAL DATA PRIVACY LAW 11-36 (feb. 2020), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3462948.

[78] Peter P. Swire y Robert E. Litan, *No es asunto tuyo: Flujos de Datos Globales, Comercio Electrónico y la Directiva de Privacidad Europea*, BROOKINGS INSTITUTION PRESS (1998).

[79] Michèle Finck y Frank Pallas, *Aquellos que No Deben Ser Identificados: Diferenciar Datos Personales de No Personales Bajo el GDPR*, 10(1) INTERNATIONAL DATA PRIVACY LAW 11-36 (feb. 2020), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3462948.

[80] Ver arriba, Parte II.a.

[81] Ver, por ejemplo, *Prasad, Mastercard Comienza a Eliminar Datos de Transacciones Indias Almacenados en el Extranjero* (2019).

[82] Daniel Castro y Alan McQuinn, *Los Flujos de Datos Transfronterizos Impulsan el Crecimiento en Todas las Industrias*, INFORMATION TECHNOLOGY & INNOVATION FOUNDATION (feb. 2015), https://www2.itif.org/2015-cross-border-data-flows.pdf.

[83] TechRadar Pro, *Los altos costos de almacenar datos localmente en una era nativa en la nube*, TECHRADAR (22 de febrero de 2019),, https://www.techradar.com/news/the-high-costs-of-storing-data-locally-in-a-cloud-native-era.

esa jurisdicción.[84] Por cualquiera de estas razones, los requisitos de localización de datos pueden excluir efectivamente a las instituciones financieras del mercado local, sofocando la competencia y privando a los residentes de esa jurisdicción del acceso a servicios importantes.[85]

Los requisitos de localización de datos también pueden inhibir la capacidad de las instituciones financieras locales para servir a clientes que viajan o viven en el extranjero. Las restricciones sobre la transferencia transfronteriza de datos pueden dificultar la consolidación y el análisis de datos de clientes de diferentes ubicaciones, lo cual es crucial para la gestión de riesgos, la detección de fraudes y el análisis de clientes. Si los datos de los clientes no pueden ser fácilmente compartidos o integrados a través de fronteras, las instituciones financieras locales enfrentarán desafíos para servir a sus clientes en otras jurisdicciones. Los requisitos de localización también pueden impedir que las instituciones financieras aprovechen la infraestructura tecnológica global, limitando su capacidad para ofrecer servicios consistentes y eficientes a clientes en el extranjero.[86]

b. La localización de datos puede comprometer la ciberseguridad y la resiliencia

Los defensores de los requisitos de localización de datos frecuentemente apelan a la supuesta mejora de la ciberseguridad y la resiliencia operativa. Estos argumentos a favor de la localización de datos están equivocados. Como se mencionó anteriormente, los proveedores de nube globales se benefician de economías de escala que les permiten realizar inversiones sustancialmente mayores en seguridad de datos y disponibilidad en comparación con los proveedores de infraestructura locales o regionales.[87]

La naturaleza distribuida del almacenamiento y procesamiento en la nube, así como los mayores recursos computacionales disponibles para los principales proveedores de nube en comparación con las instituciones financieras individuales o los proveedores tecnológicos locales, se traducen en una mayor resiliencia operativa. Los proveedores de nube permiten a una institución financiera escalar automáticamente y mantener la disponibilidad frente a un ciberataque que abrumaría la infraestructura tecnológica localmente disponible.[88] Asimismo, al permitir que las instituciones financieras distribuyan procesos y datos a través de diferentes centros de datos, la nube les permite construir aplicaciones que están en línea constantemente, incluso si un centro de datos particular, o una región completa, experimenta una interrupción.[89]

Las empresas tecnológicas locales pueden carecer de recursos que se comparen con los principales proveedores de nube, cuya infraestructura está construida con los más altos estándares de ciberseguridad.[90] Incluso los requisitos de localización que obligan a las instituciones financieras a mantener una copia local de los datos pueden

[84] INTERNATIONAL REGULATORY STRATEGY GROUP, *Cómo la Tendencia hacia la Localización de Datos Está Impactando al Sector de Servicios Financieros* (DICIEMBRE DE 2020).
[85] Margaret Doyle et al., *Cómo Prosperar en un Futuro Incierto: Banca Abierta y PSD2* (2017), https://www2.deloitte.com/content/dam/Deloitte/cz/Documents/financial-services/cz-open-banking-and-psd2.pdf.
[86] Daniel Castro y Alan McQuinn, *Los Flujos de Datos Transfronterizos Impulsan el Crecimiento en Todas las Industrias*, INFORMATION TECHNOLOGY & INNOVATION FOUNDATION (febrero de 2015), https://www2.itif.org/2015-cross-border-data-flows.pdf.
[87] Ver arriba, Parte I.b.
[88] Id.
[89] Id.
[90] Id.

comprometer su seguridad, al aumentar el número de puntos de acceso a los datos y, por lo tanto, la probabilidad de una brecha de ciberseguridad.[91] Los requisitos de localización de datos también pueden dificultar que las instituciones financieras identifiquen, prevengan y mitiguen amenazas cibernéticas, al limitar su capacidad para compartir información de una jurisdicción con reguladores en otras jurisdicciones.[92]

c. La localización de datos puede inhibir la supervisión regulatoria financiera

Facilitar la supervisión regulatoria y la aplicación de la ley es otra justificación comúnmente invocada para los requisitos de localización de datos. Muchos reguladores financieros expresan su preocupación de que una vez que los datos salen de las fronteras de su jurisdicción, ya no podrán acceder a ellos. Como se mencionó anteriormente, la localización de datos no necesariamente resuelve el problema del acceso de la aplicación de la ley o de los reguladores a los datos.[93] Además, lo contrario es igualmente probable: los requisitos de localización de datos pueden dificultar la supervisión por parte de los reguladores financieros.

Los requisitos de localización de datos probablemente provoquen o alienten requisitos recíprocos en otras jurisdicciones. Por lo tanto, incluso si los requisitos de localización en la propia jurisdicción de un regulador facilitan su acceso a algunos datos financieros, requisitos similares en otra jurisdicción impedirían su acceso a otros datos importantes. Cuando una transacción internacional involucra dos jurisdicciones que imponen requisitos de localización de datos, los reguladores financieros en cada jurisdicción solo tendrían una visión de la mitad de la transacción. Esto inhibiría el ejercicio de funciones básicas de vigilancia financiera, como la lucha contra el lavado de dinero y la detección de fraudes, así como mandatos más amplios, como la supervisión de la estabilidad financiera.

d. Beneficios de la transferencia de datos para las instituciones financieras

En ausencia de requisitos de localización de datos, las instituciones financieras pueden aprovechar la infraestructura tecnológica en la nube fuera de la jurisdicción para reducir costos, aumentar la seguridad de los datos y la resiliencia operativa, y ofrecer mejores servicios a los clientes. Esto es cierto tanto para las instituciones financieras globales que buscan ingresar a un nuevo mercado local, como para las instituciones financieras locales que intentan acceder a una mejor infraestructura tecnológica o expandirse globalmente.

Aunque muchos clientes de servicios financieros todavía dependen de una fuerza laboral en la oficina y servicios en persona, existe una demanda creciente de trabajo remoto y servicios a distancia, impulsada en parte por la pandemia de COVID-19. La tecnología en la nube facilita el trabajo remoto y la provisión de servicios digitales y otros servicios

---

[91] Anupam Chander, *¿La localización de datos puede solucionar el problema de Schrems II?*, 23 JOURNAL OF INTERNATIONAL ECONOMIC LAW 771-784 (2020), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3662626 TechRadar Pro, *TechRadar Pro, Los altos costos de almacenar datos localmente en una era nativa en la nube, TECHRADAR (22 de febrero de 2019)*, https://www.techradar.com/news/the-high-costs-of-storing-data-locally-in-a-cloud-native-era.

[92] Nigel Cory y Luke Dascoli, *Cómo las Barreras a los Flujos de Datos Transfronterizos se Están Extendiendo Globalmente, Cuánto Cuestan y Cómo Abordarlas*, INFORMATION TECHNOLOGY AND INNOVATION FOUNDATION (julio de 2021).

[93] Ver Sección II.c.

remotos. Las instituciones financieras como Societe Generale, por ejemplo, dependieron de soluciones de gestión de dispositivos basadas en la nube para apoyar a miles de trabajadores remotos durante los confinamientos relacionados con COVID-19.[94] Un banco multinacional con sede en Europa dependió de su infraestructura en la nube para continuar sirviendo a clientes en Brasil durante la pandemia, lo cual solo fue posible debido a la ausencia de requisitos de localización de datos.[95] Más allá de los cambios impulsados por la pandemia en la fuerza laboral y el servicio al cliente, las instituciones financieras han seguido dependiendo de la tecnología en la nube para ofrecer servicios digitales innovadores a los clientes. Por ejemplo, Itau Unibanco, la institución bancaria más grande de América Latina, aprovechó la tecnología en la nube para implementar Pix, el servicio de pago instantáneo digital mandatado por el banco central de Brasil.[96] Asimismo, BBVA utilizó tecnología basada en la nube para habilitar de manera segura pagos sin contacto cumpliendo con regulaciones específicas de cada país, convirtiéndose en la primera institución financiera en ofrecer pagos sin contacto en Perú, Argentina y Colombia.[97]

Las instituciones financieras también pueden utilizar la infraestructura en la nube offshore para manejar las interrupciones del mercado financiero que de otro modo abrumarían su infraestructura tecnológica. La computación en la nube permite a los usuarios escalar automáticamente sin necesidad de una presencia física en el sitio. Esto puede ayudar a las instituciones financieras a reaccionar ante eventos de estrés del mercado, como aumentos inesperados en los volúmenes de negociación o la volatilidad del mercado.[98] La escalabilidad automática de la nube, así como su mayor capacidad de procesamiento en comparación con la infraestructura tecnológica tradicional, también permite a las instituciones financieras ingerir y analizar datos en tiempo real. Por ejemplo, las soluciones en la nube hacen posible que las instituciones financieras calculen su posición de liquidez varias veces al día, incluso durante períodos de significativa volatilidad del mercado.[99]

Además, la tecnología en la nube facilita el acceso a tecnologías de vanguardia como el análisis de big data y la inteligencia artificial, que dependen de los vastos recursos informáticos disponibles en la nube. Las instituciones financieras de todo el mundo ya utilizan herramientas de IA basadas en la nube para funciones básicas como el soporte al cliente.[100] A medida que se desarrollan las capacidades de aprendizaje automático e IA,

---

[94] MICROSOFT INTUNE, *Société Générale lidera el camino hacia la nube, optimizando la experiencia del usuario y la gestión segura de dispositivos* (14 de octubre de 2022), https://customers.microsoft.com/en-us/story/1558831416191995829-societegenerale-banking-and-capital-markets-cloud.

[95] INSTITUTE OF INTERNATIONAL FINANCE, *Cloud Computing: Un Facilitador Vital en Tiempos de Disrupción* (junio de 2020).

[96] BNAMERICAS, *Itaú de Brasil migrará la mayoría de sus sistemas a la nube de AWS* (4 de agosto de 2022), https://www.bnamericas.com/en/news/brazils-itau-to-migrate-most-of-its-systems-to-aws-cloud; AMAZON WEB SERVICES, *Itaú Unibanco Acelera el Desarrollo del Sistema de Pagos Instantáneos Pix Usando AWS* (2022), https://aws.amazon.com/solutions/case-studies/itau-pix/.

[97] AMAZON WEB SERVICES, *BBVA Usa AWS CloudHSM para Habilitar Pagos NFC Completamente Conformes* (2021), https://aws.amazon.com/solutions/case-studies/bbva/?did=cr_card&trk=cr_card.

[98] RISK.NET, *Innovación Tecnológica del Año* (febrero de 2021), https://www.scotiabank.com/content/dam/scotiabank/corporate/news/assets/Technology_innovation_of_the_year_Scotiabank_Risknet.pdf.

[99] Id.

[100] MICROSOFT, *PicPay integra la Inteligencia Artificial de Microsoft en sus canales de servicio* (20 de junio de 2023), https://news.microsoft.com/es-xl/picpay-integrates-microsoft-artificial-intelligence-into-service-channels/; TRANS-BANK, *Transbank refuerza su posición como empresa tecnológica con IA generativa* (19 de febrero de

se utilizarán para el análisis de datos y otras funciones más críticas, como la gestión de riesgos. HSBC, por ejemplo, utiliza herramientas de modelado de riesgos basadas en la nube para gestionar riesgos e informar actividades de negociación y crédito.[101] Itau Unibanco trasladó su infraestructura de aprendizaje automático de centros de datos locales a la nube para acelerar el despliegue y análisis de modelos.[102] Sin embargo, estas capacidades sofisticadas solo estarán disponibles para las instituciones financieras que estén autorizadas a acceder a servicios basados en la nube que, en muchos casos, dependerán de la infraestructura tecnológica fuera de la jurisdicción y requerirán transferencia internacional de datos.

Parte IV: Recomendaciones de Política para los Reguladores Financieros

Los requisitos de localización de datos imponen costos significativos a las instituciones financieras y a los clientes que sirven. Aunque a menudo están motivados por objetivos de política legítimos, como proteger datos sensibles y garantizar el acceso a datos para la supervisión y la aplicación de la ley, esos objetivos se servirían mejor a través de políticas que eviten esos costos. Los reguladores financieros deben encontrar un equilibrio entre las preocupaciones políticas que subyacen a los requisitos de localización de datos y la necesidad de facilitar el flujo de datos transfronterizo en el sector financiero, incluido el uso de infraestructura en la nube fuera de la jurisdicción. Ese equilibrio se lograría mejor mediante reglas que: (1) se enfoquen en alcanzar los objetivos de política directamente, en lugar de indirectamente a través de requisitos de localización de datos; y (2) aborden los objetivos de política mediante la coordinación y cooperación con otros reguladores locales y reguladores en otras jurisdicciones.

a. Adoptar un enfoque basado en principios para la protección de datos

Mandar que los datos permanezcan en una jurisdicción particular no es ni necesario ni suficiente para mantener su seguridad. Los datos sensibles que no se gestionan de manera segura pueden ser comprometidos por alguien que no tiene acceso físico a ellos. En consecuencia, la localización de datos hace poco para asegurar que los datos privados permanezcan privados. Para proteger los datos privados, los reguladores financieros deben enfocarse en garantizar que los datos se almacenen de manera *segura*, ya sea localmente o en el extranjero. Como se mencionó anteriormente, las plataformas de los principales proveedores de nube están construidas para ofrecer a las instituciones financieras herramientas para implementar requisitos de seguridad rigurosos, incluida la encriptación de datos incorporada.

2024), https://ir.transbank.cl/en/transbank-further-consolidates-its-position-as-a-tech-company-with-generative-ai; AMAZON WEB SERVICES, *Cómo el Banco NatWest Personaliza la Experiencia del Cliente Usando AWS* (2023), https://aws.amazon.com/solutions/case-studies/natwest/?did=cr_card&trk=cr_card.

[101] GOOGLE CLOUD, HSBC: *Adoptando la nube para reducir la exposición al riesgo a través de capacidades rápidas de análisis e información*, https://cloud.google.com/customers/hsbc-risk-advisory-tool.

[102] AMAZON WEB SERVICES, *Itaú Mejora la Velocidad de Comercialización y la Productividad de Soluciones de ML Usando Amazon Web Services* (2024), https://aws.amazon.com/solutions/case-studies/itau-ml-case-study/?did=cr_card&trk=cr_card.

Para aliviar las preocupaciones de que las instituciones financieras puedan transferir datos sensibles a jurisdicciones que no protegen la privacidad de los datos, los reguladores podrían exigir que los datos solo se almacenen en una jurisdicción que ofrezca protecciones legales adecuadas para los datos personales. El enfoque de las Directrices de Privacidad de la OCDE para la transferencia de datos personales es instructivo.[103] Esas directrices, que fueron adoptadas en 1980 y revisadas en 2013, enfatizan que la responsabilidad legal por los datos personales se aplica sin importar la ubicación de los datos, ya sea que se almacenen localmente o en el extranjero. También estipulan que los países deben abstenerse de restringir el flujo transfronterizo de datos cuando existan suficientes salvaguardas para asegurar que los datos personales estén protegidos. Además, proporcionan que las restricciones al flujo transfronterizo de datos personales deben ser proporcionales a los riesgos presentados.[104]

La regulación de protección de datos de Brasil adopta un enfoque similar. La regulación permite la transferencia de datos a países con un "nivel adecuado de protección" para los datos personales y garantías de cumplimiento con los derechos y principios de protección de datos proporcionados por la regulación de protección de datos de Brasil.[105] Importante, esos estándares no son rígidos, sino que pueden ser satisfechos de varias maneras diferentes, incluyendo mediante disposiciones contractuales específicas o códigos de conducta generales.[106] Eso permite a las instituciones financieras flexibilidad para determinar cómo proteger mejor los datos sensibles que se transfieren fuera de la jurisdicción, siempre que existan suficientes salvaguardas de privacidad.

b. Enfocarse en la calidad de la infraestructura tecnológica, no en su ubicación

La localización de datos se justifica frecuentemente con la idea de que el almacenamiento local hace que los datos estén más disponibles y sean más resistentes a interrupciones. Sin embargo, la ubicación de los datos es solo uno de los factores que pueden afectar su disponibilidad y resiliencia operativa. Un enfoque que priorice la disponibilidad y la resiliencia operativa debe tener en cuenta los muchos factores que pueden influir en la integridad y disponibilidad de los datos. En muchos casos, confiar en un proveedor de nube importante, incluida su infraestructura fuera de la jurisdicción, brindará a las instituciones financieras un mayor grado de disponibilidad y resiliencia que la infraestructura local. Los reguladores deberían otorgar a las instituciones financieras más libertad para hacer su propia evaluación sobre la resiliencia de sus soluciones de almacenamiento y procesamiento de datos ante interrupciones, teniendo en cuenta la naturaleza e importancia del proceso y el potencial de interrupción.

c. Garantizar el acceso a los datos para la supervisión regulatoria y el cumplimiento de la ley

La supervisión efectiva de las instituciones financieras puede lograrse sin requerir el almacenamiento local de datos. Los reguladores financieros y las autoridades encargadas de hacer cumplir la ley pueden garantizar el acceso a los datos relevantes, ya sea que

[103] ORGANIZACIÓN PARA LA COOPERACIÓN Y EL DESARROLLO ECONÓMICOS, *Recomendación del Consejo sobre las Directrices para la Protección de la Privacidad y los Flujos Transfronterizos de Datos Personales* (2013), https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0188.
[104] Id, Parte IV.
[105] Ley de Protección General de Datos, Sección V.
[106] Id.

estén almacenados localmente o en una jurisdicción diferente. El acceso a los datos almacenados en el extranjero puede lograrse mediante acuerdos con reguladores financieros en otras jurisdicciones. Varios reguladores financieros han trabajado con sus contrapartes extranjeras para desarrollar marcos legales bilaterales y mecanismos de cooperación transfronteriza, que están destinados a permitir los flujos de datos transfronterizos mientras se garantiza el acceso a los datos para fines de supervisión. Por ejemplo, el Banco Central de Brasil tiene acuerdos destinados a facilitar los flujos de información supervisora con las autoridades supervisoras donde las instituciones financieras brasileñas tienen operaciones en el extranjero y aquellas donde las instituciones financieras extranjeras tienen operaciones en Brasil.[107] De manera similar, la Autoridad Monetaria de Singapur ha celebrado acuerdos con los reguladores financieros de EE. UU. y el Reino Unido que permiten a las instituciones financieras transferir datos financieros, incluida información personal, a través de fronteras, siempre que los reguladores financieros tengan acceso completo y oportuno a esos datos.[108] A nivel multilateral, el Memorando de Entendimiento Multilateral actualizado desarrollado por la Organización Internacional de Comisiones de Valores (IOSCO) requiere que los signatarios compartan cierta información con sus contrapartes regulatorias.[109]

El acceso a los datos relevantes también puede garantizarse a través de los acuerdos contractuales de las instituciones financieras con los proveedores de servicios tecnológicos. Varias jurisdicciones, por ejemplo, requieren que los acuerdos contractuales de una institución financiera con sus proveedores de servicios garanticen que los reguladores financieros tengan acceso suficiente a los datos para supervisar la institución financiera.[110] Estas disposiciones contractuales generalmente incluyen el acceso a los datos de las instituciones financieras, así como la cooperación del proveedor de servicios con el regulador en relación con las solicitudes de información y los derechos de acceso para auditorías del proveedor de servicios.[111]

d. Aumentar la coordinación a nivel local e internacional

El complejo mosaico de requisitos de localización de datos tanto dentro de las jurisdicciones como entre diferentes jurisdicciones aumenta los costos para las instituciones financieras y sofoca la competencia que, de otro modo, beneficiaría a sus clientes. Para minimizar la incertidumbre y lograr coherencia regulatoria, los reguladores financieros deben trabajar conjuntamente con las autoridades locales (como las autoridades de

[107] BANCO CENTRAL DO BRASIL, *Memorandos de Entendimiento Internacionales para Propósitos de Supervisión*, https://www.bcb.gov.br/en/financialstability/supervisionmous.
[108] DEPARTAMENTO DEL TESORO DE LOS EE.UU., *Declaración Conjunta Estados Unidos – Singapur sobre Conectividad de Datos en Servicios Financieros* (5 de febrero de 2020), https://home.treasury.gov/news/press-releases/sm899; COMISIÓN DE COMERCIO DE FUTUROS DE PRODUCTOS BÁSICOS DE EE.UU. Y LA AUTORIDAD MONETARIA DE SINGAPUR, *Cooperación e Intercambio de Información sobre Innovación en Tecnología Financiera* (13 de septiembre de 2018), https://www.cftc.gov/sites/default/files/2018-09/cftc-mas-cooparrgt091318_16.pdf; AUTORIDAD MONETARIA DE SINGAPUR, *Singapur y Reino Unido Refuerzan la Cooperación en Conectividad de Datos, Desarrollo de Talento, Finanzas Verdes y Ciberseguridad* (13 de junio de 2019), https://www.mas.gov.sg/news/media-releases/2019/singapore-and-uk-to-enhance-cooperation.
[109] ORGANIZACIÓN INTERNACIONAL DE COMISIONES DE VALORES, *Memorando de Entendimiento Multilateral sobre Consulta, Cooperación e Intercambio de Información* (mayo de 2012), https://www.iosco.org/library/pubdocs/pdf/IOSCOPD386.pdf.
[110] AUTORIDAD DE REGULACIÓN PRUDENCIAL DE AUSTRALIA, *Norma Prudencial CPS 231: Externalización, párr. 34* (julio de 2017), https://www.apra.gov.au/sites/default/files/Prudential-Standard-CPS-231-Outsourcing-%28July-2017%29.pdf.
[111] Id.

privacidad y los reguladores en otros sectores) así como con sus contrapartes extranjeras para desarrollar enfoques ampliamente consistentes sobre la transferencia de datos que permitan la transferencia transfronteriza de datos mientras se abordan las razones percibidas para la localización de datos. Hacerlo minimiza las barreras innecesarias para la transferencia de datos, permitiendo a las instituciones financieras beneficiarse de la infraestructura tecnológica fuera de la jurisdicción, incluida la computación en la nube.

La coordinación internacional puede ocurrir a nivel bilateral. Por ejemplo, Australia y Singapur firmaron un "acuerdo de economía digital" que permite a las empresas, incluida la del sector financiero, transferir datos a través de fronteras sin estar obligadas a construir o utilizar centros de datos en ninguna de las dos jurisdicciones. Lo más importante es que el acuerdo garantiza que las normas de privacidad aplicables a la información personal continúen aplicándose, ya sea que los datos se almacenen localmente o en la otra jurisdicción.[112] Singapur ha celebrado acuerdos similares con Corea y el Reino Unido.[113]

A nivel multilateral, Japón ha propuesto el concepto de "flujo libre de datos con confianza", que ha sido respaldado tanto por el G7 como por el G20.[114] El objetivo del concepto, que articula principios para la gobernanza de datos que informarían los estándares globales, es promover el flujo libre de datos mientras se protege la privacidad y la seguridad de los datos. En la región del Indo-Pacífico, el foro de Cooperación Económica Asia-Pacífico (APEC) desarrolló un sistema de Reglas de Privacidad Transfronteriza (CBPR), un marco de privacidad respaldado por el gobierno que establece un mecanismo de certificación para las empresas privadas que acuerdan implementar protecciones de privacidad de datos reconocidas internacionalmente.[115] Las empresas certificadas, cuya conformidad es evaluada por agentes de responsabilidad designados y se hace cumplir por ley, pueden transferir datos libremente entre los países participantes, permitiéndoles superar las diferencias entre las leyes de privacidad de los países participantes.[116] Varios miembros de APEC, incluidos Estados Unidos y Japón, han promovido un sistema CBPR global para expandir el modelo de APEC.[117] Sin embargo, actualmente, las instituciones financieras generalmente no pueden ser certificadas porque los reguladores financieros no participan en el sistema.[118]

En el sector financiero, el Consejo de Estabilidad Financiera (FSB) ha identificado el intercambio de datos transfronterizos y los estándares de mensajes como una prioridad

---

[112] MINISTERIO DE COMERCIO E INDUSTRIA DE SINGAPUR, *Acuerdo de Economía Digital Singapur-Australia (SADEA)* (2020), https://www.mti.gov.sg/Trade/Digital-Economy-Agreements/The-Singapore-Australia-Digital-Economy-Agreement.

[113] MINISTERIO DE COMERCIO E INDUSTRIA DE SINGAPUR, *Acuerdo de Asociación Digital Corea-Singapur (KSDPA) (2022)*, https://www.mti.gov.sg/Trade/Digital-Economy-Agreements/KSDPA; MINISTERIO DE COMERCIO E INDUSTRIA DE SINGAPUR, Acuerdo de Economía Digital Reino Unido-Singapur (UKSDEA) (2022), https://www.mti.gov.sg/Trade/Digital-Economy-Agreements/UKSDEA.

[114] G7, *Hoja de Ruta del G7 para la Cooperación en el Flujo de Datos Libre y Confiable (2021)*, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/986160/Annex_2__Roadmap_for_cooperation_on_Data_Free_Flow_with_Trust.pdf.

[115] COOPERACIÓN ECONÓMICA ASIA-PACÍFICO, *Sistema de Reglas de Privacidad Transfronteriza de APEC (CBPR) (2019)*, https://cbprs.org/wp-content/uploads/2019/11/4.-CBPR-Policies-Rules-and-Guidelines-Revised-For-Posting-3-16-updated-1709-2019.pdf.

[116] Id.

[117] DEPARTAMENTO DE COMERCIO DE EE. UU., *Declaración Global sobre Reglas de Privacidad Transfronteriza*, https://www.commerce.gov/global-cross-border-privacy-rules-declaration.

[118] NSTITUTO DE FINANZAS INTERNACIONALES, *Flujos de Datos a Través de Fronteras: Superando las Restricciones de Localización de Datos* (marzo 2019).

para mejorar los pagos transfronterizos.[119] Como parte de este proceso, el FSB planea desarrollar recomendaciones para promover la alineación y la interoperabilidad entre los diferentes marcos de datos que se aplican a los pagos transfronterizos, incluida la privacidad de los datos, la resiliencia operativa, el cumplimiento de AML/CFT y los requisitos de acceso regulatorio y de supervisión. Esas recomendaciones, a su vez, servirán como base para que las autoridades nacionales reevalúen sus propios marcos de datos.[120] La consistencia entre las jurisdicciones en la transferencia de datos financieros y la eliminación de barreras para las transferencias transfronterizas de datos permitirá a las instituciones financieras aprovechar los beneficios que la tecnología en la nube tiene para ofrecer.

[119] CONSEJO DE ESTABILIDAD FINANCIERA, *Hoja de Ruta del G20 para Mejorar los Pagos Transfronterizos* (23 de febrero de 2023), https://www.fsb.org/wp-content/uploads/P230223.pdf.
[120] Id.

Programa sobre Sistemas Financieros Internacionales (PIFS)
134 Mount Auburn Street, Cambridge, MA 02138
www.pifsinternational.org