Programa sobre
Sistemas Financeiros Internacionais

Localização de Dados, Adoção de Nuvem e o Setor Financeiro

[Traduzido do Inglês]

JULHO DE 2024

O Programa sobre Sistemas Financeiros Internacionais (PIFS) é uma organização sem fins lucrativos que investiga questões que afetam o sistema financeiro global. O PIFS também organiza simpósios internacionais, programas de formação de executivos e eventos especiais que fomentam o diálogo e promovem a educação sobre estas questões. O PIFS foi fundado em 1986 por Hal S. Scott, atualmente Professor Emérito da Faculdade de Direito de Harvard. Mais de trinta anos depois, Hal Scott continua a dirigir o PIFS.

Este relatório foi elaborado por Hal Scott (Presidente do Conselho de Administração e Presidente do PIFS), John Gulliver (Diretor Executivo), Hillel Nadler (Investigador Principal) e Jon Ondrejko (Vice-Presidente Sénior de Programas).

A Amazon Web Services, Inc. é patrocinadora financeira do PIFS.

[O relatório original foi escrito em Inglês.
Esta versão foi traduzida para o Português.]

Localização de Dados, Adoção de Nuvem e o Setor Financeiro

JULHO DE 2024

Índice

SUMÁRIO EXECUTIVO

Num mundo cada vez mais interligado, a capacidade de as instituições financeiras moverem dados através das fronteiras é fundamental não só para o seu sucesso como para a sua capacidade de servir os seus clientes. No entanto, um número crescente de jurisdições está a impor requisitos de "localização de dados" que restringem ou mesmo proíbem a transferência de dados para fora das suas fronteiras. O presente relatório analisa a forma como estes requisitos afetam o sector financeiro à luz da crescente adoção da tecnologia de computação em nuvem. Os requisitos de localização de dados, embora motivados, muitas vezes, por preocupações políticas legítimas, impõem custos significativos às instituições financeiras e aos seus clientes, nomeadamente impedindo as instituições financeiras de aproveitarem todo o potencial da computação em nuvem. As entidades reguladoras podem dar resposta a essas preocupações sem impedir o livre fluxo de dados, que é essencial para a concretização dos benefícios da adoção de nuvem no setor financeiro.

A Promessa da Tecnologia de Nuvem para o Setor Financeiro

A pandemia de COVID-19 acelerou uma tendência que estava já bem encaminhada: a adoção da computação em nuvem por parte das instituições financeiras. A tecnologia de computação em nuvem oferece benefícios significativos, incluindo eficiência de custos, maior segurança cibernética e resiliência operacional. Ao permitir que as instituições financeiras aumentem automaticamente os seus recursos informáticos, a tecnologia de computação em nuvem possibilita que lidem com eventos de stress do mercado, como picos inesperados nos volumes de negociação ou ciberataques, que poderiam sobrecarregar a infraestrutura tradicional de tecnologias da informação (TI). Além disso, os vastos recursos de computação disponíveis em nuvem facilitam o acesso a tecnologias de ponta, como a análise de dados e a inteligência artificial (IA), que prometem transformar a forma como as instituições financeiras satisfazem as necessidades dos seus clientes e gerem o risco.

O Papel Fundamental dos Fluxos de Dados Transfronteiriços no Setor financeiro

As transferências de dados transfronteiriças são essenciais para o setor financeiro mundial. São necessárias para o processamento de pagamentos internacionais, para a prestação de serviços financeiros a clientes que residem ou exercem a sua atividade em várias jurisdições e para facilitar a supervisão regulamentar. Mesmo as instituições financeiras locais dependem de fluxos de dados transfronteiriços quando ligam os seus clientes a redes financeiras mundiais. Ao impedir estes fluxos, os requisitos de localização de dados limitam a capacidade de as instituições financeiras satisfazerem as necessidades dos seus clientes e até a capacidade dos reguladores financeiros efetuarem uma supervisão eficaz.

Requisitos de Localização de Dados e Adoção de Nuvem

Os defensores da localização de dados argumentam frequentemente que esta aumenta a privacidade dos dados, assegura a disponibilidade dos dados em caso de perturbação, facilita a supervisão regulamentar e a aplicação da lei. No entanto, estes argumentos são

erróneos. A localização física dos dados não é necessária nem suficiente para a sua segurança; os dados que não são geridos de forma segura podem ser comprometidos independentemente do local onde são armazenados. Por outro lado, os grandes operadores de serviços de computação em nuvem, devido às economias de escala, podem investir muito mais em cibersegurança e resiliência do que os operadores locais de tecnologia. Para além disso, o armazenamento local de dados não garante o acesso regulamentar; as autoridades reguladoras podem garantir o acesso aos dados armazenados no estrangeiro através de acordos bilaterais ou multilaterais.

Os requisitos de localização de dados também ameaçam privar as instituições financeiras dos benefícios da adoção de nuvem, que dependem fortemente da capacidade de mover dados entre fronteiras. Os principais operadores de serviços de computação em nuvem não possuem centros de dados em todas as jurisdições. Pelo contrário, tiram partido das economias de escala operando uma rede global de centros de dados. Esta infraestrutura descentralizada é fundamental para as vantagens de resiliência e cibersegurança da nuvem: os dados e os processos são distribuídos por diferentes centros de dados, tornando-os menos vulneráveis a interrupções ou ataques localizados. Também fornece os enormes recursos de computação que permitem a análise de ponta e a IA.

Recomendações de Políticas para as Autoridades de Regulamentação Financeira

Para equilibrar as legítimas preocupações com as políticas e a necessidade imperativa de facilitar os fluxos de dados transfronteiriços de forma a permitir a adoção da computação em nuvem, o relatório recomenda que os reguladores financeiros:

- Adotem uma abordagem de proteção de dados que se concentre em garantir que os dados são armazenados de forma segura, e não no local onde são armazenados.
- Trabalhem conjuntamente com as entidades regulamentadas e os operadores de serviços de computação em nuvem com vista a tirar partido de infraestruturas de computação em nuvem globais fora das jurisdições e a reforçar a cibersegurança e a resiliência operacional.
- Assegurem o acesso aos dados para efeitos de supervisão regulamentar e aplicação da lei através de acordos com outras jurisdições e não através da localização de dados.
- Aumentem a coordenação com outras autoridades locais e congéneres estrangeiras com o objetivo de desenvolver políticas coerentes de transferência de dados.

Conclusão

Os requisitos de localização de dados, embora muitas vezes baseados em preocupações legítimas, impõem custos significativos às instituições financeiras e aos seus clientes. Inibem a capacidade de as instituições financeiras tirarem partido da tecnologia de computação em nuvem para aumentar a segurança, a resiliência e a inovação. Ao adotarem políticas que facilitem a segurança dos fluxos transfronteiriços de dados, os reguladores financeiros podem dar resposta às suas legítimas preocupações sem

prejudicar o sector financeiro mundial. Num mundo cada vez mais interligado, o livre fluxo de dados não é apenas benéfico, é essencial.

INTRODUÇÃO

O sector financeiro funciona com base na informação: o sucesso das instituições financeiras depende da sua capacidade de obter, proteger e utilizar a informação em seu benefício e em benefício dos seus clientes. Os dados financeiros incluem informações sobre os clientes, como o seu nome e número de conta, e informações sobre as empresas e os seus principais empregados. O facto de as instituições financeiras dependerem cada vez mais dos serviços de computação em nuvem para armazenar, processar e transmitir informações de forma segura e eficiente trouxe desafios à forma como as jurisdições regulam os dados financeiros.

Num mercado global, como o mercado dos serviços financeiros, o livre fluxo transfronteiriço de dados gera um valor significativo. A circulação transfronteiriça de dados é essencial para o processamento de pagamentos internacionais, a prestação de serviços financeiros a clientes individuais e empresariais e a melhoria da gestão do risco a nível das instituições financeiras. Ainda assim, nos últimos anos tem-se assistido a uma imposição de requisitos de "localização de dados": restrições que exigem diretamente, ou têm como consequência, que os dados provenientes de uma jurisdição permaneçam nessa jurisdição.[1]

Este relatório analisa os requisitos de localização de dados e o seu impacto no setor financeiro. A Parte I do relatório apresenta o contexto da adoção da computação em nuvem no setor financeiro e o papel fundamental dos fluxos transfronteiriços de dados para o setor financeiro. A Parte II aprofunda os diferentes tipos de requisitos de localização de dados, as motivações apresentadas para a adoção de requisitos de localização de dados e as suas potenciais desvantagens. A Parte III centra-se na forma como os requisitos de localização de dados afetam as instituições financeiras e a sua capacidade de beneficiar da adoção de nuvem.

A Parte IV conclui com recomendações de políticas para os reguladores financeiros no que diz respeito à transferência transfronteiriça de dados no contexto da adoção de computação em nuvem, abordando as preocupações com que os governos nacionais e os reguladores financeiros justificaram os requisitos de localização de dados. As autoridades reguladoras devem adotar uma abordagem da proteção de dados baseada em princípios que permitam a transferência segura de dados para outras jurisdições, desde que estas assegurem níveis de proteção de dados privados suficientes. Devem também reconhecer que as infraestruturas tecnológicas globais, fora da jurisdição, podem reforçar a cibersegurança e a resiliência operacional. Em vez de se centrarem no *local* onde se encontram os dados, as autoridades reguladoras devem dar resposta às preocupações relativas à supervisão regulamentar e à aplicação da lei, garantindo o *acesso* aos dados. Além disso, devem trabalhar para alinhar as políticas de transferência de dados com as autoridades locais e reguladores das outras jurisdições.

[1] David McCabe e Adam Satariano, *The Era of Borderless Data Is Ending*, New York Times (23 de maio de 2022), https://www.nytimes.com/2022/05/23/technology/data-privacy-laws.html.

PARTE I: ADOÇÃO DE NUVEM E TRANSFERÊNCIAS INTERNACIONAIS DE DADOS NO SETOR FINANCEIRO

A computação em nuvem permite que os dados sejam armazenados em servidores remotos mantidos por um operador externo e recuperados através de uma rede, como a Internet, em vez de serem armazenados numa infraestrutura proprietária localizada.[2] Embora a computação em nuvem não seja uma novidade para o setor financeiro, a pandemia de COVID-19 acelerou a adoção de nuvem por parte das instituições financeiras. A adoção de nuvem é bastante promissora para a eficiência de custos, a resiliência operacional, a segurança cibernética e a inovação das instituições financeiras. Contribui também para facilitar a segurança dos fluxos transfronteiriços de dados, que desempenham um papel fundamental no mercado mundial dos serviços financeiros. No entanto, os requisitos de localização de dados prejudicam a capacidade de as instituições financeiras tirarem partido da tecnologia de computação em nuvem em seu benefício e em benefício dos seus clientes.

a. Adoção de nuvem no setor financeiro

As instituições financeiras têm vindo a utilizar a tecnologia de nuvem, de uma forma ou de outra, há quase duas décadas.[3] A adoção de serviços em nuvem no setor financeiro já estava, portanto, em curso antes da pandemia de COVID-19.[4] A pandemia acelerou a procura de serviços em nuvem, uma vez que as instituições financeiras foram forçadas a abandonar o serviço de apoio ao cliente presencial e a recorrer a uma força de trabalho remota. A adoção de nuvem permitiu que as instituições financeiras ampliassem os serviços remotos em questão de dias.[5]

De acordo com um inquérito recente a instituições financeiras globais, 98% dos inquiridos mantinham pelo menos alguns dados, aplicações ou operações em nuvem.[6] O Banco Santander, um dos maiores bancos do mundo, planeia migrar a maior parte dos seus serviços bancários principais para a nuvem até ao final de 2024.[7] O maior banco da América Latina, o Itaú Unibanco, vai transferir a maioria dos seus sistemas para a nuvem em dez anos. [8] Alguns bancos foram ainda mais longe: O Capital One, um dos maiores bancos dos Estados Unidos, anunciou em 2021 que tinha encerrado os seus centros de dados privados e que tinha feito a transição de todos os seus serviços principais para a

[2] Peter Mell e Tim Grance, *The NIST Definition of Cloud Computing*, National Institute of Standards and Technology (setembro de 2011), https://csrc.nist.gov/pubs/sp/800/145/final.
[3] Lisa Valentine, *Clouded outlook*, 104 ABA Banking Journal 22 (setembro de 2012).
[4] Jerry Silva, *Banking on the Cloud: Results from the 2020 CloudPath Survey*, IDC Perspective 7-8 (novembro de 2020).
[5] Daniel Pujazon e Brad Carr, *Cloud Computing: A Vital Enabler in Times of Disruption*, Institute of International Finance 4-5 (junho de 2020), https://www.iif.com/portals/0/Files/content/32370132_iif_cloud_computing_resilience.pdf.
[6] Cloud Security Alliance, *State of Financial Services in Cloud* (2023). Os inquiridos incluíram bancos e cooperativas de crédito, fintech e outras instituições financeiras nas regiões das Américas (52%), EMEA (28%) e Ásia-Pacífico (20%).
[7] BANCO SANTANDER, *Santander passes key milestone in its transformation after migrating its CIB banking platform to the cloud* (11 de dezembro 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- para a nuvem .
[8] Samantha Lipana e Marissa Ramos, *Latin America's 30 largest banks by assets, 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.

nuvem.[9] Outras instituições financeiras - incluindo empresas de investimento, corretores, consultores de investimento e companhias de seguros - também migraram algumas operações para a nuvem.[10] Além disso, vários serviços de utilidade pública do mercado financeiro, incluindo câmaras de compensação e bolsas de valores, fizeram a transição para a nuvem de alguma forma.[11]

Embora instituições financeiras como o Banco Santander e o Capital One tenham apostado tudo (ou quase) na computação em nuvem, a adoção no sector financeiro ainda está na sua fase inicial. O mesmo inquérito ao setor que revelou 98% de adoção da nuvem também mostrou que quase metade dos inquiridos mantém na nuvem menos de 10% do volume de trabalho essencial para o negócio. Da mesma forma, quase metade dos inquiridos refere que menos de dez por cento do seu volume de trabalho regulamentado foi migrado para ambientes de nuvem públicos.[12] As instituições financeiras têm utilizado maioritariamente a nuvem para aplicações empresariais, como recursos humanos e ferramentas de colaboração. A maior parte das operações principais ainda é efetuada com recurso a sistemas informáticos antigos.[13]

b. As vantagens da tecnologia de nuvem para as instituições financeiras e para os seus clientes

Ainda assim, espera-se que a adoção da nuvem no setor financeiro - incluindo no que concerne as operações principais - aumente nos próximos anos. O modelo de nuvem, que disponibiliza recursos informáticos por encomenda e possibilita que os clientes paguem apenas pelos recursos que efetivamente utilizam, permite que as instituições financeiras transformem grandes despesas iniciais de TI em custos operacionais menores e regulares.[14] De acordo com algumas estimativas, a adoção de nuvem pode reduzir os custos de TI entre 20 e 50%, o que corresponde, em toda a economia, a centenas de milhões de dólares de poupança em custos.[15] Transformar elevadas despesas de capital em custos operacionais contínuos também torna as instituições financeiras mais ágeis do ponto de vista tecnológico: possibilita-lhes testar novos cenários, ferramentas de software e configurações alternativas sem um longo processo de aquisição e aprovisionamento. A redução dos custos e a maior agilidade tecnológica traduzem-se em melhores produtos e serviços para os clientes, especialmente produtos financeiros digitais com características e dados robustos. A computação em nuvem

[9] Adrian Jimenea et al., *The world's largest banks by assets, 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 (3 de janeiro de 2022), https://www.nytimes.com/2022/01/03/business/wall-street-cloud-computing.html.

[10] AMAZON WEB SERVICES, *Vanguard aumenta valor para o investidor usando Amazon ECS e AWS Fargate* (2021), https://aws.amazon.com/solutions/case-studies/vanguard-ecs-fargate-case-study/ .

[11] GRUPO CME, *CME Group Signs 10-Year Partnership with Google Cloud to Transform Global Derivatives Markets Through Cloud Adoption* (4 de novembro de 2021), https://www.cmegroup.com/media-room/press-releases/2021/11/04/cme_group_signs_10-yearpartnershipwithgooglecloudtotransformglob.html ; Nasdaq, *Nasdaq and AWS Partner to Transform Capital Markets* (30 de novembro de 2021), https://www.nasdaq.com/press-release/nasdaq-and-aws-partner-to-transform-capital-markets-2021-12-01 ; NEW YORK STOCK EXCHANGE, NYSE Market Data via Amazon Web Services (AWS),https://www.nyse.com/nyse-cloud .

[12] CLOUD SECURITY ALLIANCE, *State of Financial Services in Cloud* (2023).

[13] Id.

[14] DEPOSITORY TRUST & CLEARING CORPORATION, *Moving Financial Market Infrastructure to the Cloud*, 5-6 (maio de 2017).

[15] Patrick Wauters, et al., *Measuring the economic impact of cloud computing in Europe,* Deloitte (2016), https://ec.europa.eu/newsroom/dae/redirection/document/41184 .

também nivela o aspeto tecnológico entre instituições financeiras de diferentes dimensões, dando às instituições mais pequenas e às start-ups de fintech acesso a recursos informáticos que anteriormente só estavam disponíveis para instituições maiores e com capacidade para dedicar recursos significativos à infraestrutura tecnológica.[16]

Ao facilitar a inovação a baixo custo e o aumento da concorrência, a migração para a computação em nuvem ajuda a expandir o acesso e a inclusão financeira, especialmente para clientes em mercados em desenvolvimento ou mal servidos.[17] A nível mundial, a percentagem de adultos com uma conta numa instituição financeira ou num serviço de dinheiro móvel aumentou de 51% para 76% durante a década de 2011 a 2021.[18] As plataformas financeiras de computação em nuvem têm desempenhado um papel fundamental para chegar a empresas e indivíduos anteriormente mal servidos. Na China, por exemplo, a abordagem nativa de nuvem do WeBank permitiu que a sua plataforma de empréstimos chegasse a milhões de indivíduos e empresas com pouco ou nenhum historial de crédito.[19] O Nubank, um banco brasileiro exclusivamente móvel, utiliza uma infraestrutura baseada em nuvem para oferecer cartões de crédito e empréstimos pessoais a clientes que não podem obter empréstimos em bancos tradicionais devido à sua falta de historial de crédito.[20] No Sudeste Asiático, as aplicações de transporte de passageiros, como a Grab e a Go-Jek (agora GoTo), tiraram partido da infraestrutura de computação em nuvem para fornecer pagamentos e outros serviços financeiros aos utilizadores de retalho.[21] O Mercado Livre, o maior operador de comércio e pagamentos online da América Latina, oferece serviços de pagamento e crédito baseados em nuvem a clientes que, de outra forma, não teriam acesso a eles.[22]

A computação em nuvem pode também ser mais segura e resistente do que as infraestruturas tradicionais. Ao contrário das instituições financeiras, com exceção das maiores, os principais operadores de serviços de computação em nuvem estão na

---

[16] Wang Jin and Kristina McElheran, *Economies before Scale: IT Strategy and Performance Dynamics of Young US Businesses*, ROTMAN SCHOOL OF MANAGEMENT WORKING PAPER No. 3112901 (2018), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3112901. Os operadores de serviços na nuvem podem assegurar a conformidade com a Norma de Segurança de Dados (DSS) da Indústria de Cartões de Pagamento (PCI), oferecendo um ambiente seguro para armazenar, processar e transmitir informações de cartões de crédito. Ver, em geral, CLOUD SPECIAL INTEREST GROUP E PAYMENT CARD INDUSTRY SECURITY STANDARDS COUNCIL, *PCI SSC Cloud Computing Guidelines* (abril de 2018), https://www.pcisecuritystandards.org/pdfs/PCI_SSC_Cloud_Guidelines_v3.pdf.

[17] WORLD BANK AND THE INTERNATIONAL MONETARY FUND, Bali Fintech Agenda (2018); Max Chuard, *Cloud and SaaS technology can drive inclusive banking. Here are 3 reasons how*, WORLD ECONOMIC FORUM (10 dezembro, 2020), https://www.weforum.org/agenda/2020/12/cloud-and-saas-technology-can-drive-inclusive-banking/.

[18] WORLD BANK, *The Global Findex Database: Measuring Financial Inclusion and the Fintech Revolution* (2024), https://www.worldbank.org/en/publication/globalfindex.

[19] Sally Chen et al., *Virtual Banking and Beyond*, 120 BIS PAPERS (Jan. 2022), https://www.bis.org/publ/bppdf/bispap120.pdf.

[20] Debopriyo Bhattacharyya et al., *Global Banking Annual Review 2023: The Great Banking Transition*, MCKINSEY & COMPANY (10 outubro, 2023), https://www.mckinsey.com/industries/financial-services/our-insights/global-banking-annual-review.

[21] Grab, *Grab forges strategic cloud partnership with Microsoft to drive innovation and adoption of digital services across Southeast Asia* (9 outubro, 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, *Indonesia's GoTo Group goes with Google Cloud for next phase of Asian attack*, Channel Asia (27 julho, 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 and the changing structure of financial intermediation*, 34(100) Economic Policy 761-799 (2019).

vanguarda da investigação e implementação da segurança.[23] As plataformas dos principais operadores de serviços de computação em nuvem foram também concebidas para fornecer ferramentas aos clientes com vista a alcançar requisitos de segurança rigorosos, como a monitorização e o registo de todas as atividades e a encriptação de dados incorporada.[24] O crescimento dos serviços em nuvem permite que as instituições financeiras lidem com requisitos de capacidade inesperados - seja devido a um aumento imprevisto na atividade do mercado ou a um ciberataque malicioso - que poderiam sobrecarregar as suas próprias infraestruturas de TI. [25] Além disso, uma vez que a infraestrutura de nuvem está mais distribuída geograficamente pelos centros de dados e regiões do que a infraestrutura de TI tradicional, a adoção de nuvem facilita uma maior resiliência no caso de uma falha local.[26]

Os vastos recursos de computação e o crescimento automático da nuvem também a torna especialmente adequada para transformar a forma como as instituições financeiras lidam com o tratamento de dados. Os ambientes baseados em nuvem permitem às instituições financeiras introduzir dados a velocidades muito superiores às disponíveis na infraestrutura de TI tradicional. Além disso, facilitam uma análise e manipulação de dados sem precedentes após a sua introdução.[27] Este nível sofisticado de análise de dados pode ajudar as instituições financeiras a obter vantagens competitivas, a melhorar a sua gestão do risco e a reforçar as funções existentes, como a deteção de fraudes e de branqueamento de capitais. Os recentes avanços na formação e implementação de grandes modelos linguísticos e de outras ferramentas de aprendizagem automática e de IA teriam sido impossíveis sem os enormes recursos informáticos disponíveis nos ambientes de computação em nuvem.[28] Qualquer instituição financeira que procure tirar partido da aprendizagem automática ou da IA no futuro terá de contar com uma infraestrutura em nuvem.

c. A importância dos fluxos transfronteiriços de dados no setor dos serviços financeiros mundiais

No sector financeiro, os dados são um ativo essencial que facilita a tomada de decisões financeiras informadas. Num mercado de serviços financeiros cada vez mais globalizado,

---

[23] A título de exemplo, os principais operadores de serviços de computação em nuvem detetaram e atenuaram rapidamente vulnerabilidades de segurança significativas a nível de chip descobertas por um dos seus fornecedores. Jordan Novet, *Amazon, Microsoft, and Google respond to Intel chip vulnerability*, CNBC (Jan. 3, 2018), https://www.cnbc.com/2018/01/03/microsoft-google-respond-to-intel-chip-vulnerability.html.

[24] DEPOSITORY TRUST & CLEARING CORPORATION, *Moving Financial Market Infrastructure to the Cloud* (maio de 2017).

[25] AMAZON WEB SERVICES, *AWS Best Practices for DDoS Resiliency*, 6-15 (2021), https://d1.awsstatic.com/whitepapers/Security/DDoS_White_Paper.pdf.

[26] DEPOSITORY TRUST & CLEARING CORPORATION, *Moving Financial Market Infrastructure to the Cloud* (maio de 2017). Ver também Glen Robinson et al., *Using Amazon Web Services for Disaster Recovery*, AMAZON WEB SERVICES (outubro de 2014), https://d1.awsstatic.com/whitepapers/aws-disaster-recovery.121b65092f931567af5370b47dd12cb18866089c.pdf.

[27] Davies, New *Tools Give Better Picture, Literally, of Financial-System Risk*, WALL STREET JOURNAL (2017), https://www.wsj.com/articles/new-tools-give-better-picture-literally-of-financial-system-risk1493086260?mod=article_inline; John Ashley and Jochen Papenbrock, *Modern Computing Platforms as Key Technology for Central Banks, Financial Supervisors, and Regulators*, IRVING FISHER COMMITTEE ON CENTRAL BANK STATISTICS (2022), https://www.bis.org/ifc/publ/ifcb59_04.pdf; Joshua P. Meltzer and Peter Lovelock, *Regulating for a Digital Economy: Understanding the Importance of Cross-Border Data Flows in Asia*, GLOBAL ECONOMY AND DEVELOPMENT (março de 2018).

[28] Id.

é fundamental um fluxo seguro de dados entre fronteiras para o sucesso das instituições financeiras. Por exemplo, uma instituição financeira que tenha sucursais ou filiais em várias jurisdições pode querer partilhar informações sobre os seus clientes numa determinada jurisdição com uma filial de outra jurisdição, a fim de servir um cliente que tenha mudado de uma jurisdição para outra.[29] As instituições financeiras beneficiam de atividades de análise de mercado ou de diligência devida em que a transferência de dados transfronteiriços é de grande importância.[30] Além disso, as instituições financeiras podem basear-se na transferência internacional de dados relativos ao crédito aos consumidores ou às empresas para efeitos de avaliação da fiabilidade creditícia.[31]

Mais concretamente, as transações que são vitais para o sistema financeiro internacional, incluindo os sistemas de pagamento transfronteiriços, dependem do fluxo internacional de dados.[32] Com o aumento da mobilidade internacional de bens, serviços, capitais e pessoas, a importância das transações transfronteiriças cresceu tanto em volume como em valor.[33] Em 2022, os pagamentos transfronteiriços anuais atingiram cerca de 150 biliões de dólares.[34] E, ao longo de 2023, os créditos malparados financeiros transfronteiriços aumentaram mais de 2 biliões de dólares.[35]

O surgimento e a adoção generalizados da tecnologia de nuvem criaram novas oportunidades para as instituições financeiras beneficiarem dos fluxos de dados transfronteiriços. Embora as infraestruturas dos principais operadores de serviços de computação em nuvem estejam amplamente distribuídas pelas regiões geográficas, não possuem centros de dados em todas as jurisdições.[36] Para explorar os benefícios da tecnologia de computação em nuvem, as instituições financeiras podem ter de transferir dados para outra jurisdição. Por exemplo, os recentes avanços de alto nível nos domínios da análise de dados e da IA são muito promissores para o setor financeiro. Os bancos multinacionais recolhem informações pormenorizadas sobre o comportamento dos seus clientes e utilizam a análise de grandes volumes de dados ou a IA para desenvolver serviços adaptados, como alertas personalizados e uma deteção de fraudes mais eficaz.[37] Estes domínios dependem do processamento de volumes maciços de dados para formação e produção de conhecimentos úteis, exigindo o acesso a recursos informáticos que só estão disponíveis nos maiores operadores de serviços de

[29] Peter P. Swire and Robert E. Litan, *None of Your Business: World Data Flows, Electronic Commerce, and the European Privacy Directive*, BROOKINGS INSTITUTION PRESS (1998).
[30] Id.
[31] Id.
[32] Id.; BANK OF ENGLAND, *Cross-border Payments* (Jan. 31, 2023), https://www.bankofengland.co.uk/payment-and-settlement/cross-border-payments.
[33] BANK OF ENGLAND, *Working together to enhance cross-border payments - speech by Victoria Cleland* (22 de novembro 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., *On the cusp of the next payments era: Future opportunities for banks*, MCKINSEY & COMPANY (18 de setembro de 2023), https://www.mckinsey.com/industries/financial-services/our-insights/the-2023-mckinsey-global-payments-report#/.
[35] BANK FOR INTERNATIONAL SETTLEMENTS, *Locational banking statistics, BIS WS_LBS_D_PUB 1.0 (data set)* (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 and Alan McQuinn, *Cross-Border Data Flows Enable Growth in All Industries*, INFORMATION TECHNOLOGY & INNOVATION FOUNDATION (fevereiro de 2015), https://www2.itif.org/2015-cross-border-data-flows.pdf.
[37] Id.

computação em nuvem e que podem não estar localizados na jurisdição nacional de uma instituição financeira.[38]

As restrições às transferências transfronteiriças de dados, que aumentaram significativamente nos últimos anos, prejudicam, por conseguinte, a capacidade de as instituições financeiras competirem no mercado mundial dos serviços financeiros e dele tirarem partido. Os requisitos de localização de dados limitam a sua capacidade de melhor servir os seus clientes. E ao limitarem a oportunidade de tirar partido da tecnologia de nuvem, esses requisitos impedem o seu acesso a tecnologias - como a análise de dados e a IA - que prometem transformar o setor financeiro. Como tal, é fundamental que as autoridades reguladoras, incluindo as financeiras, ponderem as justificações para as restrições à transferência transfronteiriça de dados financeiros em função dos seus custos significativos.

PARTE II: COMPREENDER OS REQUISITOS DE LOCALIZAÇÃO DE DADOS

Desde que as empresas utilizam a tecnologia para a transferência transfronteiriça de dados, as entidades reguladoras impuseram regras à forma de o fazer. Paralelamente ao aumento do fluxo internacional de dados, aumentaram também os esforços para o regulamentar. As restrições à transferência de dados para fora da jurisdição de origem assumem diferentes formas, desde regras que exigem que os dados estejam fisicamente localizados no local de origem até requisitos de armazenamento local "de facto" que impõem condições rigorosas à transferência de dados para fora da jurisdição. As entidades reguladoras citaram vários motivos para impor requisitos de localização de dados, incluindo a privacidade, o desenvolvimento económico, a aplicação da regulamentação e preocupações geopolíticas. No entanto, os requisitos de localização de dados apresentam inconvenientes conceptuais e práticos significativos, sublinhando a importância de atingir estes objetivos de outras formas.

a. Diferentes tipos de requisitos de localização de dados

Os requisitos de localização de dados são muito anteriores à computação em nuvem. As primeiras leis nacionais de proteção de dados, introduzidas no final dos anos 70 e início dos anos 80, exigiam a localização das operações de processamento de dados ou uma autorização prévia para a exportação de dados sensíveis.[39] No entanto, na última década, à medida que tecnologias como a computação em nuvem transformaram a forma como os dados são armazenados, processados e partilhados, proliferaram as restrições à transferência transfronteiriça de dados.[40] De acordo com um estudo, o

[38] John Ashley and Jochen Papenbrock, *Modern Computing Platforms as Key Technology for Central Banks, Financial Supervisors, and Regulators*, IRVING FISHER COMMITTEE ON CENTRAL BANK STATISTICS (2022), https://www.bis.org/ifc/publ/ifcb59_04.pdf; Joshua P. Meltzer and Peter Lovelock, *Regulating for a Digital Economy: Understanding the Importance of Cross-Border Data Flows in Asia*, GLOBAL ECONOMY AND DEVELOPMENT (março de 2018).
[39] Christopher J. Millard, *Legal Protection of Computer Programs and Data*, 14(1-2) INTERNATIONAL JOURNAL OF LEGAL INFORMATION 74-75 (1985).
[40] EUROPEAN CENTRE FOR INTERNATIONAL POLITICAL ECONOMY, *Restrictions on Cross-Border Data Flows: A Taxonomy* (2017); INFORMATION TECHNOLOGY AND INNOVATION FOUNDATION (2021).

número de países que impõem restrições ao fluxo transfronteiriço de dados quase duplicou entre 2017 e 2021.[41]

Estas restrições variam consoante o país, quer em termos do seu âmbito como na forma como limitam as transferências transfronteiriças de dados. Algumas restrições aplicam-se a quaisquer dados que tenham sido gerados num país; outras aplicam-se apenas a determinadas categorias de dados, como dados financeiros, ou a setores ou entidades económicas específicas. Nalgumas jurisdições, por exemplo, os reguladores financeiros impuseram requisitos de localização de dados às instituições financeiras sem que existissem quaisquer restrições gerais à transferência de dados nessas jurisdições.[42]

No que diz respeito ao conteúdo, os requisitos de localização de dados podem ser divididos em três grandes categorias: (1) regras locais explícitas de armazenamento ou processamento de dados, que obrigam a que os dados provenientes de um país sejam armazenados ou processados nessa jurisdição; (2) regras de "espelhamento de dados", que permitem que os dados sejam transferidos para o estrangeiro desde que uma cópia desses dados seja armazenada localmente; e (3) regras que colocam restrições condicionais à transferência de dados para o estrangeiro. Dependendo do grau de exigência dessas condições, quando o custo do cumprimento é proibitivo, estas equivalem a requisitos efetivos de armazenamento local.

As regras que obrigam ao armazenamento ou processamento de dados exclusivamente local são a forma mais rigorosa de requisito de localização de dados. A República Popular da China, por exemplo, exige que os "operadores de infraestruturas críticas de informação" armazenem localmente na China Continental as informações pessoais e outros "dados importantes" recolhidos e gerados na China (embora os dados possam ser transferidos para o estrangeiro em determinadas circunstâncias). [43] Aplicam-se restrições mais rigorosas aos dados financeiros: o Banco Popular da China exige que praticamente todos os dados pessoais recolhidos no âmbito da prestação de serviços financeiros sejam armazenados, processados e analisados na China continental.[44] A Turquia exige que uma grande variedade de empresas e organizações - incluindo empresas cotadas na bolsa, fundos de pensões, bancos e reguladores e infraestruturas do mercado financeiro - localizem os seus sistemas de TI ativos e de backup no país.[45] Outras jurisdições impõem requisitos de localização de dados a tipos específicos de entidades ou infraestruturas: A Venezuela, por exemplo, exige que a infraestrutura tecnológica para o processamento de pagamentos esteja localizada no país.[46] Também o Banco Central da Nigéria exige que as transações de pagamento nacionais, incluindo

[41] Id.
[42] Javier López González, Francesca Casalini and Juan Porras, *A Preliminary Mapping of Data Localisation Measures*, ORGANIZATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT TRADE POLICY PAPERS, No. 262 (2022), https://www.oecd-ilibrary.org/trade/a-preliminary-mapping-of-data-localisation-measures_c5ca3fed-en.
[43] Lei da Cibersegurança, artigo 37.º; Lei da Proteção de Dados Pessoais.
[44] Artigo 6.º, Aviso n.º 17 (2011).
[45] CAPITAL MARKETS BOARD, *Communique on the Management of Information Systems*, VII-128.9 (2018) (publicly traded companies and financial markets regulators and infrastructures); BANKING REGULATORY AND SUPERVISORY AUTHORITY, *Regulation on Information Systems and Electronic Banking Services of Banks* (2020) (banks).
[46] Nigel Cory and Luke Dascoli, *How Barriers to Cross-Border Data Flows Are Spreading Globally, What They Cost, and How to Address Them*, Information Technology and Innovation Foundation (julho de 2021).

as transações em pontos de venda e caixas automáticos, sejam encaminhadas internamente para troca entre emissores e adquirentes nigerianos.[47]

Os requisitos de "espelhamento de dados" são menos restritivos do que as regras de armazenamento de dados apenas local, uma vez que apenas exigem que seja mantida uma cópia dos dados em servidores ou centros de dados locais, para garantir a resiliência operacional em caso de falha ou outra perturbação. Isto significa que os dados podem ser transferidos e tratados no estrangeiro, desde que seja mantida uma cópia dos dados a nível local. No entanto, o requisito de manter uma cópia redundante dos dados a nível local aumenta o custo relativo do armazenamento de dados no estrangeiro, pelo que, na prática, pode ter o mesmo efeito que as regras de armazenamento exclusivamente local.[48] O México exige que certas instituições financeiras, como bancos e empresas fintech, que armazenam dados em centros de dados localizados fora do México, mantenham cópias dos registos contabilísticos e transacionais localmente, de forma a garantir a continuidade operacional.[49] Também o Chile exige que os bancos que terceirizam volumes de trabalho críticos no exterior, inclusive por meio do uso de serviços de nuvem, mantenham um centro de processamento de dados local para fins de contingência.[50]

Há outras jurisdições que impõem restrições condicionais às transferências internacionais de dados. Estas restrições condicionais assumem várias e diferentes formas. Alguns países exigem que os dados só sejam transferidos para outra jurisdição que tenha em vigor regras de proteção de dados equivalentes ou que a proteção de dados seja assegurada por contrato. Por exemplo, a lei de proteção de dados do Brasil só permite transferências internacionais de dados pessoais se o país destinatário proporcionar um nível "adequado" de proteção de dados ou se estiverem em vigor determinadas disposições contratuais.[51] Outras jurisdições exigem que as empresas obtenham o consentimento das entidades reguladoras ou dos clientes antes de transferirem dados para o estrangeiro. A Arábia Saudita, por exemplo, exige que os dados pessoais sejam armazenados e tratados localmente, a menos que tenha sido obtida uma aprovação por escrito da autoridade reguladora competente.[52] Também a título de exemplo, os reguladores dos mercados bancários e de capitais do Panamá exigem que as entidades regulamentadas obtenham aprovação prévia para a utilização de serviços de computação em nuvem estrangeiros operados por terceiros.[53] As instituições financeiras mexicanas estão sujeitas a requisitos semelhantes.[54]

[47] CENTRAL BANK OF NIGERIA, *Guidelines on Point of Sale Card Acceptance Services* 4.4.8.
[48] Id.
[49] Electronic payment funds institutions (Fintechs), Article 49, IV; Banks (Annex 52(I)(e)); Brokerage houses, Annex 12(I)(e). Adicionalmente, as instituições financeiras mexicanas que utilizam serviços em nuvem só podem ligar-se ao Sistema de Pagamentos Eletrónicos Interbancários (SPEI) utilizando centros de dados locais.
[50] Circular Banking 2409/Financial 798 Chapter 20-7. Os bancos só podem subcontratar serviços de processamento de dados a jurisdições que tenham uma classificação de risco de país com grau de investimento e proteção jurídica adequada para a segurança dos dados pessoais.
[51] Law on General Data Protection, Chapter V – International Data Transfer. Ver também Peru's draft regulation on data protection.
[52] National Data Governance Interim Regulations, Section 5.4 (2020).
[53] Acuerdo No. 003-2012; Acuerdo No. 005-2018.
[54] Ver, por exemplo, Electronic payment funds institutions (Fintechs), Article 49, VIII.

b. Razões para os requisitos de localização de dados

Há uma grande variedade de motivações para as políticas de localização de dados. Uma preocupação comum é o facto de os dados transferidos para o estrangeiro, especialmente dados pessoais sensíveis como os dados financeiros, por exemplo, não estarem adequadamente protegidos contra potenciais violações da segurança ou contra o acesso de governos estrangeiros.[55] Por outro lado, os reguladores temem a indisponibilidade de dados armazenados no estrangeiro em caso de perturbação.[56] De acordo com este argumento, é necessário que o armazenamento de dados seja local para proteger os dados contra intrusões indesejadas e interrupções imprevistas.

Para além das alegadas preocupações com a privacidade e a disponibilidade, os países associam os requisitos de localização de dados ao conceito alargado de "soberania digital". No contexto europeu, a soberania digital foi definida como a "capacidade de agir de forma independente no mundo digital", em relação "quer aos mecanismos de proteção quer às ferramentas ofensivas para promover a inovação digital".[57]

Assim, alguns países justificaram os requisitos de localização de dados com base no facto de o acesso direto às empresas poder facilitar a aplicação de leis, como as leis fiscais e de combate ao branqueamento de capitais.[58] Quando os dados estão localizados no estrangeiro, as autoridades judiciais receiam dificuldades de acesso aos dados. Este argumento é particularmente relevante para setores, como o setor dos serviços financeiros, que estão sujeitos a requisitos de divulgação e conservam dados que são muito visados pelas autoridades responsáveis pela aplicação da lei. O armazenamento de dados local pode facilitar a vigilância e outras divulgações involuntárias de dados pelas entidades regulamentadas. No entanto, esta lógica contraria, de certo modo, o argumento da privacidade a favor da localização de dados.[59]

Os países também introduzem requisitos de localização de dados com o objetivo de incentivar o investimento nos seus setores locais de tecnologia de informação, outro objetivo relacionado com a noção de soberania digital. Se as empresas forem obrigadas a armazenar e processar dados localmente, serão forçadas a investir em servidores e centros de dados locais. Este investimento, em teoria, poderia criar benefícios indiretos para o setor local de alta tecnologia.[60] Para além dos benefícios económicos do investimento nacional em infraestruturas tecnológicas como os centros de dados, alguns governos consideram os centros de processamento de dados locais como infraestruturas críticas necessárias para a segurança e soberania nacionais.[61] Além disso, a interrupção

---

[55] Christopher Millard, *Forced Localization of Cloud Services: Is Privacy the Real Driver?*, Cloud and the Law (2015).
[56] Id.
[57] EUROPEAN PARLIAMENTARY RESEARCH SERVICE, *Digital sovereignty for Europe* (julho de 2020), https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651992/EPRS_BRI(2020)651992_EN.pdf.
[58] INSTITUTE OF INTERNATIONAL FINANCE, *Data Flows Across Borders: Overcoming Data Localization Restrictions* (março de 2019).
[59] Christopher Millard, *Forced Localization of Cloud Services: Is Privacy the Real Driver?*, Cloud and the Law (2015).
[60] INSTITUTE OF INTERNATIONAL FINANCE, *Data Flows Across Borders: Overcoming Data Localization Restrictions* (março de 2019).
[61] CENTER FOR STRATEGIC AND INTERNATIONAL STUDIES, *The Real National Security Concerns over Data Localization* (2021); ASSOCIATION FOR FINANCIAL MARKETS IN EUROPE, *European Cybersecurity Certification Scheme for Cloud Services (EUCS) – Solutions on the Issue of Independence to Non-EU Law* (13 de março de 2023), https://www.afme.eu/Portals/0/DispatchFeaturedImages/230310_AFME%20Comments%20on%20EUCS_FINAL.pdf;

de certos serviços críticos, como os serviços financeiros, poderia prejudicar gravemente o funcionamento básico do país, o que justifica requisitos especiais para garantir a resiliência e a disponibilidade destes serviços.[62]

c. Custos de localização de dados em geral

Embora estes objetivos políticos sejam legítimos (apesar de potencialmente contraditórios), a utilização dos requisitos de localização de dados com o intuito de lhes poder aceder é provavelmente ineficaz. A localização física dos dados pode ser um fator importante para a sua privacidade, mas não é o mais importante. Do ponto de vista técnico, o acesso físico a um servidor ou a outro dispositivo de armazenamento de dados não é necessário nem suficiente para aceder às informações nele armazenadas. Os dados que não são geridos de forma segura podem ser acedidos mesmo que um utilizador não tenha acesso físico a um servidor. E se os dados estiverem encriptados de forma segura, o acesso físico por si só não os tornará acessíveis de forma inteligível. Além disso, se os dados forem encriptados de forma segura, o acesso físico aos dados não dará origem a riscos de privacidade, independentemente do local onde estejam fisicamente armazenados.[63]

O armazenamento local de dados não melhora necessariamente a segurança ou a disponibilidade dos dados. O recurso a uma infraestrutura externa de um grande operador de serviços de computação em nuvem pode oferecer maior segurança e disponibilidade. As economias de escala permitem que os grandes operadores de serviços de computação em nuvem façam investimentos nas capacidades de resiliência e cibersegurança que excedem em muito as disponíveis numa infraestrutura tecnológica local.[64] Além disso, os principais operadores de serviços de computação em nuvem garantem a segurança e a disponibilidade dos dados através da distribuição de dados e processos entre vários sistemas e locais, tornando-os menos vulneráveis a uma violação ou interrupção.[65] Ao obrigar a que os dados permaneçam numa determinada jurisdição, os requisitos de localização inibem a utilização dessa infraestrutura distribuída. Adicionalmente, ao aumentar o número e a localização de centros de dados que as empresas que operam em diferentes jurisdições tem de equipar e manter, os requisitos de localização de dados também aumentam o risco e a complexidade das suas operações de cibersegurança. Exigir que qualquer empresa multinacional crie e defenda várias versões dos seus sistemas em diferentes locais corresponde a mais hardware, mais funcionários e mais fornecedores, aumentando a área de superfície para potenciais perturbações ou ciberataques.[66]

A obrigatoriedade de armazenamento local de dados também não elimina o risco de acesso por parte de governos estrangeiros. A legislação dos EUA, por exemplo,

---

INTERNATIONAL ORGANIZATION OF SECURITIES COMMISSIONS, *Multilateral Memorandum of Understanding Concerning Consultation and Cooperation and the Exchange of Information* (maio de 2012), https://www.iosco.org/library/pubdocs/pdf/IOSCOPD386.pdf.

[62] Id.

[63] Christopher Millard, *Cloud Computing Law*, OXFORD UNIVERSITY PRESS (2013).

[64] Ver acima, Part I.b.

[65] Id.

[66] Anupam Chander, *Is Data Localization a Solution for Schrems II?*, 23 JOURNAL OF INTERNATIONAL ECONOMIC LAW 771-784 (2020), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3662626; Blancco, *The High Cost of Cluttered Data Centers* (2019).

determina que os operadores de serviços de computação em nuvem sujeitos à jurisdição dos EUA não podem evitar o cumprimento de um pedido de acesso das autoridades responsáveis pela aplicação da lei simplesmente porque os dados estão localizados numa jurisdição fora dos EUA.[67] O armazenamento local de dados também não garante a supervisão regulamentar local ou o acesso às autoridades policiais locais. Os operadores de serviços em nuvem sediados nos EUA, por exemplo, estão geralmente impedidos de partilhar dados com governos estrangeiros, independentemente da localização dos dados. Do ponto de vista da legislação dos EUA, não importa se os dados são armazenados num centro de dados dos EUA ou num localizado noutro país. A melhor forma de os reguladores e as autoridades responsáveis pela aplicação da lei garantirem o acesso aos dados não é a localização, mas sim através de acordos bilaterais ou multilaterais de partilha de dados. Algumas jurisdições trabalharam com governos estrangeiros para facilitar o acesso aos dados dos seus próprios cidadãos armazenados no estrangeiro. Vários países, por exemplo, celebraram acordos bilaterais com os Estados Unidos para que os operadores de serviços de computação em nuvem dos EUA possam cumprir os pedidos legais de dados eletrónicos emitidos pelo outro país, sem necessidade de um mandado judicial.[68]

Mesmo que a localização de dados possa oferecer alguns benefícios económicos diretos, esses benefícios são limitados. Embora a localização de dados possa atrair investimentos em infraestruturas tecnológicas nacionais, como centros de dados, os benefícios de repercussão são mínimos porque estes centros são altamente automatizados e exigem relativamente poucos empregados permanentes.[69] Basicamente, a concorrência pela localização da infraestrutura dos principais operadores de serviços em nuvem é insustentável: não é economicamente viável que estes construam centros de dados, que custam centenas de milhões de dólares ou mais,[70] em *todas as* jurisdições. Os principais operadores de serviços em nuvem podem optar por não desenvolver uma infraestrutura local. Nesse caso, os requisitos de localização de dados prejudicarão a economia local, impedindo que as empresas nacionais beneficiem da melhor infraestrutura tecnológica dos grandes operadores de serviços de computação em nuvem. Isto traduz-se em custos tecnológicos mais elevados: de acordo com um estudo, os requisitos de localização de dados podem aumentar os custos de alojamento de dados entre 30 a 60%.[71] O aumento dos custos implica uma redução da capacidade de as empresas locais competirem à escala mundial e resulta em menos inovação para os clientes locais. Além disso, o aumento do carácter restritivo das regras de

[67] CLOUD Act.
[68] Id.
[69] Nigel Cory, *The False Appeal of Data Nationalism: Why the Value of Data Comes from How It's Used, Not Where It's Stored*, Information Technology and Innovation Foundation (abril de 2019).
[70] Matt Vincent, *Hyperscale Cloud Giants' Data Center Mega Deals Keep Sprouting Zeroes*, Data Center Frontier (1 de abril de 2024), https://www.datacenterfrontier.com/hyperscale/article/55001427/hyperscale-cloud-giants-data-center-mega-deals-keep-sprouting-zeroes; Amazon Web Services, AWS to Launch an Infrastructure Region in Mexico (26 de fevereiro de 2024), https://press.aboutamazon.com/2024/2/aws-to-launch-an-infrastructure-region-in-mexico.
[71] LEVIATHAN SECURITY GROUP, *Quantifying the Cost of Forced Localization* (2015), https://static1.squarespace.com/static/6128b1eb2eb2cf15b7a35a2f/t/65af6b484ec970386fd56386/1705995081389/Quantifying%2Bthe%2BCost%2Bof%2BForced%2BLocalization.pdf.

transferência de dados de um país tem sido associado a reduções significativas da produtividade e a aumentos de preços nas indústrias afetadas.[72]

Algumas jurisdições reconheceram que a confidencialidade, a integridade e a disponibilidade dos dados podem ser mais facilmente alcançadas através da utilização de servidores em nuvem localizados no estrangeiro.[73] A Estónia, por exemplo, criou uma "embaixada de dados" virtual que utiliza serviços de computação em nuvem estrangeiros para assegurar a continuidade dos dados considerados críticos para o funcionamento do Estado. Outros governos reviram os requisitos de localização de dados existentes, tendo em conta os custos que lhes estão associados. A Indonésia, por exemplo, reduziu os seus rigorosos requisitos de localização de dados, que anteriormente se aplicavam a qualquer fornecedor de "serviços públicos" eletrónicos, aplicando-os apenas a entidades governamentais.[74] E a Ucrânia levantou os requisitos de localização de dados para poder transferir dados críticos do governo e do setor privado, incluindo os dados do seu maior banco privado, para servidores em nuvem estrangeiros seguros antes da invasão da Rússia.[75]

PARTE III: REQUISITOS DE LOCALIZAÇÃO DE DADOS E O SETOR FINANCEIRO

A proliferação de requisitos de localização de dados, que impedem o fluxo de dados através das fronteiras, levanta questões específicas para os serviços financeiros. A transferência transfronteiriça de dados no interior de entidades multinacionais e entre entidades de diferentes jurisdições é fundamental para o funcionamento do setor financeiro mundial. As grandes instituições financeiras dependem do livre fluxo de dados para operarem sem problemas em diferentes jurisdições em todo o mundo. E as instituições financeiras locais de menor dimensão dependem dessas instituições de maior dimensão para prestar serviços internacionais aos seus próprios clientes, que - num mundo em que o comércio global é a norma - podem necessitar de serviços financeiros onde a instituição local não opera.

Um cidadão francês de férias na República Dominicana pode precisar de levantar dinheiro utilizando uma máquina ATM local; ou um vendedor peruano que venda produtos no Japão através da Internet pode querer receber o pagamento em moeda estrangeira. Em ambos os casos, a transação só pode ser processada, e o dinheiro transferido, se os dados atravessarem fronteiras internacionais. A autorização para o

---

[72] INFORMATION TECHNOLOGY AND INNOVATION FOUNDATION (2021); EUROPEAN CENTRE FOR INTERNATIONAL POLITICAL ECONOMY (2014); Martina F. Ferracane, *The Costs of Data Protectionism*, BIG DATA AND GLOBAL TRADE LAW (9 de julho de 2021). A adoção da nuvem também tem sido associada a reduções de emissões, uma vez que a atividade dos centros de dados é transferida de servidores locais menos eficientes para servidores de nuvem pública mais recentes e mais eficientes. FTI Consulting, *Economic Impact of Cloud Adoption in Six Latin American Countries* (Oct. 20, 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-Governance*, https://e-estonia.com/solutions/e-governance/data-embassy/.

[74] Government Regulation No. 71 (2019).

[75] Ryan White, *How the cloud saved Ukraine's data from Russian attacks*, C4ISRNET (22 de junho de 2022), https://www.c4isrnet.com/2022/06/22/how-the-cloud-saved-ukraines-data-from-russian-attacks/; David E. Sanger, *New Biden Cybersecurity Strategy Assigns Responsibility to Tech Firms*, New York Times (Mar. 2, 2023), https://www.nytimes.com/2023/03/02/us/politics/biden-cybersecurity-strategy.html.

levantamento em ATM deve provir de um sistema informático em França, o que exige a transferência dos dados do cliente para o estrangeiro. A venda online implica a transferência de dados do cliente e do vendedor entre bancos e processadores de pagamentos localizados em ambas as jurisdições.

Estas são apenas algumas das formas em que os fluxos de dados transfronteiriços são fundamentais para o funcionamento do setor financeiro. Os requisitos de localização de dados limitam a capacidade das instituições financeiras de operarem além fronteiras, inibindo a sua capacidade de satisfazer as necessidades dos seus clientes e até a capacidade de os reguladores financeiros levarem a cabo a supervisão. Além disso, impedem as instituições financeiras de tirar partido das novas oportunidades, como a análise de dados em grande escala e a IA, proporcionadas pela tecnologia de computação em nuvem.

a. A regulamentação complexa em matéria de dados aumenta os custos e asfixia a concorrência

Para além das restrições substantivas no que respeita à transferência transfronteiriça de dados, as regras de localização de dados podem também ser difíceis de implementar e cumprir. Por um lado, pode haver uma incerteza considerável quanto ao âmbito das regras de proteção da privacidade dos dados. Pode não ser claro quais as entidades que estão sujeitas a elas e a que dados se aplicam.[76] Embora as regras de localização de dados façam frequentemente a distinção entre dados pessoais e não pessoais, a linha que os separa nem sempre é clara.[77] As informações sobre indivíduos específicos, como os principais empregados (dados pessoais), são por vezes incorporadas em informações sobre empresas (dados não pessoais).[78] Além disso, as ferramentas sofisticadas de análise de dados facilitam como nunca a interferência nas informações pessoais a partir de dados supostamente não pessoais.[79] Consequentemente, os requisitos de localização que aparentemente se aplicam apenas aos dados pessoais podem, na prática, limitar a transferência de todos os dados, sejam eles pessoais ou não. Outra fonte de complexidade é o facto de as instituições financeiras poderem estar sujeitas a regras específicas de localização de dados que complementam as leis gerais de proteção de dados numa determinada jurisdição.[80] A combinação de regras gerais de proteção de dados com regras específicas aplicáveis aos serviços financeiros pode dar origem a custos de compliance significativos.

Imagine-se uma instituição financeira global que está a ponderar abrir uma sucursal ou filial numa jurisdição que exige o armazenamento local (ou cópias) de determinados

[76] Dmitry Kurochkin, Marat Agabalyan and Saglara Ildzhirinova, *Russia's New Server Localization Law: Implications for Foreign Companies*, Bloomberg BNA WORLD DATA PROTECTION REPORT (fevereiro de 2015), https://news.bloomberglaw.com/privacy-and-data-security/russias-new-server-localization-law-implications-for-foreign-companies.
[77] Michèle Finck and Frank Pallas, *They Who Must Not Be Identified – Distinguishing Personal from Non-Personal Data Under the GDPR*, 10(1) International Data Privacy Law 11-36 (fevereiro de 2020), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3462948.
[78] Peter P. Swire and Robert E. Litan, *None of Your Business: World Data Flows, Electronic Commerce, and the European Privacy Directive*, BROOKINGS INSTITUTION PRESS (1998).
[79] Michèle Finck and Frank Pallas, *They Who Must Not Be Identified – Distinguishing Personal from Non-Personal Data Under the GDPR*, 10(1) International Data Privacy Law 11-36 (fevereiro de 2020), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3462948.
[80] Ver acima, Parte II.a.

dados. Para abrir a sucursal, a instituição financeira teria de implementar uma solução operacional alternativa, como a utilização de um fornecedor local de software ou de um centro de dados para processar e armazenar dados nessa jurisdição. Estabelecer e manter esta solução local exigirá tempo e dinheiro, tanto a nível operacional como em termos de garantir a conformidade com os requisitos de localização de dados aplicáveis.[81] Esses custos adicionais serão obrigatoriamente transferidos para os clientes locais da instituição financeira, deixando-os em pior situação do que os seus clientes noutras jurisdições.

Em alternativa, a instituição financeira pode decidir que o custo de estabelecer uma solução local é proibitivo e renunciar totalmente à sucursal ou filial.[82] Mesmo que o custo da solução local não a exclua, a instituição financeira pode descobrir que não existe uma solução local que cumpra as suas próprias normas - ou as normas impostas pelo seu país de origem - em termos de segurança ou resiliência dos dados.[83] Ou pode decidir que é demasiado complicado desenvolver políticas de compliance e de gestão de riscos que sejam adaptadas aos requisitos específicos dessas jurisdições.[84] Por qualquer uma destas razões, os requisitos de localização de dados podem efetivamente excluir as instituições financeiras do mercado local, sufocando a concorrência e privando os residentes dessa jurisdição do acesso a serviços importantes.[85]

Os requisitos de localização de dados podem também inibir a capacidade das instituições financeiras locais servirem os clientes que viajam ou vivem no estrangeiro. As restrições à transferência transfronteiriça de dados podem dificultar a consolidação e a análise dos dados dos clientes provenientes de diferentes locais, o que é fundamental para a gestão do risco, a deteção de fraudes e a análise dos clientes. Se os dados dos clientes não puderem ser facilmente partilhados ou integrados além fronteiras, as instituições financeiras locais terão dificuldade em servir os seus clientes noutras jurisdições. Os requisitos de localização podem também impedir que as instituições financeiras tirem partido da infraestrutura tecnológica global, limitando a sua capacidade de oferecer serviços consistentes e eficientes aos clientes no estrangeiro.[86]

b. A localização de dados pode comprometer a cibersegurança e a resiliência

Os defensores dos requisitos de localização de dados apelam frequentemente ao alegado reforço da cibersegurança e da resiliência operacional. Estes argumentos a favor da localização de dados são erróneos. Como já foi referido, os operadores globais de serviços de computação em nuvem beneficiam de economias de escala que lhes

[81] Ver, por exemplo, Prasad, *Mastercard Begins Deleting Indian Transactions Data Stored Overseas* (2019).
[82] DANIEL CASTRO AND ALAN MCQUINN, *Cross-Border Data Flows Enable Growth in All Industries*, INFORMATION TECHNOLOGY & INNOVATION FOUNDATION (FEVEREIRO DE 2015), https://www2.itif.org/2015-cross-border-data-flows.pdf.
[83] TechRadar Pro, *The high costs of storing data locally in a cloud native era*, TECHRADAR (FEB. 22, 2019), https://www.techradar.com/news/the-high-costs-of-storing-data-locally-in-a-cloud-native-era.
[84] International Regulatory Strategy Group, *How the Trend Towards Data Localisation is Impacting the Financial Services Sector* (dezembro de 2020).
[85] Margaret Doyle et al., *How to flourish in an uncertain future: Open banking and PSD2* (2017), https://www2.deloitte.com/content/dam/Deloitte/cz/Documents/financial-services/cz-open-banking-and-psd2.pdf.
[86] Daniel Castro and Alan McQuinn, *Cross-Border Data Flows Enable Growth in All Industries*, INFORMATION TECHNOLOGY & INNOVATION FOUNDATION (fevereiro de 2015), https://www2.itif.org/2015-cross-border-data-flows.pdf.

permitem fazer investimentos substancialmente maiores na segurança e disponibilidade dos dados, comparativamente a operadores de infraestruturas locais ou regionais.[87]

A natureza distribuída do armazenamento e do processamento em nuvem, bem como os maiores recursos de computação disponíveis junto dos principais operadores de nuvem, em comparação com as instituições financeiras individuais ou os operadores de tecnologia locais, traduzem-se numa maior resiliência operacional. Os operadores de serviços de computação em nuvem possibilitam que uma instituição financeira aumente automaticamente a sua escala e mantenha a disponibilidade face a um ciberataque que sobrecarregue a infraestrutura tecnológica disponível localmente.[88] Do mesmo modo, ao permitir que as instituições financeiras distribuam processos e dados por diferentes centros de dados, a nuvem permite-lhes criar aplicações que estão constantemente online, mesmo que um determinado centro de dados - ou toda uma região - sofra uma perturbação.[89]

As empresas tecnológicas locais podem não dispor de recursos comparáveis aos dos grandes operadores de serviços de computação em nuvem, cujas infraestruturas são construídas de acordo com os mais elevados padrões de cibersegurança.[90] Mesmo os requisitos de localização que obrigam as instituições financeiras a manter uma cópia local dos dados podem comprometer a sua segurança, aumentando o número de pontos de acesso aos dados e, por conseguinte, a probabilidade de uma violação da cibersegurança.[91] Os requisitos de localização de dados também podem fazer com que as instituições financeiras se deparem com mais dificuldades para identificar, prevenir e mitigar ciberameaças, ao limitar a sua capacidade de partilhar informações de uma jurisdição com os reguladores de outra jurisdição.[92]

c. A localização de dados pode inibir a supervisão regulamentar financeira

Facilitar a supervisão regulamentar e a aplicação da lei é outra justificação comummente invocada para os requisitos de localização de dados. Muitas entidades reguladoras financeiras receiam deixar de conseguir aceder aos dados quando estes saírem das fronteiras da sua jurisdição. Como já foi referido, a localização de dados não resolve necessariamente o problema da aplicação da lei ou do acesso regulamentar aos dados.[93] Além disso, é igualmente provável que o contrário seja verdade: os requisitos de localização de dados podem dificultar a supervisão por parte dos reguladores financeiros.

Os requisitos de localização de dados são suscetíveis de provocar, ou encorajar, requisitos recíprocos noutras jurisdições. Assim, mesmo que os requisitos de localização na própria jurisdição de um regulador facilitassem o seu acesso a alguns dados financeiros, requisitos semelhantes noutra jurisdição impediriam o seu acesso a outros

[87] Ver acima, Parte I.b.
[88] Id.
[89] Id.
[90] Id.
[91] Anupam Chander, *Is Data Localization a Solution for Schrems II?*, 23 JOURNAL OF INTERNATIONAL ECONOMIC LAW 771-784 (2020), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3662626 TechRadar Pro, *The high costs of storing data locally in a cloud native era*, TechRadar (22 de fevereiro de 2019), https://www.techradar.com/news/the-high-costs-of-storing-data-locally-in-a-cloud-native-era.
[92] Nigel Cory and Luke Dascoli, *How Barriers to Cross-Border Data Flows Are Spreading Globally, What They Cost, and How to Address Them*, INFORMATION TECHNOLOGY AND INNOVATION FOUNDATION (julho de 2021).
[93] Ver Secção II.c.

dados importantes. Quando uma transação internacional envolve duas jurisdições que impõem requisitos de localização de dados, a entidade reguladora financeira de cada jurisdição só teriam uma visão de metade da transação. Este facto inibiria o exercício de funções básicas de supervisão financeira, como a luta contra o branqueamento de capitais e a deteção de fraudes, bem como mandatos mais amplos, como a supervisão da estabilidade financeira.

d. Vantagens da transferência de dados para as instituições financeiras

Na ausência de requisitos de localização de dados, as instituições financeiras podem aproveitar a infraestrutura de tecnologia de nuvem fora da jurisdição para reduzir os custos, aumentar a segurança dos dados e a resiliência operacional e oferecer melhores serviços aos clientes. Isto é verdade quer a instituição financeira seja uma instituição financeira global que procura entrar num novo mercado local, quer seja uma instituição financeira local que tenta obter acesso a uma melhor infraestrutura tecnológica ou expandir-se globalmente.

Embora muitos clientes de serviços financeiros ainda dependam de uma força de trabalho de escritório e de serviços presenciais, há uma procura crescente de trabalho e serviços à distância, impulsionada em parte pela pandemia da COVID-19. A tecnologia de computação em nuvem facilita o trabalho à distância e a prestação de serviços digitais, bem como outros serviços à distância. Instituições financeiras como a Societé Generale, por exemplo, confiaram em soluções de gestão de dispositivos baseadas na nuvem para apoiar milhares de trabalhadores remotos durante os confinamentos relacionados com a COVID-19.[94] Um banco multinacional sediado na Europa contou com a sua infraestrutura de nuvem para continuar a servir os clientes no Brasil durante a pandemia, o que só foi possível devido à ausência de requisitos de localização de dados.[95] Para além das mudanças provocadas pela pandemia na força de trabalho e no serviço ao cliente, as instituições financeiras continuaram a confiar na tecnologia de nuvem para oferecer serviços digitais inovadores aos clientes. Por exemplo, o Itaú Unibanco, a maior instituição bancária da América Latina, aproveitou a tecnologia em nuvem para implementar o Pix, o serviço de pagamento digital instantâneo exigido pelo Banco Central do Brasil.[96] Da mesma forma, o BBVA confiou na tecnologia baseada na nuvem para permitir pagamentos contactless de forma segura, cumprindo os regulamentos específicos de cada país - tornando-se a primeira instituição financeira a oferecer pagamentos contactless no Peru, Argentina e Colômbia.[97]

As instituições financeiras podem também utilizar a infraestrutura de nuvem offshore para lidar com as perturbações do mercado financeiro que, de outra forma, poderiam sobrecarregar a sua infraestrutura tecnológica. A computação em nuvem permite que os

[94] MICROSOFT INTUNE, *Société Générale leads the way to the cloud, optimizing user experience and secure device management* (14 de outubro de 2022), https://customers.microsoft.com/en-us/story/1558831416191995829-societegenerale-banking-and-capital-markets-cloud.
[95] INSTITUTE OF INTERNATIONAL FINANCE, *Cloud Computing: A Vital Enabler in Times of Disruption* (junho de 2020).
[96] BNAMERICAS, *Brazil's Itaú to migrate most of its systems to AWS cloud* (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 Accelerates Pix Instant Payment System Development Using AWS* (2022), https://aws.amazon.com/solutions/case-studies/itau-pix/.
[97] AMAZON WEB SERVICES, *BBVA Uses AWS CloudHSM to Enable Fully Compliant NFC Payments* (2021), https://aws.amazon.com/solutions/case-studies/bbva/?did=cr_card&trk=cr_card.

utilizadores aumentem automaticamente a sua capacidade sem qualquer presença física no local. Isto pode ajudar as instituições financeiras a reagir a situações de tensão no mercado, como picos inesperados nos volumes de transações ou na volatilidade do mercado.[98] A escalabilidade automática da nuvem, bem como a maior capacidade de processamento em comparação com a infraestrutura tecnológica tradicional, também permite às instituições financeiras introduzir e analisar dados em tempo real. As soluções de nuvem permitem, por exemplo, que as instituições financeiras calculem a sua posição de liquidez várias vezes por dia, mesmo em períodos de grande volatilidade do mercado.[99]

Além disso, a tecnologia de computação em nuvem facilita o acesso a tecnologias de ponta, como a análise de grandes volumes de dados e a IA, que dependem dos vastos recursos de computação disponíveis na nuvem. As instituições financeiras mundiais já utilizam ferramentas de IA baseadas em nuvem para funções básicas como o apoio ao cliente.[100] À medida que a aprendizagem automática e as capacidades de IA se desenvolvem, elas serão utilizadas para a análise de dados e outras funções mais críticas, como a gestão de riscos. O HSBC, por exemplo, utiliza ferramentas de modelação do risco baseadas em nuvem para gerir o risco e reportar a atividade comercial e de crédito.[101] O Itaú Unibanco transferiu a sua infraestrutura de aprendizagem automática dos centros de dados locais para a nuvem, a fim de acelerar a implementação e análise de modelos.[102] Estas capacidades sofisticadas, no entanto, só estarão disponíveis para as instituições financeiras autorizadas a aceder a serviços baseados em nuvem que, em muitos casos, dependerão de infraestruturas tecnológicas fora da jurisdição e exigirão a transferência internacional de dados.

Parte IV: Recomendações de Políticas para as Autoridades de Regulamentação Financeira

Os requisitos de localização de dados impõem custos significativos às instituições financeiras e aos clientes que estas servem. Embora sejam frequentemente motivados por objetivos baseados em políticas legítimas, como a proteção de dados sensíveis e a garantia de acesso aos dados para efeitos de supervisão e aplicação da regulamentação, esses objetivos seriam mais bem servidos através de políticas que evitassem esses custos. Os reguladores financeiros devem encontrar um equilíbrio entre as preocupações com as políticas subjacentes aos requisitos de localização de dados e o imperativo de

[98] RISK.NET, *Technology innovation of the year* (fevereiro 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 integrates Microsoft Artificial Intelligence into service channels* (20 de junho de 2023), https://news.microsoft.com/es-xl/picpay-integrates-microsoft-artificial-intelligence-into-service-channels/; Transbank, *Transbank further consolidates its position as a tech company with generative AI* (19 de fevereiro de 2024), https://ir.transbank.cl/en/transbank-further-consolidates-its-position-as-a-tech-company-with-generative-ai; AMAZON WEB SERVICES, *How NatWest Bank Personalizes the Customer Experience Using AWS* (2023), https://aws.amazon.com/solutions/case-studies/natwest/?did=cr_card&trk=cr_card.
[101] GOOGLE CLOUD, *HSBC: Embracing the cloud to lower risk exposure through rapid insight and analysis capabilities*, https://cloud.google.com/customers/hsbc-risk-advisory-tool.
[102] AMAZON WEB SERVICES, *Itaú Improves Speed to Market and Productivity of ML Solutions Using Amazon Web Services* (2024), https://aws.amazon.com/solutions/case-studies/itau-ml-case-study/?did=cr_card&trk=cr_card.

facilitar o fluxo transfronteiriço de dados no setor financeiro, incluindo a utilização de infraestruturas de computação em nuvem fora da jurisdição. Esse equilíbrio será mais facilmente alcançado através de regras que: (1) se concentrem diretamente no alcance dos objetivos dessas políticas, em vez de indiretamente através de requisitos de localização de dados; e (2) abordem objetivos das políticas através da coordenação e cooperação com outros reguladores locais e reguladores de outras jurisdições.

a. Adoção de uma abordagem da proteção de dados baseada em princípios

Obrigar a que os dados permaneçam numa determinada jurisdição não é necessário nem suficiente para manter a sua segurança. Os dados sensíveis que não são geridos de forma segura podem ser comprometidos por alguém que não tenha acesso físico aos mesmos. Por conseguinte, a localização de dados pouco faz para garantir que os dados privados permaneçam privados. Para proteger os dados privados, os reguladores financeiros devem concentrar-se em garantir que os dados são armazenados *de forma segura* - seja localmente ou no estrangeiro. Tal como referido anteriormente, as plataformas dos principais operadores de serviços de computação em nuvem foram concebidas para fornecer às instituições financeiras ferramentas para implementar requisitos de segurança rigorosos, incluindo a encriptação incorporada de dados.

Para atenuar as preocupações de que as instituições financeiras possam transferir dados sensíveis para jurisdições que não protegem a privacidade dos dados, as entidades reguladoras podem exigir que os dados sejam armazenados apenas numa jurisdição que ofereça proteção jurídica dos dados pessoais suficiente. A abordagem das Diretrizes de Privacidade da OCDE à transferência de dados pessoais é instrutiva.[103] Estas orientações, adotadas em 1980 e revistas em 2013, sublinham que a responsabilidade jurídica pelos dados pessoais se aplica independentemente da localização dos dados, quer estejam armazenados localmente ou no estrangeiro. Estipulam também que os países devem abster-se de restringir o fluxo transfronteiriço de dados sempre que existam garantias suficientes que assegurem a proteção dos dados pessoais. Além disso, determinam que as restrições ao fluxo transfronteiriço de dados pessoais devem ser proporcionais aos riscos existentes.[104]

O regulamento de proteção de dados do Brasil adota uma abordagem semelhante. Ele permite a transferência de dados para países com um "nível adequado de proteção" dos dados pessoais e garantias de cumprimento dos direitos e princípios de proteção de dados previstos no regulamento de proteção de dados do Brasil.[105] É importante notar que estas normas não são rígidas, podendo ser satisfeitas de várias formas, nomeadamente através de disposições contratuais específicas ou de códigos de conduta gerais.[106] Isto permite às instituições financeiras flexibilidade para determinar a melhor forma de proteger os dados sensíveis que são transferidos para fora da jurisdição, desde que existam salvaguardas de privacidade suficientes.

---

[103] ORGANIZATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT, *Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data* (2013), https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0188.
[104] Id, Parte IV.
[105] Law on General Data Protection, Section V.
[106] Id.

b. Foco na qualidade da infraestrutura tecnológica e não na sua localização

A localização de dados é frequentemente justificada com base na noção de que o armazenamento local de dados significa que os dados estão mais prontamente disponíveis e são mais resistentes a perturbações. Mas a localização dos dados é apenas um fator que pode afetar a disponibilidade e a resiliência operacional. Uma abordagem que dê prioridade à disponibilidade e à resiliência operacional deve ter em conta os muitos fatores que podem afetar a integridade e a disponibilidade dos dados. Em muitos casos, confiar num grande operador de serviços em nuvem - incluindo a sua infraestrutura fora da jurisdição - proporcionará às instituições financeiras um maior grau de disponibilidade e resiliência do que a infraestrutura local. As entidades reguladoras devem dar às instituições financeiras mais margem de manobra para elas efetuarem a sua própria avaliação no que respeita à resiliência das suas soluções de armazenamento e processamento de dados em caso de perturbações, tendo em conta a natureza e a importância do processo e o potencial da perturbação.

c. Garantia de acesso aos dados para efeitos de supervisão regulamentar e aplicação da lei

A supervisão efetiva das instituições financeiras pode ser conseguida sem necessidade de armazenamento local de dados. Os reguladores financeiros e as autoridades responsáveis pela aplicação da lei podem garantir o acesso aos dados relevantes, quer estejam armazenados localmente ou numa jurisdição diferente. O acesso aos dados armazenados no estrangeiro pode ser conseguido através de acordos com os reguladores financeiros de outras jurisdições. Várias autoridades de regulamentação financeira trabalharam com as suas congéneres estrangeiras para desenvolver quadros jurídicos bilaterais e mecanismos de cooperação transfronteiriça, com o objetivo de permitir fluxos de dados transfronteiriços, assegurando simultaneamente o acesso aos dados para efeitos de supervisão. O Banco Central do Brasil, por exemplo, tem acordos, com o objetivo de facilitar os fluxos de informação de supervisão, com as autoridades de supervisão onde as instituições financeiras brasileiras têm operações no estrangeiro e com aquelas onde as instituições financeiras estrangeiras têm operações no Brasil.[107] Do mesmo modo, o Monetary de Singapura celebrou acordos com os reguladores financeiros dos EUA e do Reino Unido que permitem que as instituições financeiras transfiram além fronteiras dados financeiros, incluindo informações pessoais, desde que os reguladores financeiros tenham acesso total e atempado a esses dados.[108] A nível multilateral, o Memorando de Entendimento Multilateral atualizado, desenvolvido pela Organização Internacional das Comissões de Valores Mobiliários (IOSCO), exige que os

[107] BANCO CENTRAL DO BRASIL, *International MoUs for Supervisory Purposes*, https://www.bcb.gov.br/en/financialstability/supervisionmous.

[108] U.S. DEPARTMENT OF THE TREASURY, *United States – Singapore Joint Statement on Financial Services Data Connectivity* (5 de fevereiro de 2020), https://home.treasury.gov/news/press-releases/sm899; U.S. COMMODITY FUTURES TRADING COMMISSION AND THE MONETARY AUTHORITY OF SINGAPORE, *Cooperation and the Exchange of Information on Financial Technology Innovation* (13 de setembro de 2018), https://www.cftc.gov/sites/default/files/2018-09/cftc-mas-cooparrgt091318_16.pdf; Monetary Authority of Singapore, *Singapore and UK to Enhance Cooperation in Data Connectivity, Talent Development, Green Finance and Cybersecurity* (Jun. 13, 2019), https://www.mas.gov.sg/news/media-releases/2019/singapore-and-uk-to-enhance-cooperation.

signatários partilhem determinadas informações com as entidades reguladoras homólogas.[109]

O acesso a dados relevantes pode também ser assegurado através de acordos contratuais entre as instituições financeiras e os operadores de serviços tecnológicos. Várias jurisdições, por exemplo, exigem que os acordos contratuais de uma instituição financeira com os seus prestadores de serviços garantam que os reguladores financeiros tenham acesso suficiente aos dados para supervisionar a instituição financeira.[110] Estas disposições contratuais geralmente incluem o acesso aos dados das instituições financeiras, bem como a cooperação do operador de serviços com o regulador em relação a pedidos de informação e direitos de acesso para auditorias.[111]

d. Aumento da coordenação a nível local e internacional

A complexa manta de retalhos dos requisitos de localização de dados, tanto no interior das jurisdições como entre jurisdições diferentes, aumenta os custos para as instituições financeiras e asfixia a concorrência que, de outro modo, beneficiaria os seus clientes. Para minimizar a incerteza e alcançar a coerência regulamentar, as entidades reguladoras financeiras devem trabalhar em conjunto com as autoridades locais (como as autoridades responsáveis pela proteção da privacidade e as entidades reguladoras de outros setores), bem como com as suas congéneres estrangeiras, para desenvolver abordagens amplamente coerentes em matéria de transferência de dados que permitam a transferência transfronteiriça de dados e, ao mesmo tempo, resolvam as razões que justificam a localização de dados. Desta forma, minimizam-se as barreiras desnecessárias à transferência de dados, permitindo que as instituições financeiras beneficiem de infraestruturas tecnológicas fora da jurisdição, incluindo a computação em nuvem.

A coordenação internacional pode ocorrer a nível bilateral. Por exemplo, a Austrália e Singapura celebraram um "acordo de economia digital" que permite às empresas, nomeadamente do setor financeiro, transferir dados através das fronteiras sem serem obrigadas a construir ou utilizar centros de dados em qualquer uma das jurisdições. É importante notar que o acordo garante que as regras de proteção da privacidade aplicáveis aos dados pessoais continuam a aplicar-se, sejam os dados armazenados localmente ou em outra jurisdição.[112] Singapura celebrou acordos semelhantes com a Coreia e o Reino Unido.[113]

---

[109] ORGANIZAÇÃO INTERNACIONAL DE COMISSÕES DE VALORES MOBILIÁRIOS, *Memorando de Entendimento Multilateral sobre Consulta e Cooperação e Troca de Informações* (maio de 2012), https://www.iosco.org/library/pubdocs/pdf/IOSCOPD386.pdf .

[110] AUSTRALIAN PRUDENTIAL REGULATION AUTHORITY, *Prudential Standard CPS 231: Outsourcing*, par. 34 (julho de 2017), https://www.apra.gov.au/sites/default/files/Prudential-Standard-CPS-231-Outsourcing-%28July-2017%29.pdf.

[111] Id.

[112] MINISTRY OF TRADE AND INDUSTRY SINGAPORE, *Singapore-Australia Digital Economy Agreement (SADEA)* (2020), https://www.mti.gov.sg/Trade/Digital-Economy-Agreements/The-Singapore-Australia-Digital-Economy-Agreement.

[113] MINISTRY OF TRADE AND INDUSTRY SINGAPORE, *Korea-Singapore Digital Partnership Agreement (KSDPA)* (2022), https://www.mti.gov.sg/Trade/Digital-Economy-Agreements/KSDPA; Ministry of Trade and Industry Singapore, *UK-Singapore Digital Economy Agreement (UKSDEA)* (2022), https://www.mti.gov.sg/Trade/Digital-Economy-Agreements/UKSDEA.

A nível multilateral, o Japão propôs o conceito de "livre fluxo de dados com confiança", que foi aprovado tanto pelo G7 como pelo G20.[114] O objetivo do conceito, que articula princípios para a governação dos dados que servirão de base a normas globais, é promover o livre fluxo de dados, protegendo simultaneamente a privacidade e a segurança dos mesmos. No Indo-Pacífico, o fórum da Cooperação Económica Ásia-Pacífico (APEC) desenvolveu um sistema de Regras de Privacidade Transfronteiriças (CBPR), que consiste num quadro de privacidade apoiado pelo governo que estabelece um mecanismo de certificação para empresas privadas que deram o seu acordo à implementação de formas de proteção de privacidade de dados reconhecidas internacionalmente.[115] As empresas certificadas, cuja conformidade é avaliada por agentes de responsabilização designados e é imposta por lei, podem transferir livremente dados entre os países participantes, o que lhes permite ultrapassar as diferenças das legislações sobre privacidade dos países participantes.[116] Vários membros da APEC, incluindo os Estados Unidos e o Japão, promoveram um sistema global de CBPR para alargar o modelo da APEC.[117] Atualmente, porém, as instituições financeiras não podem, em geral, ser certificadas porque os reguladores financeiros não participam no sistema.[118]

No setor financeiro, o Conselho de Estabilidade Financeira (FSB) identificou a troca de dados e os padrões de mensagens transfronteiriças como uma prioridade para melhorar os pagamentos internacionais.[119] Como parte deste processo, o CEF planeia desenvolver recomendações para promover o alinhamento e a interoperabilidade entre os diferentes quadros de dados aplicáveis aos pagamentos transfronteiriços, incluindo a privacidade dos dados, a resiliência operacional, a conformidade com a LBC/CFT e os requisitos de acesso regulamentares e de supervisão. Essas recomendações, por sua vez, servirão de base para que as autoridades nacionais reavaliem os seus próprios quadros de dados.[120] A coerência entre jurisdições no que respeita à transferência de dados financeiros e a eliminação de barreiras às transferências transfronteiriças de dados permitirão às instituições financeiras tirar partido das vantagens que a tecnologia de computação em nuvem tem para oferecer.

---

[114] G7, *G7 Roadmap for Cooperation on Data Free Flow with Trust* (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] ASIA-PACIFIC ECONOMIC COOPERATION, *APEC Cross Border Privacy Rules (CBPR) System* (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] U.S. DEPARTMENT OF COMMERCE, *Global Cross-Border Privacy Rules Declaration*, https://www.commerce.gov/global-cross-border-privacy-rules-declaration.

[118] INSTITUTE OF INTERNATIONAL FINANCE, *Data Flows Across Borders: Overcoming Data Localization Restrictions* (março de 2019).

[119] FINANCIAL STABILITY BOARD, *G20 Roadmap for Enhancing Cross-border Payments* (13 def evereiro de 2023), https://www.fsb.org/wp-content/uploads/P230223.pdf.

[120] Id.

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