Panorama Setorial da Internet

Número 2
Junho, 2023
Ano 15

Proteção de dados pessoais: privacidade e confiança no ambiente digital

Perspectivas da sociedade brasileira em relação à privacidade e à proteção de dados pessoais

Por Winston Oyadomari[1], Ramon Silva Costa[2] e Manuella Maia Ribeiro[3]

Introdução

As pesquisas a respeito do uso da Internet no Brasil revelam um crescimento do número de usuários acompanhado de uma diversificação das atividades realizadas na rede. Em 2022, 93% dos usuários de Internet mandaram mensagens instantâneas, 80% usaram redes sociais, 69% compartilharam conteúdo na Internet e 45% compraram produtos e serviços por meio da rede (Comitê Gestor da Internet no Brasil [CGI.br], 2023). A onipresença do celular como dispositivo de acesso, na maioria das vezes de modo exclusivo, sugere que grande parte desses usos seja acessada no Brasil por meio de aplicativos de celular, responsáveis pela coleta de uma extensa gama de dados pessoais dos usuários. Tais atividades também se relacionam cada vez mais com o debate sobre como os dados de indivíduos são utilizados e compartilhados, com foco tanto no desenvolvimento econômico e social como na regulação e monitoramento de potenciais abusos do uso indiscriminado desses dados, principalmente daqueles que possam gerar prejuízos irreparáveis à sociedade. Nesse sentido, um exemplo são usos que levem a incidentes de segurança, acessos não autorizados e decisões baseadas em vieses discriminatórios. Diante desse cenário, a necessidade de uma governança de dados[4] sólida torna-se cada vez mais importante.

---

[1] Bacharel em Administração Pública pela Escola de Administração de Empresas de São Paulo da Fundação Getulio Vargas (FGV EAESP), é pesquisador na Coordenação de Métodos Quantitativos e Estudos Setoriais do Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação (Cetic.br), departamento do Núcleo de Informação e Coordenação do Ponto BR (NIC.br).

[2] Doutorando em Direito pela Pontifícia Universidade Católica do Rio de Janeiro (PUC-Rio), mestre em Direito pela Universidade Federal de Juiz de Fora (UFJF), especialista em Direito Digital pela Universidade do Estado do Rio de Janeiro (UERJ) e pelo Instituto de Tecnologia e Sociedade do Rio de Janeiro (ITS-Rio) e graduado em Direito pela Universidade Federal Fluminense (UFF). É pesquisador do Núcleo Legalite – Direito e Novas Tecnologias da PUC-Rio e advogado especialista em Conformidade e Proteção de Dados do NIC.br.

[3] Doutora e mestre em Administração Pública e Governo pela FGV EAESP, é pesquisadora na Coordenação de Projetos de Pesquisa do Cetic.br|NIC.br, onde lidera as pesquisas TIC Governo Eletrônico e TIC Centros Públicos de Acesso.

[4] Para fins deste artigo, governança de dados será tratada como "regras, processos e comportamentos relacionados à coleta, gestão, análise, uso, compartilhamento e descarte de dados — pessoais e/ou não pessoais" (Datasphere Initiative, 2023, p. 5).

Ao mesmo tempo em que os órgãos públicos devem atuar para regular e fiscalizar o tratamento de dados pessoais, também precisam garantir o uso adequado de dados dos cidadãos para a realização de suas atividades, como a prestação de serviços públicos.

As atividades realizadas no ambiente digital mobilizam uma ampla rede de atores em um ecossistema baseado em dados que tem crescido massivamente. Nesse contexto, foram estabelecidas normas legais recentes que regulamentam parte desse ecossistema no que tange aos riscos de violações de direitos relacionados à privacidade e à proteção de dados pessoais, como o Regulamento Geral sobre a Proteção de dados (RGPD), na União Europeia (2016), e a Lei Geral de Proteção de Dados Pessoais (LGPD) (2018), no Brasil. O aumento do interesse em torno do tema também inspirou iniciativas de produção de dados estatísticos acerca da perspectiva dos usuários sobre sua privacidade e sua percepção a respeito do uso de seus dados pessoais por atores públicos e privados, como a Pesquisa sobre Proteção de Dados realizada pelo Eurobarômetro, em 2015 (Commissão Europeia, 2015), e o estudo Americans and Privacy, realizado pelo Pew Research Center, em 2019 (Auxier *et al*., 2019). Tais estudos também geram insumos para compreender o papel dessa dimensão na confiança dos usuários de Internet no ambiente digital, apontando que receios dos indivíduos quanto ao uso de seus dados pessoais podem ter impactos na adoção de serviços digitais, sejam públicos ou privados (Fundo de Desenvolvimento de Capital das Nações Unidas [UNCDF], 2021).

No contexto brasileiro, a pesquisa *Privacidade e proteção de dados pessoais 2021: perspectivas de indivíduos, empresas e organizações públicas no Brasil* (CGI.br, 2022), realizada pelo Cetic.br|NIC.br com usuários de Internet, apresentou uma medição inovadora a respeito de como a população entende a temática de privacidade e proteção de dados e se posiciona frente a temas como as práticas de coleta de dados e os riscos percebidos nessas operações. Além disso, o estudo também incluiu indicadores relacionados à implementação de ações voltadas para privacidade e proteção de dados pessoais entre empresas e órgãos públicos no país, o que permitiu mapear o processo de adaptação à legislação vigente, promulgada em 2018, e os principais desafios enfrentados pelas organizações públicas e privadas.

Este artigo apresenta um recorte dos indicadores da pesquisa *Privacidade e proteção de dados pessoais 2021* (CGI.br, 2022), com ênfase na percepção dos usuários de Internet acerca desse tema. Além disso, destaca as percepções dos usuários em relação ao setor público, apontando o duplo papel das autoridades públicas na garantia dos direitos relacionados à privacidade e à proteção de dados. Ao mesmo tempo em que os órgãos públicos devem atuar para regular e fiscalizar o tratamento de dados pessoais, também precisam garantir o uso adequado de dados dos cidadãos para a realização de suas atividades, como a prestação de serviços públicos. Assim, tanto no monitoramento da adequação à legislação, como a LGPD, quanto para assegurar a segurança dos dados pessoais em sua custódia, a atuação do setor público pode ser um aspecto-chave para a confiança da sociedade nas atividades *online*.

Privacidade e proteção de dados pessoais na perspectiva da sociedade brasileira

PERCEPÇÃO SOBRE O CONCEITO

A pesquisa explorou o entendimento do conceito de privacidade entre os usuários de Internet no país por meio de uma pergunta aberta[5]. As respostas foram analisadas e codificadas de forma automatizada em categorias amplas, o que permitiu compreender a quais domínios as pessoas se referem quando pensam em "privacidade".

O exercício de categorização das respostas abertas gerou seis categorias:

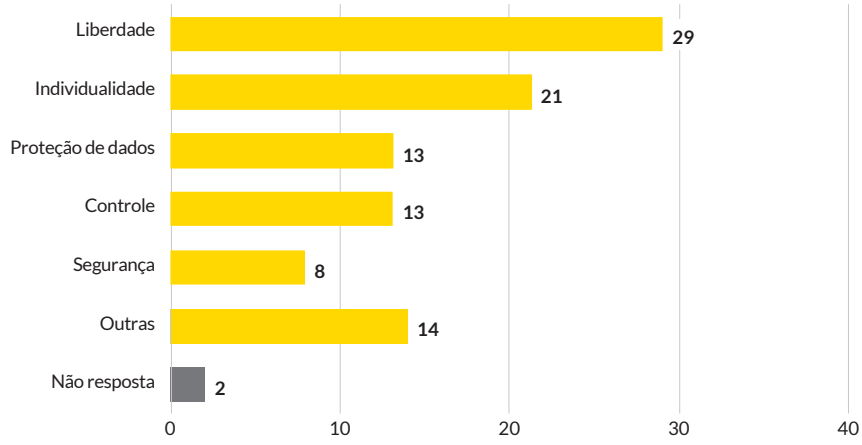
- Liberdade: garantia da liberdade de aspectos privados da vida ("liberdade" — própria e de outros —, "direito").
- Individualidade: a busca pela individualidade, seja em espaços, seja em situações ("individualidade", "intimidade", "espaço", "particular", "privado").
- Proteção (de dados): desejo de proteção contra acesso a seus dados por terceiros ("proteção de dados contra terceiros", "vazamentos").
- Controle (de dados): desejo de ter controle sobre seus próprios dados ("controle sobre acesso a dados", "escolha sobre o que é público", "consentimento").
- Segurança: menções mais genéricas a segurança ("segurança", "proteção", "sigilo", "monitoramento").
- Outras: respostas válidas não enquadradas nas demais categorias ("paz", "tranquilidade", "sossego", "importante", "essencial", "tudo" [não elaborado], "não existe").

Os resultados indicam que a maior parte dos usuários de Internet define "privacidade" partindo de domínios associados à liberdade e à individualidade (Gráfico 1) — entendidos como aspectos cruciais da vida cotidiana — e, em alguns casos, equiparada a um direito fundamental. Em um patamar inferior, estão aqueles que descrevem a lógica de dados associada ao uso da Internet, de plataformas *online* e de redes sociais. A proteção de dados é descrita tanto como uma barreira ao acesso desautorizado (controlado ou configurado), quanto pela perspectiva sobre quem pode ter acesso a eles (como em configurações de redes sociais) e a segurança contra roubos e vazamentos no ambiente digital.

Há ainda um grupo de usuários que forneceram respostas associadas estritamente à segurança contra invasões e roubos de dados, o que revela uma preocupação acerca dos riscos associados ao ecossistema de dados. Finalmente, há ainda respostas que não puderam ser classificadas em nenhum dos grupos anteriores, agrupadas na categoria "Outras". Essa pluralidade de percepções reforça o caráter multifacetado do tema entre os respondentes.

[5] Para a análise das respostas abertas, foi utilizado um método de aprendizado de máquina supervisionado. Em um primeiro momento, uma amostra de 500 respostas foi selecionada aleatoriamente e categorizada manualmente por um grupo de pesquisadores. Posteriormente, foi aplicada modelagem de tópico (Chen *et al*., 2016).

Gráfico 1 – CATEGORIZAÇÃO DA DEFINIÇÃO DO CONCEITO DE PRIVACIDADE
Total de usuários de Internet com 16 anos ou mais (%)



Fonte: CGI.br (2022).

Valer apontar que a categoria "Proteção de dados" apresentou variações por classe social (17% entre os usuários das classes AB e 8% entre os das classes DE) e grau de instrução (6% entre aqueles com até o Ensino Fundamental e 17% entre os com Ensino Superior). Ao analisar as respostas por grupos etários, também foram encontradas diferenças relevantes: as respostas dadas pelos mais jovens foram categorizadas em maior proporção como "Individualidade" (32% dos que têm de 16 a 24 anos e 27% daqueles entre 25 e 34 anos) e, entre os mais velhos, como "Liberdade" (43% dos que têm 60 anos ou mais).

CANAIS DE SOLICITAÇÃO

Em 2020, foi criada a Autoridade Nacional de Proteção de Dados (ANPD), entidade que tem entre suas responsabilidades o recebimento e o encaminhamento de solicitações, reclamações ou denúncias relativas a dados pessoais e promoção de boas práticas de gestão dos dados pelas organizações controladoras, ou seja, aquelas que realizam tratamento de dados pessoais. A pesquisa do Cetic.br|NIC.br (CGI.br, 2022) realizada no final de 2021 demonstra que a possibilidade de realizar solicitações à ANPD ainda não é plenamente explorada pelos usuários de Internet. Também é possível identificar o direcionamento das demandas majoritariamente às organizações controladoras dos dados, seguidas de órgãos relacionados ao direito ao consumidor, como os Procons.

A busca por canais de atendimento para solicitações, reclamações ou denúncias foi feita por 24% dos usuários de Internet com 16 anos ou mais. Entre os que buscaram, o canal mais mencionado foi a própria empresa ou órgão público controlador do dado (80%), seguido de órgãos de defesa do consumidor, como o Procon (48%). Já a ANPD aparece em um patamar bastante inferior (27%).

Entre os que não buscaram canais de atendimento para solicitações, reclamações ou denúncias, os canais mais mencionados em caso de necessidade futura seriam o Procon (79%), seguido da empresa ou do órgão público controlador do dado (74%), da polícia (65%) e da ANPD (62%). Portanto, a ANPD ainda não é percebida como um dos principais espaços para buscar auxílio em situações de potenciais violações à privacidade e à proteção de dados pessoais da mesma forma que os órgãos de defesa do consumidor, estabelecidos desde a criação do Código de Defesa do Consumidor (CDC) (1990). Assim, os titulares vinculam suas reclamações ou solicitações a uma relação de consumo, ou até relacionam diretamente a um crime, realizando as denúncias junto às autoridades policiais.

PERCEPÇÕES ACERCA DO TRATAMENTO DE DADOS PESSOAIS SENSÍVEIS

Governos trabalham com uma quantidade massiva de dados pessoais dos cidadãos no desempenho de suas atividades regulares, como segurança, tributação e prestação de serviços públicos. Além disso, são capazes de relacionar dados de origens e natureza distintas, inclusive dados de natureza sensível. Nesse contexto, 40% dos usuários de Internet declaram estar muito preocupados e 29% preocupados com o uso que o poder público faz de seus dados. Esse nível de preocupação é um pouco inferior em relação ao uso feito por empresas: 47% declararam estar muito preocupados e 28% preocupados com tal uso.

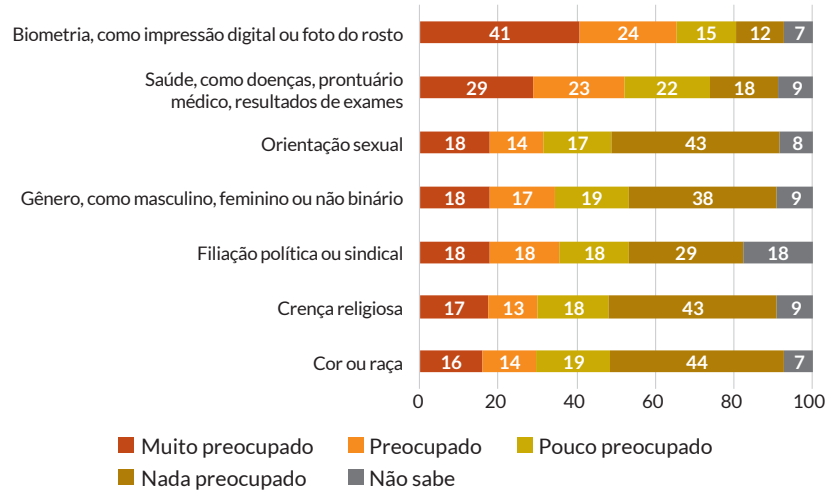
Os dados também mostram uma diferença no nível de preocupação sobre o uso dos dados feito pelas empresas no que tange à cor ou à raça do respondente. Pessoas pretas (52%) e pardas (49%) declaram estar muito preocupados numa proporção maior do que brancas (43%), o que sugere uma percepção de potencial uso discriminatório desse dado por parte de empresas contra essa população. A diferença também ocorre quando o uso é feito por governos: 47% dos pretos declaram estar muito preocupados, enquanto esse percentual é inferior entre pardos (41%) e brancos (37%).

Os usuários de Internet declaram elevado nível de preocupação com o fornecimento de dados biométricos em proporção maior do que com relação aos demais tipos de dados pessoais sensíveis investigados: 41% disseram estar muito preocupados e 24% preocupados (Gráfico 2). Outra categoria que se destaca são os dados de saúde: 29% dos respondentes declaram estar muito preocupados e 23% preocupados.

(...) 40% dos usuários de Internet declaram estar muito preocupados e 29% preocupados com o uso que o poder público faz de seus dados.

Gráfico 2 – NÍVEL DE PREOCUPAÇÃO COM FORNECIMENTO DE INFORMAÇÕES PESSOAIS SENSÍVEIS

Total de usuários de Internet com 16 anos ou mais (%)



Fonte: CGI.br (2022).

O avanço da biometria sobre diversos contextos da vida cotidiana, tanto na forma de impressão digital quanto de reconhecimento facial, aliado à natureza íntima, tangível e material desse dado e seu elevado potencial de dano em caso de comprometimento, pode ajudar a compreender esses resultados. O uso de dados biométricos em eleições brasileiras foi testado inicialmente no pleito de 2008, contava com cerca de 120 milhões de biometrias cadastradas em 2020 e pretende alcançar a totalidade dos eleitores até 2026[6]. Também se pode observar o uso da biometria pelo setor privado em bancos, farmácias, academias de ginástica e condomínios privados, gerando uma série de questionamentos no âmbito judicial quanto à coleta e ao uso desse tipo de dados em determinados contextos.

Além disso, o tratamento de dados biométricos para fins de segurança e vigilância pública tem provocado um debate extenso no contexto brasileiro. Nesse ponto, destaca-se o tratamento automatizado de dados pessoais sensíveis por meio do uso de tecnologias de reconhecimento facial munidas de Inteligência Artificial (IA). A implementação dessas tecnologias enfrenta críticas e resistência de alguns setores, visto que o reconhecimento facial tem sido o carro-chefe de grandes promessas na segurança pública, ao passo que populações socialmente vulneráveis têm sido constantemente sujeitas à automatização de constrangimentos e violências, incluindo abordagens policiais indevidas e atribuição inverídica de antecedentes criminais, com a população negra sendo a mais violada neste cenário[7] (Costa & Kremer, 2022).

[6] Em 2022, o Brasil tinha 156 milhões de eleitores aptos, segundo o TSE. Detalhamento acerca do uso de informações biométricas em eleições pode ser consultado em: https://www.tse.jus.br/eleicoes/biometria/biometria

[7] Sobre racismo e uso de tecnologias de reconhecimento facial: https://www.brasildefato.com.br/2019/11/27/cerca-de-90-das-pessoas-presas-com-uso-de-reconhecimento-facial-sao-negras

Nesse ponto, embora a LGPD não regule diretamente os casos de uso de dados para fins de segurança pública e persecução penal, estipula a necessidade de criação de uma legislação específica (Art. 4º, Inc. III). Em 2019, a Câmara dos Deputados tomou a iniciativa de criar uma Comissão de Juristas para elaboração do anteprojeto da chamada "LGPD Penal"; um ano após a formação da Comissão, foi apresentada à Presidência da Câmara uma proposta de anteprojeto. O documento está na Câmara dos Deputados à espera de ser apresentado formalmente por algum parlamentar a fim de tornar-se um Projeto de Lei (PL) (Costa & Kremer, 2022).

Contudo, a coleta de dados relacionados ao reconhecimento facial não é uma prática restrita ou problemática apenas no setor público. A ViaQuatro, empresa que tem a concessão da linha 4-amarela do Metrô de São Paulo, foi condenada pelo Tribunal de Justiça de São Paulo, a pagar R$500 mil pelo reconhecimento facial realizado por câmeras sem o consentimento dos passageiros: as câmeras instaladas no metrô captavam expressões faciais e até mesmo identificavam emoções com fins comerciais e publicitários. A decisão foi resultado de uma ação civil pública em defesa dos consumidores dos serviços do Metrô[8].

Os indicadores sobre dados sensíveis revelam um debate importante sobre essa categoria especial de dados pessoais. A LGPD indica a categoria de dados pessoais sensíveis em seu Art. 5°, Inciso II, criada em razão da potencialidade discriminatória e danosa gerada para titulares pelo tratamento indevido de determinados dados. Dentre esses dados, estão indicados expressamente na lei informações como raça, etnia, religião, opinião política, filiação a sindicato ou organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, e dados genéticos ou biométricos, quando vinculados a uma pessoa natural.

Segundo Doneda (2019), a própria seleção sobre quais dados seriam sensíveis demonstra que a circulação de determinadas informações pode acarretar maior potencial lesivo a seus titulares em uma determinada configuração social, acrescentando que os efeitos discriminatórios não estão no dado em si, mas nos usos que são feitos dele. Partindo desse pressuposto, a compreensão sobre os mecanismos empregados na proteção de dados sensíveis perpassa um entendimento sobre as dinâmicas discriminatórias articuladas na sociedade. Tal entendimento colabora na compreensão sobre os indicadores de preocupação dos usuários com o tratamento de dados sensíveis operado por agentes públicos, especialmente quando se abordam dados de saúde, raça e biometria.

Nesse sentido, proteger de maneira rigorosa os dados sensíveis é instrumento indispensável para a efetivação da igualdade e da liberdade das pessoas diante de um contexto informacional marcado pela implementação de tecnologias avançadas e por assimetrias de poder entre titulares e controladores de dados pessoais (Mulholland, 2020). Assim, as empresas e as organizações públicas devem considerar que a LGPD impõe um padrão mais elevado de proteção e segurança para as informações pessoais sensíveis, o que estimula processos de adequação que envolvam a criação de normas internas condizentes com a legislação, como fortalecimento de códigos de ética e conduta, especificando valores e princípios relacionados aos direitos fundamentais, de modo a coibir iniciativas que violem a

(...) a compreensão sobre os mecanismos empregados na proteção de dados sensíveis perpassa um entendimento sobre as dinâmicas discriminatórias articuladas na sociedade.

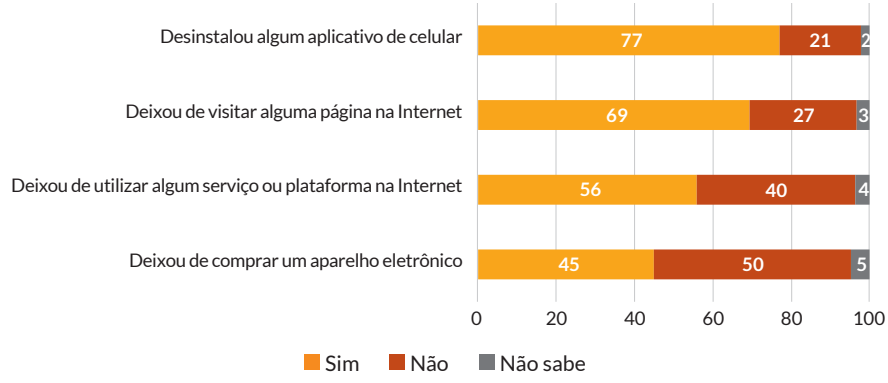
[8] Saiba mais em: https://idec.org.br/noticia/idec-vence-acao-contra-uso-de-reconhecimento-facial-e-viaquatro-e-condenada-pagar

personalidade e dignidade de titulares. Nesse ponto, ações, como diálogos multissetoriais entre agentes, são importantes para a troca e a elaboração de boas práticas (Teffé, 2022).

RESTRIÇÕES AO USO

Para além de estratégias de prevenção de riscos e de controle sobre as configurações de privacidade de aplicativos e serviços, a pesquisa também revelou que usuários de Internet podem adotar restrições a seu uso devido à preocupação com o uso de seus dados pessoais. Motivados por essa preocupação, 77% dos usuários de Internet de 16 anos ou mais já desinstalaram aplicativos, 69% deixaram de visitar algum *website*, 56% deixaram de utilizar algum serviço na Internet e 45% deixaram de comprar algum equipamento eletrônico (Gráfico 3).

Gráfico 3 – ATIVIDADES QUE DEIXOU DE REALIZAR POR PREOCUPAÇÕES COM DADOS PESSOAIS
Total de usuários de Internet com 16 anos ou mais (%)



Fonte: CGI.br (2022).

Esse indicador revela, portanto, que grande parte dos usuários de Internet no Brasil já restringiu de alguma forma suas ações na Internet por preocupações relacionadas aos dados pessoais. A desconfiança a respeito da forma como os dados pessoais serão utilizados, compartilhados ou mesmo vazados afeta o nível de adoção de serviços, o uso de aplicativos e a visita a *websites*. Nesse sentido, essa percepção de risco diante do ambiente *online* pode diminuir o acesso a oportunidades oferecidas pela Internet e representa uma mensagem relevante para o desenvolvimento de serviços e aplicações no ambiente digital, especialmente para o contexto da governança de dados.

Considerações finais

A governança de dados desempenha um papel fundamental na gestão eficaz das informações, estabelecendo políticas e práticas para garantir qualidade, conformidade e uso adequado dos dados. Nesse contexto, a proteção de dados pessoais assume uma importância central, pois busca preservar a confidencialidade, a integridade e a disponibilidade das informações, mitigando, por exemplo, riscos de acesso não autorizado, perda ou uso indevido.

A pesquisa do Cetic.br|NIC.br (CGI.br, 2022) demonstra que os usuários de Internet no Brasil estão receosos quanto ao uso de seus dados pessoais, especialmente os de natureza sensível, como dados biométricos; ademais, a percepção sobre o conceito de privacidade está associada às práticas *online* para uma parcela dos entrevistados. Tais resultados levantam uma série de implicações para a confiança da sociedade no ambiente digital, incluindo o acesso a atividades e serviços *online*.

Em relação ao contato com organizações para denunciar ou buscar seus direitos relacionados à proteção de dados, além das entidades controladoras de seus dados, os usuários de Internet citam mais frequentemente órgãos de defesa do consumidor e autoridades policiais como o *locus* de denúncias ou reclamações. Geralmente, a ANPD ainda não é percebida como um espaço de interação para esse tema entre os usuários de Internet. Nesse sentido, estratégias de divulgação de atribuições e atividades dessas diferentes organizações podem orientar os cidadãos quanto à entidade mais adequada para tratar de solicitações referentes ao tema, a fim de trazer maior segurança quanto aos canais voltados para a garantia desses direitos.

Os dados biométricos foram os mais mencionados entre os investigados como tipo de informação sensível que preocupa os usuários de Internet, o que também demanda uma reflexão por parte de organizações públicas e privadas sobre as estratégias para sua coleta e seu processamento. Também é importante ressaltar a diferença nos resultados em relação aos temas de discriminação mencionados por pessoas de cor preta, o que reflete um cenário de temor de uma parcela da população cotidianamente vulnerabilizada em relação à intensificação de práticas discriminatórias. Desse modo, verifica-se que essas preocupações estão inseridas no cotidiano dos usuários de Internet brasileiros e se relacionam à necessidade de um maior rigor para a legalidade no tratamento de dados pessoais sensíveis, tendo em vista a potencialidade lesiva e discriminatória de tratamento indevidos desses tipos de dados pessoais.

Um resultado surpreendente levantado por esta pesquisa é a restrição feita por usuários de Internet sobre seu próprio comportamento, motivados pela preocupação com o uso de seus dados. Isso demonstra que usuários podem optar por não realizar serviços por canais digitais devido a receio da coleta e uso de seus dados, impactando a prestação de informações e serviços públicos pelos meios digitais. Além disso, preocupação quanto a ciberataques, fraudes, segurança, falta de transparência no uso de dados, entre outros, podem diminuir a confiança nos serviços de governo e afetar sua adoção pela sociedade (Departamento de Assuntos Econômicos e Sociais das Nações Unidas [UN DESA], 2022).

(...) usuários podem optar por não realizar serviços por canais digitais devido a receio da coleta e uso de seus dados, impactando a prestação de informações e serviços públicos pelos meios digitais.

(...) a adoção de práticas voltadas para gerar maior confiança no uso de aplicações digitais torna-se fundamental para as estratégias e os modelos de governança de dados adotados pelas organizações públicas.

Ao avaliar, por exemplo, a adoção de aplicativos governamentais de *contact tracing*[9] durante a pandemia, estudos sugerem que ampliar a transparência e a confiança na segurança do uso de seus dados nesses serviços também aumenta a propensão a utilizá-los (Hermosilla & Lapostol, 2022; Lin *et al*., 2020; Conselho Europeu, 2020). Portanto, a adoção de práticas voltadas para gerar maior confiança no uso de aplicações digitais torna-se fundamental para as estratégias e os modelos de governança de dados adotados pelas organizações públicas. Nesse sentido, os resultados ajudam a reforçar a importância do tema para o debate público e lançam novas perguntas que deverão ser endereçadas por futuros estudos sobre privacidade e proteção de dados pessoais no país, especialmente para a promoção da boa governança de dados.

Referências

Auxier, B., Rainie, L., Anderson, M., Perrin, A., Kumar, M., & Turner, E. (2019). *Americans and privacy: Concerned, confused and feeling lack of control over their personal information (American Trends Panel Wave 49).* Pew Research Center. https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/

Chen, Q., Yao, L., & Yang, J. (2016). Short text classification based on LDA topic model. *2016 International Conference on Audio, Language and Image Processing (ICALIP)*, 749-753. https://doi.org/10.1109/ICALIP.2016.7846525

Código de Defesa do Consumidor. (1990). *Lei n. 8.078, de 11 de setembro de 1990. Dispõe sobre a proteção do consumidor e dá outras providências.* Brasília: Presidência da República. https://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm

Comitê Gestor da Internet no Brasil. (2023). *Pesquisa sobre o uso das Tecnologias de Informação e Comunicação nos domicílios brasileiros – TIC Domicílios 2022*. São Paulo: CGI.br. https://cetic.br/pt/tics/domicilios/2022/individuos/

Comitê Gestor da Internet no Brasil. (2022). *Privacidade e proteção de dados pessoais 2021: perspectivas de indivíduos, empresas e organizações públicas no Brasil*. São Paulo: CGI.br. https://cetic.br/pt/publicacao/privacidade-e-protecao-de-dados-2021/

Comissão Europeia. (2015). *Special Eurobarometer 431: Data Protection*. (Special Eurobarometer 431 / Wave EB83.1). European Commission, Directorate-General for Justice and Consumers. https://doi.org/10.2838/552336

Conselho Europeu. (2020). *2020 Data protection report*. https://rm.coe.int/prems-120820-gbr-2051-digital-solutions-to-fight-covid-19-texta4-web-/16809fe49c

Costa, R., & Kremer, B. (2022, outubro). Inteligência Artificial e Discriminação: desafios e perspectivas para a proteção de grupos vulneráveis diante das tecnologias de reconhecimento facial. *Direitos Fundamentais & Justiça*, ano 16, número especial, p. 145-167. https://dfj.emnuvens.com.br/dfj/article/view/1316/1065

Datasphere Initiative. (2023). Governança de dados e a Datasfera: revisão da literatura. *Panorama Setorial da Internet, 15*(1). https://cetic.br/pt/publicacao/ano-xv-n-1-ecossistema-e-producao-de-dados/

[9] Inclui atividades de identificar, avaliar e orientar pessoas expostas a uma doença para evitar a transmissão posterior, podendo adotar o apoio de tecnologias digitais nesse processo (Organização Mundial da Saúde [OMS], 2020).

Departamento de Assuntos Econômicos e Sociais das Nações Unidas. (2022). *E-Government Survey 2022: The future of digital government*. https://publicadministration.un.org/en/Research/UN-eGovernment-Surveys

Doneda, D. (2019). *Da privacidade à proteção de dados pessoais*. São Paulo: Revista dos Tribunais.

Fundo de Desenvolvimento de Capital das Nações Unidas. (2021, November). *The role of data protection in the digital economy*. https://static1.squarespace.com/static/5f2d7a54b7f75718fa4d2eef/t/61c39ac52e86d360a8301fd6/1640210452857/EN-UNCDFBrief-Data-Protection-2021.pdf

Hermosilla, M. P., & Lapostol, P. (2022). Limites para a transparência algorítmica. In Comitê Gestor da Internet no Brasil. *Pesquisa sobre o uso das tecnologias de informação e comunicação no setor público brasileiro: TIC Governo Eletrônico 2021* (pp. 131-137). São Paulo: CGI.br. https://cetic.br/pt/publicacao/pesquisa-sobre-o-uso-das-tecnologias-de-informacao-e-comunicacao-no-setor-publico-brasileiro-tic-governo-eletronico-2021/

Lei Geral de Proteção de Dados Pessoais. (2018). *Lei n. 13.709, de 14 de agosto de 2018. Dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural*. https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm

Lin, J., Carter, L., & Liu, D. (2021). Privacy concerns and digital government: exploring citizen willingness to adopt the COVIDSafe app. *European Journal of Information Systems, 30*(4), 389-402. https://doi.org/10.1080/0960085X.2021.192085

Mulholland, C. (2020). O tratamento de dados pessoais sensíveis. In C. Mulholland (Org.). *A LGPD e o novo marco normativo no Brasil* (pp. 121-156). Porto Alegre: Arquipélago.

Office of the Privacy Commissioner of Canada. (2021). *2020 Survey of Canadians on Privacy-Related Issues: Final Report*. Prepared by Phoenix SPI for the Office of the Privacy Commissioner of Canada. Office of the Privacy Commissioner of Canada. https://publications.gc.ca/collections/collection_2021/cpvp-opc/IP54-109-2021-eng.pdf

Organização Mundial da Saúde. (2020). *Ethical considerations to guide the use of digital proximity tracking technologies for COVID-19 contact tracing: Interim guidance*. https://apps.who.int/iris/bitstream/handle/10665/332200/WHO-2019-nCoV-Ethics_Contact_tracing_apps-2020.1-eng.pdf

Teffé, C. S. (2022). *Dados pessoais sensíveis: qualificação, tratamento e boas práticas*. Indaiatuba: Foco.

União Europeia. (2016, abril 27). Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). *Jornal Oficial da União Europeia*. https://eur-lex.europa.eu/eli/reg/2016/679/oj/por

Entrevista I

Foto: Arquivo Pessoal

Rafael Zanatta
Diretor da Associação Data Privacy Brasil de Pesquisa. Doutor pelo Instituto de Energia e Ambiente da Universidade de São Paulo (USP)

Privacidade e segurança de dados no Brasil: desafios da atualidade

Nesta entrevista, Rafael Zanatta, diretor da Data Privacy Brasil, discute os aspectos de governança de dados necessários para proteção de dados pessoais, o impacto das desigualdades socioeconômicas nas experiências individuais de privacidade, o modo como o conceito de *feedback loop* de injustiça se relaciona às questões de vigilância pelos setores público e privado e trata ainda dos principais riscos associados a coleta de dados biométricos no Brasil.

Panorama Setorial da Internet (P.S.I.)_ Quais aspectos devem ser contemplados em políticas de governança de dados de modo a garantir a proteção de dados pessoais?

Rafael Zanatta (R.Z.)_ Governança de dados é um termo guarda-chuva, que significa uma consciência sobre a razão do uso de dados pessoais em uma organização e uma intencionalidade sobre seu uso em todo seu ciclo de vida. Muitas organizações tratam uma vasta quantidade de dados pessoais, mas não possuem uma reflexão interna sobre a necessidade de tais dados, porquê devem ser usados, os limites de extração de valor econômico dessas informações, com quem tais dados podem ser compartilhados e o que deve ser feito para que os direitos básicos dos titulares dos dados sejam respeitados.

A governança de dados pode ser vista de uma perspectiva bastante ampla e holística, pois abrange pessoas, processos e ferramentas necessárias para criar um tratamento consistente e adequado de dados pessoais em uma organização, seja ela pública ou privada.

A Organização para a Cooperação e Desenvolvimento Econômico (OCDE) define que políticas de governança de dados incluem arranjos e previsões técnicas e institucionais que afetam todo o ciclo de vida de dados, como criação, coleta, armazenamento, uso, proteção, acesso, compartilhamento e exclusão. Além disso, orientam-se pelo equilíbrio entre inovação e respeito a direitos fundamentais; por isso, ao se pensar em políticas de governança de dados, deve-se incluir medidas de respeito aos direitos básicos dos titulares e de mitigação de riscos em casos de incidentes de segurança ou ilícitos que podem afetar as pessoas e a sociedade.

Cada organização possui seus próprios contextos e particularidades e, por isso, uma definição única e definitiva sobre "em que consiste a governança de dados" é limitada. Por exemplo, quando trabalhamos em convênio com as Defensorias Públicas de São Paulo e Rio de Janeiro para pensarmos a governança de dados, partimos da reflexão das funções primordiais das defensorias, do tipo de serviço público prestado, dos tipos distintos de dados tratados, das ferramentas tecnológicas usadas e da centralidade do

compartilhamento de dados para pesquisas e promoção de acesso à justiça. Logo, a construção da política de governança de dados foi internalizada como algo estratégico, envolvendo toda a equipe executiva e diretiva dessas organizações. Esse é um elemento que julgo central: deve ser considerado estratégico e não algo periférico e terceirizável.

P.S.I._ No contexto brasileiro, em que medida as desigualdades sociais e econômicas interferem nas percepções e nas experiências individuais em relação à privacidade e à proteção de dados?

R.Z._ Condições sociais e econômicas determinam posições assimétricas quando comparamos cidadãos em contextos absolutamente diferentes. Por exemplo, para pessoas muito bem instruídas e com recursos financeiros, as possibilidades de proteção de dados pessoais são múltiplas. Como pessoa privilegiada no Brasil, você pode pagar por serviços de criptografia e Virtual Private Networks (VPN). Você pode assinar contas no Spotify e YouTube e estar menos submetido à coleta massiva de dados para publicidade comportamental. Você pode pagar serviços especializados em mascaramento de informações pessoais ao registrar um domínio na Internet. Você pode utilizar serviços pagos de email, como ProtonMail, que são seguros e pouco dependentes de perfilização e modulação comportamental. Você pode também se dar ao luxo de não depender de redes sociais, em razão de sua condição econômica, e não estar exposto ao Instagram e TikTok. Além disso, você não precisa ser usuário de políticas públicas e ceder seus dados para o Governo Federal no caso de utilização do Programa Universidade para Todos (Prouni) ou do Bolsa Família.
Agora, pensemos na situação oposta. Como pessoa vulnerável, precarizada e marginalizada sócio e economicamente, você acessará a Internet somente pelo celular e estará submetido a uma extração massiva de dados pessoais. Você utilizará contas gratuitas, freemium, que vão te transformar em produto ao modular seu comportamento por meio de perfilização e publicidade comportamental. Você não terá condições de pagar por qualquer serviço de mascaramento ao registrar um domínio do website de seu pequeno empreendimento. Você terá uma ampla exibição de seus dados pessoais ao se registrar como Microempreendedor Individual (MEI). Você terá seus dados pessoais coletados e compartilhados no Cadastro Base do Cidadão (CBC) ao ser beneficiário do Bolsa Família e do Prouni. Enfim, suas relações sociais e sujeições ao que chamamos de "extrativismo digital" serão absolutamente distintas de uma pessoa de classe média alta ou alta.
Por isso, na Data Privacy Brasil, dizemos que uma cultura de proteção de dados pessoais deve ser construída pensando nas assimetrias de poder e nas questões estruturais de injustiça no Brasil. Uma política nacional de proteção de dados pessoais não pode tratar todos os brasileiros e brasileiras como iguais, simplesmente como "titulares de dados". Embora o princípio de igualdade perante a lei seja importante, precisamos qualificar a discussão com uma análise profunda sobre nossas desigualdades e como contextos sociais distintos implicam sociabilidades distintas, bem como processos de datificação e de ameaças a direitos que também são profundamente distintos.

"Basicamente, o mecanismo de *feedback loop* de injustiça ocorre da seguinte maneira: se você é usuário de políticas públicas assistencialistas, você se torna alvo de uma coleta de dados massiva e um processo bastante intenso de vigilância por parte do Estado."

P.S.I._ O que é* feedback loop *de injustiça? Como esse processo se relaciona com as discussões sobre vigilância pelos setores público e privado?

R.Z._ Essa é uma ótima pergunta. Esse conceito tem sido utilizado pela cientista política Virginia Eubanks para descrever uma situação de vulnerabilização de populações que dependem de políticas públicas nos Estados Unidos da América. Basicamente, o mecanismo de *feedback loop* de injustiça ocorre da seguinte maneira: se você é usuário de políticas públicas assistencialistas, você se torna alvo de uma coleta de dados massiva e um processo bastante intenso de vigilância por parte do Estado. Por exemplo, pessoas beneficiárias de auxílio-maternidade em comunidades marginalizadas passam a ser catalogadas e todos os seus rastros digitais, como a quantidade de idas ao hospital, compras em farmácias populares e outros tipos de dados, passam a ser registrados e unificados em uma base de dados integradora.

O que Eubanks demonstrou é que várias dessas pessoas beneficiárias de políticas públicas e que passam por uma intensificação no processo de vigilância e tratamento de dados, posteriormente, passam a ser prejudicadas em processos automatizados de análise e tomada de decisão, como sistemas automatizados de alocação de pessoas para oportunidades de emprego, porque o processo de hipervigilância coloca aquela pessoa em uma categoria discriminada em um processo de análise automatizada posterior. Por exemplo, a análise automatizada de alocação de emprego leva em consideração a pessoa ter sido usuária de serviços de saúde pública por um longo período de tempo e pode ser considerado um *input* para avaliar um grau de risco maior daquela pessoa em termos de estabilidade. Nesse sentido, essas ações constroem um sistema de perpetuação de injustiças automatizadas e profundamente invisíveis.

Outra filósofa muito importante que tem pensado sobre isso é a professora Anita Allen. Ela inclusive chegou a cunhar novos conceitos, que vão além da ideia de *panopticon* elaborada por Jeremy Bentham. Para ela, além do *panopticon* como arquitetura de vigilância (quem é visto não pode ver quem vigia), temos hoje uma "situação complicada" para as pessoas negras nos Estados Unidos, que são também submetidas a uma hipervigilância que promove uma espécie de *banopticon* (barreiras de entrada, catracas automatizadas por processos movidos a dados e situações de exclusão com base em perfis) e um *conopticon* (essas mesmas pessoas hipervigiadas estão mais suscetíveis a golpes, fraudes, esquemas lesivos, etc.). Tanto Allen quanto Eubanks estão preocupadas em realizar uma crítica ao modo como as sociedades atuais podem aprofundar desigualdades e racismo no uso de Inteligência Artificial (IA) e sistemas de decisão automatizados.

P.S.I._ Qual é o debate atual a respeito da coleta de dados biométricos no Brasil? Quais são os principais riscos associados a esse tipo de prática?

R.Z._ Hoje, vivemos um dilema gerado pela segurança pública. Vivemos uma espécie de "canto da sereia" com relação às promessas de que as tecnologias vão solucionar nossos problemas sociais e nossas mazelas de violência e de segurança pública. Vivemos um tecnossolucionismo ingênuo.

Muitos prefeitos embarcaram na onda do reconhecimento facial em espaços abertos como principal solução para segurança pública, como se fosse uma solução mágica para combate ao crime. Cidades como Salvador (Bahia) e Maringá (Paraná) estão comemorando a utilização de sistemas modernos para identificar criminosos em festas públicas, por exemplo carnavais ou festas de São João. Contudo, isso tem sido feito sem uma reflexão sobre os múltiplos riscos associados à naturalização do reconhecimento facial automatizado em locais públicos. O que se observa é uma celebração sobre os "resultados mágicos alcançados", no sentido de automação de um trabalho visual que deveria ser realizado por policiais. Porém, essas ações resolvem muito pouco sobre as causas dos problemas e sobre suas raízes.

Essa naturalização é perigosa, pois ela cria uma sensação falsa de que os problemas serão resolvidos. Cria também um estímulo perverso para que prefeituras invistam milhões de reais em soluções de reconhecimento facial, deixando de direcionar recursos, já escassos, em outras políticas públicas, como alimentação adequada, saúde e capacitação profissional de jovens em escolas periféricas. Quem ganha muito com isso são poucas empresas que cobram preços artificiais e inflados.

Há contramovimentos importantes. A ação civil pública que conduzimos em 2018 contra o tratamento indevido de dados biométricos de passageiros no metrô de São Paulo, no período que estive no Instituto Brasileiro de Defesa do Consumidor (Idec) (caso "Idec contra Viaquatro", julgado pelo Tribunal de Justiça de São Paulo - TJSP), é um caso importante de limites impostos pelo judiciário. Neste caso, o sistema de justiça disse claramente: você não pode tratar as pessoas como coisas e extrair a emoção de seu rosto sem transparência, necessidade e respeito a direitos básicos.

Penso que esse é um remédio importante para a discussão dos dados biométricos no Brasil. Estamos falando de suas coisas básicas. Primeiro, uma concepção simples, inspirada em Kant: somos sujeitos de direito e não coisas ou ratos em laboratório que podem ser usados. Temos dignidade e direitos de personalidade. Segundo, algumas perguntas essenciais: Precisamos mesmo? Faz bem? Resolve algo? Por isso, insistimos em avaliações de impacto e debates públicos que mostrem que há boas razões nessas decisões.

"(...) isso tem sido feito sem uma reflexão sobre os múltiplos riscos associados à naturalização do reconhecimento facial automatizado em locais públicos. (...) Essa naturalização é perigosa, pois ela cria uma sensação falsa de que os problemas serão resolvidos."

Artigo II

Tecnologias emergentes de aprimoramento da privacidade: abordagens políticas e regulatórias atuais[10]

Por Organização para a Cooperação e Desenvolvimento Econômico[11]

Este artigo examina as tecnologias de aprimoramento da privacidade (*privacy-enhancing technologies* [PET]), soluções digitais que permitem a coleta, o tratamento, a análise e o compartilhamento de informações, enquanto protegem a confidencialidade e a privacidade dos dados. O texto analisa os recentes avanços tecnológicos e avalia a efetividade de diferentes tipos de PET, bem como os desafios e as oportunidades que elas apresentam. Descreve igualmente as atuais abordagens políticas e regulatórias em relação às PET, a fim de ajudar as autoridades de proteção de dados (*privacy enforcement authorities* [PEA]) e os formuladores de políticas a compreender melhor a forma como podem ser utilizadas para reforçar a privacidade e a proteção de dados e melhorar a governança geral dos dados.

Em especial, as PET permitem um nível relativamente elevado de utilidade dos dados, ao mesmo tempo em que minimizam a necessidade de coleta e processamento de dados. Ainda que as PET não sejam novas, os mais recentes avanços em termos de conectividade e capacidade computacional conduziram-nas a uma mudança fundamental na forma como os dados podem ser processados e compartilhados. Embora ainda incipientes, estas tecnologias têm um enorme potencial para aproximar a sociedade do processo contínuo e da prática de privacidade desde a concepção (*privacy by design*) e, assim, promover a confiança no compartilhamento e na reutilização de dados.

Um número crescente de formuladores de políticas e autoridades de proteção de dados está analisando meios de incorporar as PET em seus marcos nacionais de privacidade e de proteção de dados. No entanto, a natureza altamente técnica e em rápida evolução dessas tecnologias constitui frequentemente um obstáculo para sua implementação pelas organizações e à sua consideração nas políticas e nos marcos legais aplicáveis aos dados.

---

[10] Este artigo baseia-se no trabalho da Organização para a Cooperação e Desenvolvimento Econômico (OCDE) intitulado: OECD. (2023). *Emerging privacy-enhancing technologies: Current regulatory and policy approachs*, OECD Digital Economy Papers, n. 351. Paris: OECD Publishing, disponível em: https://doi.org/10.1787/bf121be4-en. As opiniões expressas e os argumentos aqui utilizados são inteiramente os dos autores e não devem ser atribuídos de forma alguma à OCDE ou aos seus países membros.

[11] Este artigo foi elaborado para a OCDE por Christian Reimsbach-Kounatze (Digital Economy Policy Division) juntamente com o consultor externo Taylor Reynolds (Diretor de Política Tecnológica da Iniciativa de Pesquisa de Políticas de Internet do MIT), sob a supervisão de Clarisse Girot (Digital Economy Policy Division).

O surgimento de tecnologias de aprimoramento da privacidade

A coleta e o tratamento de dados pessoais têm se transformado de forma a permitir um uso que proteja mais a privacidade dos dados pessoais no nível técnico, aproximando a sociedade do processo e da prática da privacidade desde a concepção (*privacy by design*). Um vasto conjunto de abordagens está surgindo, com base em novas técnicas criptográficas e em mudanças estruturais na forma como os dados são processados. Essas abordagens têm introduzido novas formas de proteção de privacidade e segurança digital na coleta e no processamento de dados.

Apesar de não serem fundamentalmente novas[12], essas tecnologias e técnicas digitais oferecem novas abordagens para *accountability* e a proteção de dados enquanto estão em uso. Podem também alterar ligeiramente os dados, permitindo ao mesmo tempo que sejam tratados para determinados usos sem divulgar as informações que contêm. Essas abordagens são frequentemente agrupadas sob o termo "tecnologias de aprimoramento da privacidade", ou PET. No entanto, o termo subestima o papel essencial que tais tecnologias e abordagens disruptivas podem ter na governança de dados de forma mais ampla.

As PET alteram a forma como as organizações coletam, acessam e processam dados, especialmente dados pessoais. Elas são promissoras porque ampliam o acesso à análise de dados e, ao mesmo tempo, aumentam a segurança digital e a proteção à privacidade e aos dados. Por exemplo, as PET apoiam a análise colaborativa de dados que, de outra forma, seriam demasiado sensíveis para serem divulgados, combinados e utilizados entre indivíduos ou organizações.

Governos e entidades reguladoras, nomeadamente as autoridades de proteção de dados (*privacy enforcement authorities* [PEA]), identificaram e enfatizaram esses tipos de tecnologias como soluções proeminentes para a proteção da privacidade e dos dados pessoais (Comitê Europeu para a Proteção de Dados [EDPB], 2020; Agência da União Europeia para a Cibersegurança [ENISA], 2021; Office of the Privacy Commissioner of Canada [OCP], 2021; Casa Branca [Estados Unidos], 2022; Information Commisioner's Office [ICO], 2022).

O *Communiqué* de 2022 "Promover o Livre Fluxo de Dados com base na Confiança e no compartilhamento de conhecimento sobre as perspectivas dos Espaços Internacionais de Dados" ("Promoting Data Free Flow with Trust and knowledge sharing about the prospects for International Data Spaces"*)* da Mesa Redonda das Autoridades de Proteção de Dados e Privacidade do G7 (G7, 2022) reconhece que

> [o] uso das PET pode facilitar o compartilhamento seguro, lícito e economicamente valioso de dados que, de outra forma, não seria possível, gerando benefícios significativos para inovadores, governos e o público em geral.

As PET alteram a forma como as organizações coletam, acessam e processam dados (...) são promissoras porque ampliam o acesso à análise de dados e, ao mesmo tempo, aumentam a segurança digital (...).

[12] A OCDE realizou uma conferência ministerial em Ottawa (Canadá) em 1998, sobre a realização do potencial do comércio eletrônico mundial. Nos círculos políticos internacionais, a conferência representou uma das primeiras conferências de grande escala dedicadas à política da Internet. As conclusões da conferência elaboradas há quase 25 anos, em 1998, apelavam especificamente aos governos para que "incentivassem a utilização de tecnologias de aprimoramento da privacidade" (OCDE, 1998).

> Em reconhecimento a esses benefícios [...] as autoridades de privacidade e de proteção de dados do G7 [...] buscarão promover o uso responsável e inovador das PET para facilitar o compartilhamento de dados, com o apoio de medidas técnicas e organizacionais adequadas. (G7, 2022)

A análise da aplicação da *Recomendação do Conselho da OCDE (2013) sobre às Diretrizes que Regem a Proteção da Privacidade e os Fluxos Transfronteiriços de Dados Pessoais* (diretrizes de privacidade da OCDE) salientou a necessidade de examinar as PET e sua aplicação aos fluxos transfronteiriços de dados:

> Os países respondentes à solicitação também concordaram que são necessárias orientações adicionais sobre as salvaguardas técnicas e organizacionais disponíveis. Mais especificamente, os países respondentes e os especialistas salientaram a necessidade de uma análise aprofundada das oportunidades e das barreiras na utilização das novas tecnologias emergentes de aprimoramento da privacidade (PET), incluindo sua aplicação aos fluxos transfronteiriços de dados. (OCDE, 2021)

Embora algumas dessas tecnologias não sejam novas, muitas estão em evolução e podem, em última análise, justificar uma reavaliação das regulações sobre a coleta e o processamento de dados. Como um dos principais desafios, essas tecnologias frequentemente ficam fora do radar dos formuladores de políticas e dos reguladores, dada a natureza altamente inovadora das próprias tecnologias e de suas áreas de aplicação. Além disso, elas são altamente técnicas, criando uma "barreira linguística" significativa entre engenheiros que constroem esses sistemas e formuladores de políticas e reguladores que, em última análise, determinarão como utilizá-las. Essas tecnologias, que estão em diferentes estágios de desenvolvimento e maturidade, provavelmente precisarão fazer parte de marcos de governança de dados mais amplos. Isso deverá garantir que elas sejam utilizadas de acordo com os riscos associados, inclusive os riscos de privacidade, e a segurança dos dados. Os governos e as PET precisarão cada vez mais considerar a forma como os dados pessoais são coletados e processados com o uso das PET e como essas tecnologias se integram em seus marcos de privacidade e proteção de dados.

Paradigmas em evolução

A evolução dos paradigmas para a proteção da confidencialidade, da integridade e da disponibilidade dos dados (segurança de dados) oferece uma boa maneira de contextualizar o cenário em transformação da privacidade e da proteção de dados com relação às novas abordagens das PET. A segurança dos dados está passando por uma evolução significativa. Inicialmente, a segurança buscava proteger os dados no perímetro da organização. Agora, ela está mudando para um novo paradigma de "confiança zero", em que se presume que os agentes mal-intencionados já estejam dentro da organização. A segurança digital, portanto, é realizada por meio do bloqueio de todos os dados, exceto para usos específicos aprovados por pessoas autorizadas. As abordagens de confiança zero na segurança digital ajudam a mitigar o risco de danos que um agente mal-intencionado pode causar se conseguir obter acesso aos recursos digitais internos.

Uma evolução semelhante poderia ser vista como emergente na privacidade e na proteção de dados. Atualmente, a privacidade e a proteção de dados ainda dependem principalmente de regras sobre a forma como os dados podem ser coletados, processados e utilizados. Uma vez que os dados são coletados e/ou transferidos, "os indivíduos perdem a capacidade de controlar a forma como os seus dados são reutilizados e de contestar ou (tecnicamente) se opor a tais usos e podem contar exclusivamente com a aplicação da lei e com a indenização. Os riscos de perda de controle são multiplicados quando os dados são compartilhados posteriormente em várias camadas, especialmente quando essas camadas estão localizadas em várias jurisdições" (OCDE, 2019). Isso aumenta o risco de vazamento e uso indevido de dados em grande escala, como no caso da Cambridge Analytica (Isaak e Hanna, 2018).

A evolução do paradigma de governança de dados possibilitada pelas PET segue uma trajetória semelhante à abordagem de confiança zero na segurança digital: a confiança não é mais pressuposta e os dados pessoais devem permanecer protegidos em um ambiente contraditório. Nesse sentido, as PET podem ajudar a garantir a continuidade da privacidade e da proteção de dados por meios técnicos, mesmo após a coleta e, eventualmente, a transferência de dados para outras organizações, incluindo, eventualmente, a localização dessas entidades fora da jurisdição original. Dessa forma, elas podem complementar efetivamente a proteção oferecida principalmente por medidas legais ou contratuais para essas transferências. Portanto, as PET não devem ser consideradas uma solução mágica para todos os desafios de privacidade e proteção de dados. As PET, por exemplo, não necessariamente ajudam a resolver problemas relacionados a vieses indevidos que possam estar refletidos nos dados originais. Sua utilização também não garante a segurança de todos os sistemas de tecnologia da informação (TI) que dependem dos dados para os quais as PET são utilizadas. Consequentemente, as PET não podem substituir os marcos legais, mas operam dentro deles, de modo que as suas aplicações precisarão ser combinadas com obrigações juridicamente vinculantes e impositivas para proteger a privacidade e os direitos de proteção de dados.

A evolução do paradigma de governança de dados possibilitada pelas PET segue uma trajetória semelhante à abordagem de confiança zero na segurança digital: a confiança não é mais pressuposta e os dados pessoais devem permanecer protegidos em um ambiente contraditório.

Definições e categorizações atuais das PET

PARA UM ENTENDIMENTO COMUM DAS TECNOLOGIAS DE APRIMORAMENTO DA PRIVACIDADE

Embora o conceito de PET esteja longe de ser novo e a sua utilização esteja se espalhando, nunca houve uma definição universalmente aceita. Ao longo dos anos, diferentes organizações elaboraram definições para PET e categorizações das tecnologias correspondentes. Cada uma delas tem seus próprios méritos e requer consideração. No entanto, essas definições e categorizações foram também influenciadas pelo contexto em que foram desenvolvidas, visto que refletem o estado da tecnologia em um determinado momento ou o objetivo de um estudo ou projeto ao qual as PET deram apoio.

A ausência de uma definição estável nesse campo pode dificultar uma análise concertada por parte dos formuladores de políticas e, em particular, das autoridades de proteção de dados sobre os potenciais impactos das PET nas avaliações de privacidade e de proteção de dados.

Para o presente artigo, as PET são entendidas como um conjunto de tecnologias, abordagens e ferramentas digitais que permitem o processamento e a análise de dados, ao mesmo tempo em que protegem a confidencialidade e, em alguns casos, também a integridade e a disponibilidade dos dados e, por conseguinte, a privacidade dos titulares dos dados e os interesses comerciais dos responsáveis pelo tratamento dos dados.

Normalmente, as PET não são ferramentas independentes. Pelo contrário, podem ser utilizadas em conjunto com outros instrumentos organizacionais e jurídicos para implementar objetivos de governança de dados. As PET podem depender uma das outras para funcionar: da mesma forma que os *chefs* usam diversos ingredientes para executar a receita de um prato, as PET são os ingredientes que podem ser combinados para alcançar determinados objetivos de privacidade e proteção de dados.

CATEGORIAS DE TECNOLOGIAS DE APRIMORAMENTO DA PRIVACIDADE (PET)

Com base nas definições e categorizações das PET, esta seção propõe uma nova taxonomia para a classificá-las. Ela associa cada uma das PET (seja ela antiga, emergente ou eventual) a uma categoria de tecnologias que aborda Princípio(s) Básico(s) específico(s) das diretrizes de privacidade da OCDE. Essas categorias são (i) ofuscação de dados, (ii) processamento de dados criptografados, (iii) análises federadas e distribuídas e (iv) ferramentas de *accountability* de dados.

- **As ferramentas de ofuscação de dados** incluem provas de conhecimento zero (*zero-knowledge proofs* [ZKP]), privacidade diferencial, dados sintéticos e ferramentas de anonimização e pseudonimização. Essas ferramentas aumentam as proteções de privacidade alterando os dados, adicionando "ruído" ou removendo detalhes de identificação. A ofuscação de dados permite o aprendizado de máquina que preserva a privacidade e permite a verificação de informações (por exemplo, verificação de idade) sem exigir a divulgação de dados confidenciais. No entanto, as ferramentas de ofuscação de dados podem vazar informações se não forem implementadas com cuidado. Os dados anonimizados, por exemplo, podem ser reidentificados com a ajuda de ferramentas de processamento de dados e de conjuntos de bancos de dados complementares.
- **As ferramentas de processamento de dados criptografados** incluem criptografia homomórfica, computação multipartidária, intersecção de conjunto privado, bem como ambientes de execução confiáveis. As PET de processamento de dados criptografados permitem que os dados permaneçam criptografados durante o uso (criptografia em uso), evitando assim a necessidade de descriptografar os dados antes do processamento. Por exemplo,

ferramentas de processamento de dados criptografados foram amplamente implantadas em aplicativos de rastreamento de ocorrências de COVID-19. No entanto, essas ferramentas têm limitações. Por exemplo, os seus custos de computação tendem a ser elevados, embora estejam surgindo ferramentas que abordam essa limitação.

- **A análise federada e distribuída** permite a execução de tarefas analíticas em dados que não são visíveis ou acessíveis àqueles que executam as tarefas. Na aprendizagem federada, por exemplo, técnica que tem ganhado maior atenção, os dados são pré-processados na fonte de dados. Dessa forma, apenas os sumários das estatísticas/resultados são transferidos para aqueles que executam as tarefas. Os modelos de aprendizagem federada são implantados em escala, como em aplicativos preditivos de texto em sistemas operacionais de dispositivos móveis para evitar o envio de dados sensíveis de volta para o controlador de dados. No entanto, a análise federada e distribuída requer conectividade confiável para operar.
- **As ferramentas de *accountability* de dados** incluem sistemas *accountable*, compartilhamento de segredos limiar e armazenamentos de dados pessoais. Esses instrumentos não visam prioritariamente proteger a confidencialidade dos dados pessoais em um nível técnico e, portanto, muitas vezes não são considerados PET no sentido estrito. No entanto, essas ferramentas procuram reforçar a privacidade e a proteção de dados, permitindo que os titulares dos dados controlem seus próprios dados, definam e apliquem regras sobre quando eles podem ser acessados. A maioria dessas ferramentas está em estágio inicial de desenvolvimento, tem conjuntos limitados de casos de uso e não possui aplicações independentes.

A Tabela 1 apresenta 14 PET que foram identificadas com base em pesquisa e desenvolvimento no setor privado, incluindo instituições acadêmicas como o Instituto de Tecnologia de Massachusetts (Massachusetts Institute of Technology [MIT]). Estão divididas nas quatro grandes categorias apresentadas: (i) ofuscação de dados, (ii) processamento de dados criptografados, (iii) análise federada e distribuída e (iv) ferramentas de *accountability* dos dados. Algumas das 14 PET podem se enquadrar em mais de uma categoria; nesse caso, são atribuídas a uma categoria principal. Note-se também que a maioria das PET, tal como se discute no presente artigo, não endereça o risco de danos para o grupo que resultariam de um eventual uso indevido dos *insights* obtidos a partir da análise dos dados disponibilizados por meio das PET[13]. A Tabela 1 apresenta um panorama das principais oportunidades e desafios das PET.

[13] Para discussões sobre o risco de danos de grupo, ver (Hausman, 2007; Hausman, 2008; Harmon, 2010; Cargill *et al.*, 2016).

Tabela 1 – VISÃO GERAL DOS PRINCIPAIS TIPOS DE PET, SUAS OPORTUNIDADES E DESAFIOS

TIPOS DE PET	PRINCIPAIS TECNOLOGIAS	APLICAÇÕES ATUAIS E POTENCIAIS*	DESAFIOS E LIMITAÇÕES
Ferramentas de ofuscação de dados	Anonimização / Pseudonimização	Armazenamento seguro	• Garantir que as informações não vazem (risco de reidentificação) • Viés amplificado, em particular para dados sintéticos • Aptidões e competências insuficientes
	Dados sintéticos	Aprendizagem de máquina com preservação da privacidade	
	Privacidade diferencial	Ampliação das oportunidades de pesquisa	
	Provas de conhecimento zero	Verificação de informações sem exigir sua divulgação (por exemplo, verificação de idade)	• As aplicações ainda estão numa fase inicial
Ferramentas de processamento de dados criptografados	Criptografia homomórfica	Computação de dados criptografados dentro da mesma organização Computação de dados privados que são muito sensíveis para serem divulgados Rastreamento/descoberta de contatos	• Desafios da limpeza de dados • Garantir que as informações não vazem • Custos de computação mais elevados
	Computação multipartidária (incluindo conjunto privado de intersecção)		
	Ambientes de execução confiáveis	Computação usando modelos que precisam permanecer privados	• Custos de computação mais elevados • Desafios de segurança digital
Análise distribuída e federada	Aprendizagem federada	Aprendizagem de máquina com preservação da privacidade	• Necessidade de conectividade confiável • As informações sobre os modelos de dados devem ser disponibilizadas ao processador de dados
	Análise distribuída		
Ferramentas de *accountability* de dados	Sistemas *accountable*	Definição e aplicação de regras sobre quando os dados podem ser acessados Rastreamento imutável do acesso aos dados pelos controladores de dados	• Casos de uso restritos e falta de aplicações independentes • Complexidade da configuração • Riscos de conformidade relativos à privacidade e à proteção de dados quando são utilizadas tecnologias de registro distribuído • Desafios da segurança digital • Não são consideradas PET no sentido estrito
	Compartilhamento de segredos limiar		
	Armazenamento de dados pessoais / Sistemas de gerenciamento de informações pessoais	Assegurar o controle dos titulares dos dados sobre os seus próprios dados	

Nota: (*) Apenas uma aplicação foi incluída para fins de legibilidade.

Abordagens regulatórias e políticas das PET

As PET são frequentemente abordadas explícita e/ou implicitamente em leis e regulações de privacidade e proteção de dados dos países por meio de: requisitos legais relativos à privacidade e à proteção de dados desde a concepção (*privacy by design*) e por padrão (*privacy by default*); requisitos de desidentificação, segurança digital e *accountability*; e/ou mandatos regulatórios para que as autoridades responsáveis pela aplicação da legislação que rege a privacidade promovam ainda mais a adoção das PET.

Essas medidas são frequentemente complementadas por orientações emitidas pelos governos ou pelas autoridades responsáveis pela aplicação da legislação que rege a privacidade, a fim de esclarecê-las. No entanto, as entidades regulatórias tendem a não adotar posições definitivas sobre os méritos de determinadas PET para cumprir requisitos legais específicos, por exemplo, em transferências de dados transfronteiriços, o que salienta a dificuldade em validar definitivamente soluções PET específicas num cenário em rápida evolução.

Além disso, os países têm adotado uma grande variedade de iniciativas políticas para promover a inovação nas e com as PET. Fazem isso por meio de pesquisa e desenvolvimento tecnológico, adoção de plataformas seguras de processamento de dados, certificação de PET confiáveis, concursos de inovação, "caixas de areia" (*sandboxes*) regulatórias, entre outras, e implantação de soluções de identidade digital.

Conclusões

As PET encontram-se em diferentes fases de desenvolvimento e, provavelmente, terão de fazer parte dos marcos de governança de dados para garantir a sua utilização adequada, em consonância com os riscos associados à privacidade. Muitas dessas ferramentas ainda estão dando os primeiros passos e limitadas a casos específicos de uso em processamento de dados.

Dado o seu caráter inovador e elevado potencial, as PET justificam uma reavaliação abrangente da aplicação da regulamentação sobre coleta e processamento de dados. É importante que essa reavaliação se concentre nos resultados efetivos de privacidade para os quais as PET podem contribuir e não nos processos de utilização de uma PET específica.

Os formuladores de políticas, e as autoridades de proteção de dados em particular, precisarão cada vez mais considerar como o uso das PET pode afetar as avaliações regulatórias de acordo com as estruturas nacionais de privacidade e proteção de dados, levando em conta a contribuição das PET para os resultados de proteção da privacidade.

As PET exigirão ferramentas, testes e procedimentos complementares para garantir que sejam usadas com segurança e em conformidade com a lei em todo o setor econômico.

À medida que as PET amadurecem, haverá uma necessidade crescente de sensibilização e formação para melhor desenhar, construir, implementar, utilizar e auditar essas novas tecnologias.

Dado o seu caráter inovador e elevado potencial, as PET justificam uma reavaliação abrangente da aplicação da regulamentação sobre coleta e processamento de dados.

Será necessária uma cooperação regulatória transfronteiriça e intersetorial mais forte para melhor considerar a evolução tecnológica das PET em termos de proteção à privacidade e dos dados.

Para isso, uma análise de casos concretos de uso das PET, incluindo, entre outras, seu uso visando facilitar a circulação transfronteiriça de dados, pode contribuir para os debates políticos, nomeadamente no que diz respeito à privacidade e aos resultados econômicos que as PET prometem ajudar a alcançar.

Referências

Cargill, S. S., DeBruin, D., Eder, M. M., Heitman, E., Kaberry, J. M., McCormick, J. B., Opp, J., Sharp, R., Strelnick, A. H., Winkler, S. J., Yarborough, M., & Anderson, E. E. (2016). Community-engaged research ethics review: Exploring flexibility in federal regulations. *IRB Ethics and Human Research*, *38*(3), 11-19. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4997782/

Comitê Europeu para a Proteção de Dados. (2020). *Guidelines 4/2019 on Article 25 Data Protection by Design and by Default*. Comitê Europeu para a Proteção de Dados, Bruxelas. https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-42019-article-25-data-protection-design-and_en

Agência da União Europeia para a Cibersegurança. (2021). *Data Pseudonymisation: Advanced Techniques and Use Cases*. Agência da União Europeia para a Cibersegurança, Atenas. https://www.enisa.europa.eu/publications/data-pseudonymisation-advanced-techniques-and-use-cases

G7 (2022). *Communiqué Mesa Redonda das Autoridades de Proteção de Dados e Privacidade do G7: Promovendo o Livre Fluxo de Dados com Confiança e compartilhamento de conhecimento sobre as perspectivas para os Espaços Internacionais de Dados*.

Harmon, A. (2010). Indian Tribe Wins Fight to Limit Research of Its DNA. *The New York Times*. https://www.nytimes.com/2010/04/22/us/22dna.html

Hausman, D. (2008). Protecting groups from genetic research. *Bioethics*, *22*(3), 157-165. http://dx.doi.org/10.1111/j.1467-8519.2007.00625.x.

Hausman, D. (2007). Group risks, risks to groups, and group engagement in genetics research. *Kennedy Institute of Ethics journal*, *17*(4), 351-369. http://dx.doi.org/10.1353/KEN.2008.0009.

Information Commisioner's Office. (2022). *Chapter 5: Privacy-enhancing technologies (PETs)*. Information Commissioner's Office, London. https://ico.org.uk/media/about-the-ico/consultations/4021464/chapter-5-anonymisation-pets.pdf

Isaak, J., & Hanna, M. J. (2018). User data privacy: Facebook, Cambridge Analytica, and Privacy Protection. *Computer*, *51*(8), pp. 56-59. http://dx.doi.org/10.1109/MC.2018.3191268

OCDE (2021). *Report on the Implementation of the Recommendation of the Council Recommendation Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*. OECD, Paris.

OCDE (2019). *Enhancing Access to and Sharing of Data: Reconciling Risks and Benefits for Data Re-use across Societies*. OECD Publishing, Paris. http://dx.doi.org/10.1787/276aaca8-en.

OCDE (2013). *Recomendação do Conselho relativa a Diretrizes que regem a Proteção da Privacidade e dos Fluxos Transfronteiriços de Dados Pessoais*. n. OCDE/Legal 0188, OCDE, Paris. https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0188

OCDE (1998). *Declaração Ministerial sobre a Proteção da Privacidade nas Redes Mundiais*. Revogada em: 18/11/2016. https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0301

Office of the Privacy Commissioner of Canada. (2021). *Privacy Tech-Know blog: Privacy Enhancing Technologies for Businesses*. https:// www.priv.gc.ca/en/blog/20210412/

Casa Branca [Estados Unidos] (2022). *Request for Information on Advancing Privacy-Enhancing Technologies*. https://www.federalregister.gov/documents/2022/06/09/2022-12432/request-for- information-on-advancing-privacy-enhancing-technologies

Entrevista II

Governança de dados para proteção de dados pessoais e políticas de segurança digital na América Latina

Foto: Arquivo Pessoal

Carolina Botero Cabrera
Diretora da Fundação Karisma

Nesta entrevista, Carolina Botero Cabrera, Diretora da Fundação Karisma, aborda os desafios para América Latina e Caribe (ALC) em estabelecer modelos de governança que garantam a privacidade e proteção de dados pessoais, o cenário atual das políticas de segurança digital na região e os fundamentos de uma perspectiva de privacidade baseada em Direitos Humanos.

Panorama Setorial da Internet (P.S.I.)_ Considerando a crescente demanda pelo uso de dados e as possíveis implicações para garantir a privacidade e a proteção de dados pessoais, é possível pensar em um modelo de governança de dados para a região da ALC? Quais aspectos devem ser considerados no desenho de tal modelo?

Carolina Botero Cabrera (C.B.)_ Os países latino-americanos possuem não apenas uma história e experiência semelhantes, mas também compartilham muitas semelhanças em relação ao quadro jurídico. No que diz respeito aos Direitos Humanos, o sistema interamericano estabeleceu um quadro jurídico abrangente que permite à região ter uma referência e desenvolver modelos de governança de dados com características comuns, que garantam não apenas o direito à privacidade, mas também o direito à liberdade de expressão e o acesso à informação, por exemplo. Em relação à privacidade, o primeiro problema é que as leis de proteção de dados, necessárias para se pensar a partir das garantias aos Direitos Humanos e à privacidade, não são homogêneas na região. Por outro lado, os modelos de governança de dados baseiam-se principalmente na ideia de facilitação de modelos de exploração (pensando também nos direitos de maneira individual, a partir do consentimento das pessoas para sua gestão e exploração por parte de governos e entidades privadas) e não a partir da justiça (mesmo pensada de forma coletiva). Portanto, talvez seja necessário pensar se a região da ALC contemplaria outros tipos de visões sobre essa governança.

P.S.I._ Qual o cenário atual das políticas nacionais de segurança digital na região da ALC? Qual sua importância para fazer a gestão de possíveis incidentes de segurança?

C.B._ Quando se trata de políticas nacionais de segurança digital na região, deve-se olhar para a Organização dos Estados Americanos (OEA), que tem

"Os países da região estão em atraso para seguir esse percurso, implementar visões mais amplas e integrais de segurança cibernética à segurança digital, e investir mais recursos para poder responder adequadamente ao desafio."

desempenhado um papel importante na construção e no monitoramento dessas políticas.

A OEA apoiou o desenvolvimento da primeira geração de planos nacionais de segurança digital, os quais, atualmente, estão sendo revisados. Inicialmente, esses planos ecoavam a origem militar dessa disciplina, concentrando-se em infraestruturas críticas relacionadas à segurança nacional e adotando uma visão em que as pessoas eram consideradas destinatárias passivas desses marcos jurídicos que, além de garantir a segurança, eram também uma forma de expressar uma meta de securitização. A função de coordenação e resposta a incidentes foi, consequentemente, influenciada por essa perspectiva.

A OEA realizou algumas avaliações (2016 e 2020) que nos permitem analisar parte do impacto, lições aprendidas e obstáculos enfrentados por essa primeira geração de planos. No entanto, essas avaliações são muito focadas nas infraestruturas estatais, deixando de analisar o impacto sobre as pessoas em geral. O que se percebe é que, nos últimos anos, tem havido uma aproximação mais realista com o setor, que terá impacto nas políticas nacionais.

Consideremos, por exemplo, a maneira como o *ransomware*, quando afeta determinados sistemas de dados (os de saúde, por exemplo), representa um desafio para as políticas de segurança nacional: não só revela fragilidades dos sistemas, mas também da capacidade de resposta do Estado. Trata-se também de um desafio porque é um campo que tradicionalmente está associado aos cibercrimes, mas que tangencia também a segurança digital – embora sejam discussões diferentes, elas se juntam em algumas áreas.

Certamente as estruturas de resposta, como os Grupos de Resposta a Incidentes de Segurança (*Computer Emergency Response Teams* [CERT]) e os Grupos de Resposta a Incidentes de Segurança em Computadores (*Computer Security Incident Response Teams* [CSIRT]), têm possibilitado certo grau de reação e mitigado de alguma forma os impactos. No entanto, percebo que em casos muito graves, como o da Costa Rica[14], ficou evidente que tais estruturas não eram suficientes, e foram outros países e grandes empresas que precisaram prestar os primeiros socorros e contribuir para a recuperação do paciente.

A OEA tem realizado algumas avaliações adicionais, considerando, por exemplo, o problema da demanda de mão de obra e a insuficiência de profissionais nessa área. Trata-se de uma questão global, mas com números específicos na região. Os dados coletados permitem discutir a necessidade de haver também uma perspectiva de gênero para a cibersegurança. Esse foi um primeiro passo para reconhecer a necessidade de mais mulheres atuando nessa área.

Os países da região estão em atraso para seguir esse percurso, implementar visões mais amplas e integrais da segurança cibernética à segurança digital, e investir mais recursos para poder responder adequadamente ao desafio.

[14] Saiba mais: https://en.wikipedia.org/wiki/2022

P.S.I._ Quais os principais desafios para garantir a autonomia e a autodeterminação dos cidadãos sobre a forma como seus dados pessoais são utilizados pelos diferentes atores (públicos e privados)?

C.B._ Trata-se de um campo de múltiplos atores, os quais não têm a mesma capacidade de participação na discussão nem os mesmos recursos para implementar o que é decidido. Por isso, é problemático começar a pensar em garantir a autonomia e a determinação como um terreno nivelado para todos os atores, exceto para os cidadãos.

Como eu disse, não há um compromisso real com a privacidade, pois isso implicaria mudar o modelo econômico (que não é discutido); já em relação à legislação de proteção de dados existente, a opacidade é preocupante.

Embora as leis de proteção de dados tenham aumentado na região, quando buscamos informações sobre como nossos dados são utilizados, os direitos que temos ou a responsabilidade pelo mal uso, as políticas das entidades são ruins, confusas, gerais, quando não inexistentes. Não é possível entender se é feita uma boa ou má gestão dos dados e, ao ocorrerem incidentes, nada acontece.

Nos setores nos quais temos feito monitoramento, não há informações sobre vazamento de dados (quando isso acontece), e menos sobre quando ocorrem incidentes. Além disso, os incidentes não são reportados aos grupos de resposta, não há rotas para denunciá-los, nem recomendações sobre como lidar com eles. Agora, no cenário atual, é difícil pensar que a solução seja obrigar que se façam reportes de incidentes, uma vez que não há a confiança necessária para que isso realmente fortaleça o ecossistema. Talvez, nesse caso, seja importante começar com recomendações e respostas que sirvam como incentivo.

"Embora as leis de proteção de dados tenham aumentado na região, quando buscamos informações sobre como nossos dados são utilizados, os direitos que temos ou a responsabilidade pelo mal uso, as políticas das entidades são ruins, confusas, gerais, quando não inexistentes."

P.S.I._ Como uma perspectiva de privacidade baseada nos Direitos Humanos pode contribuir para a formulação de políticas que mitiguem a reprodução das desigualdades sociais e econômicas?

C.B._ Promover uma perspectiva de Direitos Humanos em que as pessoas estejam no centro significa se preocupar com o que acontece com os dados das pessoas, buscando reduzir seus riscos e dar-lhes mais possibilidade de tomar decisões sobre eles. Esses tipos de perspectivas mudam o cenário. Por exemplo, se adotássemos essa perspectiva, as permissões de um aplicativo seriam do tipo *opt-in* e não *opt-out*, e pediríamos explicações sobre os riscos de privacidade e segurança digital.

Relatório de Domínios

A dinâmica dos registros de domínios no Brasil e no mundo

O Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação (Cetic.br), departamento do Núcleo de Informação e Coordenação do Ponto BR (NIC.br), monitora mensalmente o número de nomes de domínios de topo de código de país (*country code Top-Level Domain* [ccTLD]) registrados entre os países que compõem a Organização para a Cooperação e Desenvolvimento Econômico (OCDE) e o G20[15]. Considerados os membros de ambos os blocos, as 20 nações com maior atividade somam mais 90,39 milhões de registros. Em junho de 2023, os domínios registrados sob .de (Alemanha) chegaram a 17,56 milhões. Em seguida, aparecem Reino Unido (.uk), China (.cn) e Países Baixos (.nl), com, respectivamente, 9,58 milhões, 7,45 milhões e 6,30 milhões de registros. O Brasil teve 5,16 milhões de registros sob .br, ocupando a quinta posição na lista, como mostra a Tabela 1[16].

[15] Grupo composto pelas 19 maiores economias mundiais e a União Europeia. Saiba mais: https://g20.org/

[16] A tabela apresenta a contagem de domínios ccTLD segundo as fontes indicadas. Os valores correspondem ao registro publicado por cada país, tomando como base os membros da OCDE e do G20. Para países que não disponibilizam uma estatística oficial fornecida pela autoridade de registro de nomes de domínios, a contagem foi obtida em: https://research.domaintools.com/statistics/tld-counts. É importante destacar que há variação no período de referência, embora seja sempre o mais atualizado para cada localidade. A análise comparativa de desempenho de nomes de domínios deve considerar ainda os diferentes modelos de gestão de registros ccTLD. Assim, ao observar o ranking, é preciso atentar para a diversidade de modelos de negócio existentes.

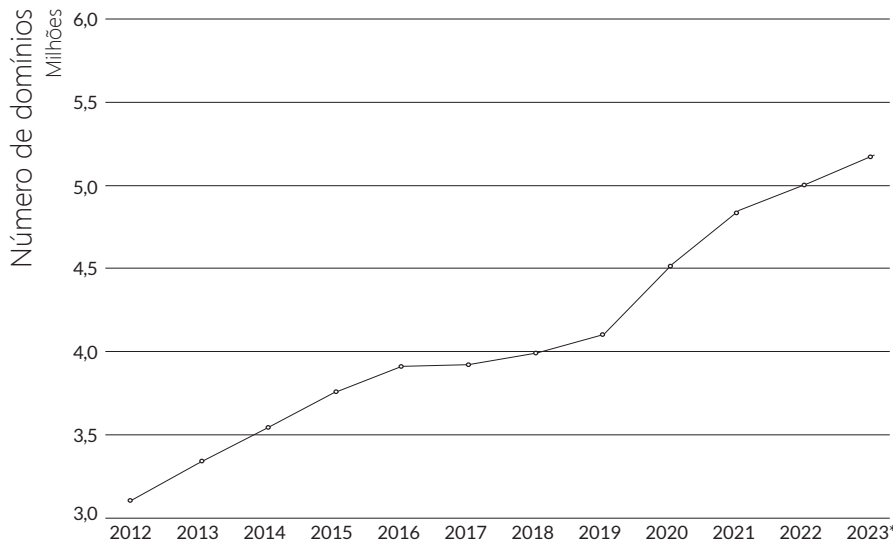
Tabela 1 – TOTAL DE REGISTROS DE NOMES DE DOMÍNIOS ENTRE OS PAÍSES DA OCDE E DO G20

Posição	País	Número de domínios	Data de referência	Fonte (*website*)
1	Alemanha (.de)	17.562.869	03/07/2023	https://www.denic.de
2	Reino Unido (.uk)	9.583.168	31/05/2023	https://www.nominet.uk/news/reports-statistics/uk-register-statistics-2023
3	China (.cn)	7.452.014	03/07/2023	https://research.domaintools.com/statistics/tld-counts
4	Países Baixos (.nl)	6.306.044	03/07/2023	https://stats.sidnlabs.nl/en/registration.html
5	**Brasil (.br)**	**5.169.143**	**30/06/2023**	**https://registro.br/dominio/estatisticas**
6	Rússia (.ru)	5.009.209	03/07/2023	https://cctld.ru
7	Austrália (.au)	4.240.809	03/07/2023	https://www.auda.org.au
8	França (.fr)	4.065.102	01/07/2023	https://www.afnic.fr/en/observatory-and-resources/statistics
9	União Europeia (.eu)	3.660.646	03/07/2023	https://research.domaintools.com/statistics/tld-counts
10	Itália (.it)	3.493.525	04/07/2023	http://nic.it
11	Canadá (.ca)	3.357.415	03/07/2023	https://www.cira.ca
12	Colômbia (.co)	3.350.767	03/07/2023	https://research.domaintools.com/statistics/tld-counts
13	Índia (.in)	2.920.842	03/07/2023	https://research.domaintools.com/statistics/tld-counts
14	Suíça (.ch)	2.549.083	15/06/2023	https://www.nic.ch/statistics/domains
15	Polônia (.pl)	2.518.070	03/07/2023	https://www.dns.pl/en
16	Espanha (.es)	2.059.470	28/06/2023	https://www.dominios.es/dominios/en
17	Estados Unidos da América (.us)	1.900.711	03/07/2023	https://research.domaintools.com/statistics/tld-counts
18	Japão (.jp)	1.742.261	01/07/2023	https://jprs.co.jp/en/stat
19	Bélgica (.be)	1.741.657	03/07/2023	https://www.dnsbelgium.be/en
20	Portugal (.pt)	1.714.217	03/07/2023	https://www.dns.pt/en/statistics

Data de coleta: 03 de julho de 2023.

O Gráfico 1 apresenta o desempenho do .br desde o ano de 2012.

Gráfico 1 – TOTAL DE REGISTROS DE DOMÍNIOS DO .BR – 2012 a 2023*



*Data de coleta: 30 de junho de 2023.
Fonte: Registro.br
Recuperado de: https://registro.br/dominio/estatisticas/

Em junho de 2023, os cinco principais domínios genéricos (*generic Top-Level Domain* [gTLD]) totalizaram mais de 190,32 milhões de registros. Com 159,57 milhões de registros, destaca-se o .com, conforme apontado na Tabela 2.

Tabela 2 – TOTAL DE REGISTROS DE DOMÍNIOS DOS PRINCIPAIS gTLD

Posição	gTLD	Número de domínios
1	**.com**	159.570.312
2	**.net**	12.907.966
3	**.org**	10.760.810
4	**.info**	3.766.205
5	**.xyz**	3.318.500

Data de coleta: 03 de julho de 2023.
Fonte: DomainTools.com
Recuperado de: research.domaintools.com/statistics/tld-counts

Marcadores da Internet no Brasil

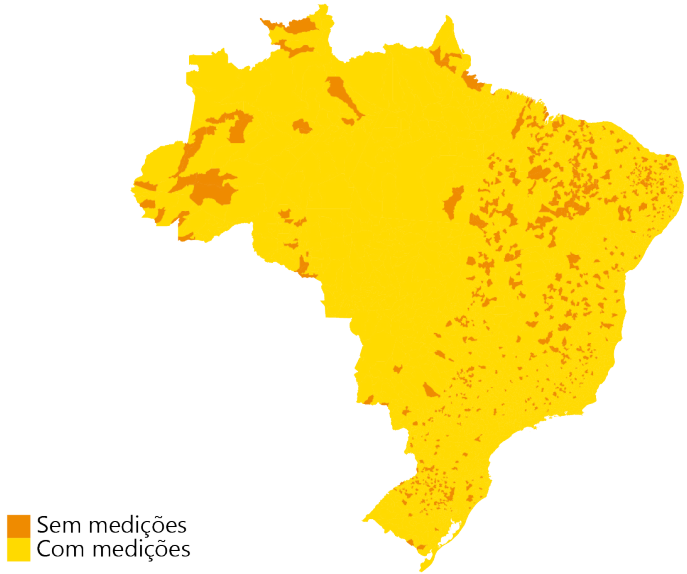
Indicadores do Sistema de Medição de Tráfego Internet (SIMET)[17]

O Centro de Estudos e Pesquisas em Tecnologia de Redes e Operações (Ceptro.br),[18] departamento do Núcleo de Informação e Coordenação do Ponto BR (NIC.br), é responsável pelo SIMET, ferramenta para aferir a qualidade da Internet. Os testes, realizados pelos usuários de maneira instantânea, coletam diversas métricas, como latência, *jitter*, perda de pacotes e velocidade de *download* e *upload*.

A vantagem de utilizar o SIMET é a forma como a qualidade da Internet é aferida. Com base em uma metodologia que visa garantir a isenção e a neutralidade das medições, os testes são realizados primordialmente fora da rede da operadora ou do provedor de acesso, de modo a coletar dados com a melhor qualidade possível da informação.

As medições podem ser feitas a partir dos medidores Web (navegador em qualquer dispositivo com acesso à rede) e *Mobile* (aplicativo disponível para dispositivos móveis). Nos últimos seis meses computados, foram realizadas 666.626 medições, considerando ambas as modalidades. O Gráfico 1 apresenta a cobertura de medições voluntárias usando o SIMET: dos 5.568 municípios brasileiros, 4.676 (84%) tiveram ao menos uma medição no período, ao passo que o Gráfico 2 mostra o número de medições por município.

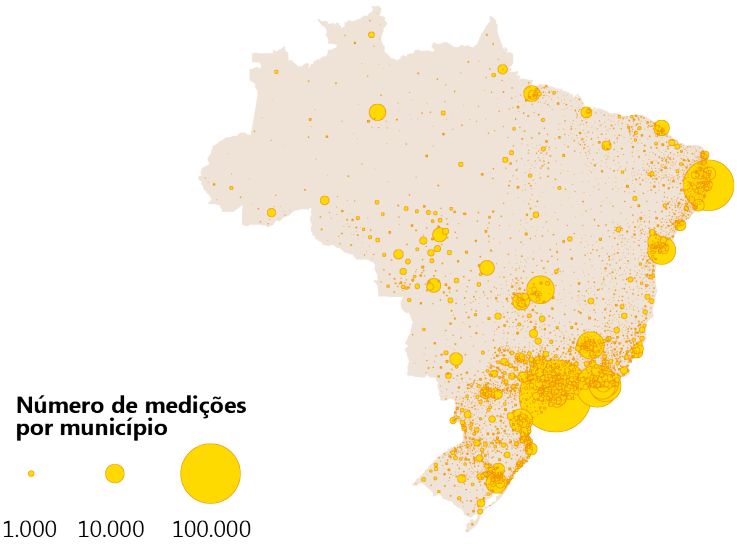
Gráfico 1 – MUNICÍPIOS COM REGISTRO DE MEDIÇÕES A PARTIR DOS MEDIDORES WEB E *MOBILE*



Período de coleta: dezembro de 2022 a maio de 2023.
Fonte: Ceptro.br | NIC.br

[17] Saiba mais: https://medicoes.nic.br/
[18] Saiba mais: https://ceptro.br/

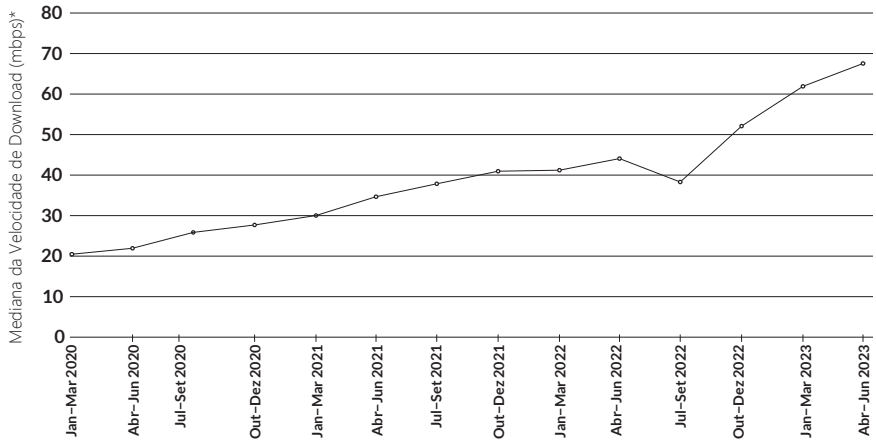
Gráfico 2 – NÚMERO DE MEDIÇÕES A PARTIR DOS MEDIDORES WEB E *MOBILE*, POR MUNICÍPIO



Período de coleta: dezembro de 2022 a maio de 2023.
Fonte: Ceptro.br | NIC.br

A velocidade de *download*, uma das métricas para analisar a qualidade da Internet, refere-se à taxa de transmissão de dados ou velocidade com que ocorrem as transações entre os servidores de medição e o dispositivo medido. Quanto maior a velocidade, melhor a conexão. O Gráfico 3 apresenta a mediana do total de medições de velocidade de *download* por trimestre desde 2020, enquanto o Gráfico 4 mostra a mediana da velocidade de *download* dos últimos seis meses para cada Unidade da Federação (UF).

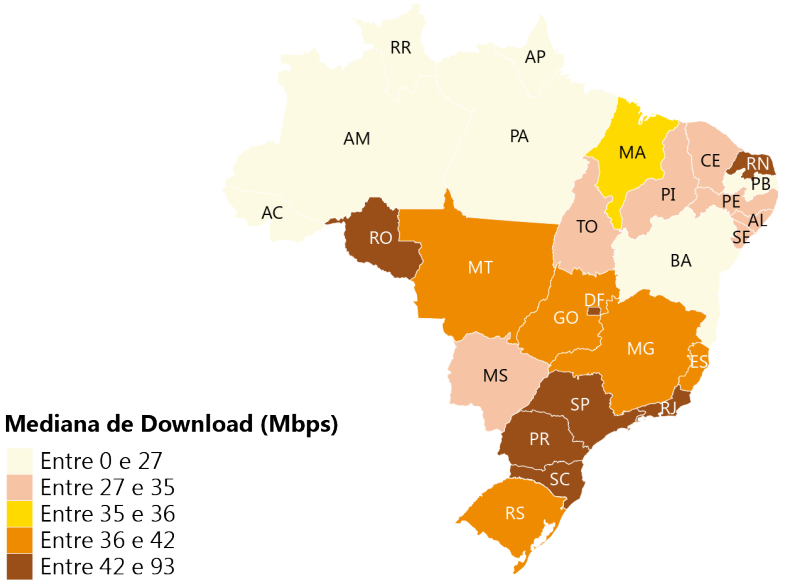
Gráfico 3 – MEDIANA DA VELOCIDADE DE *DOWNLOAD* POR TRIMESTRE – 2020 A 2023[19]



Período de coleta: janeiro de 2020 a maio de 2023.
Fonte: Ceptro.br | NIC.br

[19] As flutuações observadas refletem variações existentes na proporção de medições via medidor *mobile* e medidor web em cada trimestre. Apesar disso, nota-se uma clara tendência geral de incremento na velocidade de *download* ao longo do tempo.

Gráfico 4 – MEDIANA DA VELOCIDADE DE *DOWNLOAD* POR UF



Período de coleta: dezembro de 2022 a maio de 2023.
Fonte: Ceptro.br | NIC.br

As medições são subsídio essencial para fomentar estudos, gerar análises e propor ações para uma melhor Internet. Quanto mais medições forem realizadas em todos os municípios brasileiros, melhores serão as estimativas de qualidade da Internet.

Empresas e a proteção de dados pessoais

Dados da pesquisa TIC Domicílios 2022[20] mostram que, entre os motivos para não realizar compras *online*, cerca de 41 milhões de usuários de Internet no Brasil declararam ter preocupação em fornecer informações pessoais[21].

Em 2021, 78% das empresas no Brasil declararam manter dados pessoais: 67% indicam manter dados de clientes e usuários, 62% de parceiros e fornecedores e 37% de funcionários terceirizados. Os indicadores[22] a seguir apresentam ações[23] adotadas por essas empresas para adequação à Lei Geral de Proteção de Dados Pessoais (LGPD).

EMPRESAS, POR TIPO DE AÇÃO DE ADEQUAÇÃO À LGPD (2021)

Total de empresas que mantêm dados pessoais (%)

32% desenvolveram uma política de privacidade que informa como os dados pessoais são tratados pela empresa;

30% realizaram testes de segurança contra vazamento de dados;

24% ofereceram canal de atendimento para os titulares dos dados, como endereço de *email*, *website*, ou outros canais;

17% nomearam um encarregado de proteção de dados (*Data Protection Officer* – DPO), responsável pela comunicação com os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD).

[20] Dados da pesquisa TIC Domicílios, do Cetic.br|NIC.br. Disponível em: https://cetic.br/pt/pesquisa/domicilios/

[21] Outros motivos para não comprar pela Internet coletados pela pesquisa *TIC Domicílios 2022* podem ser encontrados em: https://cetic.br/pt/tics/domicilios/2022/individuos/H6/

[22] Dados da pesquisa *Privacidade e proteção de dados pessoais 2021: perspectivas de indivíduos, empresas e organizações públicas no Brasil*. Disponível em: https://cetic.br/pt/publicacao/privacidade-e-protecao-de-dados-2021/

[23] Outros tipos de ações de adequação à LGPD coletados pela pesquisa *Privacidade e proteção de dados pessoais 2021* podem ser encontrados em: https://cetic.br/pt/publicacao/privacidade-e-protecao-de-dados-2021/

/Créditos

REDAÇÃO

RELATÓRIO DE DOMÍNIOS
Thiago Meireles (Cetic.br|NIC.br)

MARCADORES DA INTERNET NO BRASIL
Paulo Kuester, Solimary García, Cristiane Millan e Gabriela Marin (Ceptro.br|NIC.br)

PROJETO GRÁFICO E INFOGRAFIA
Giuliano Galves, Larissa Paschoal e Maricy Rabelo (Comunicação|NIC.br)

DIAGRAMAÇÃO
Grappa Marketing Editorial (www.grappa.com.br)

EDIÇÃO DE TEXTO EM PORTUGUÊS
Érica Santos Soares de Freitas

TRADUÇÃO INGLÊS-PORTUGUÊS
Ana Zuleika Pinheiro Machado e Robert Dinham

TRADUÇÃO ESPANHOL-PORTUGUÊS
Ana Zuleika Pinheiro Machado

COORDENAÇÃO EDITORIAL
Alexandre F. Barbosa, Graziela Castello, Javiera F. M. Macaya e Mariana Galhardo Oliveira (Cetic.br|NIC.br)

AGRADECIMENTOS
Carolina Botero Cabrera (Fundação Karisma)

Christian Reimsbach-Kounatze (OCDE)

Manuella Maia Ribeiro, Ramon Silva Costa e Winston Oyadomari (NIC.br)

Organização para a Cooperação e Desenvolvimento Econômico

Rafael Zanatta (Data Privacy Brasil)

SOBRE O CETIC.br

O Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação – Cetic.br (https://www.cetic.br/), departamento do NIC.br, é responsável pela produção de estudos e estatísticas sobre o acesso e o uso da Internet no Brasil, divulgando análises e informações periódicas sobre o desenvolvimento da rede no país. O Cetic.br atua sob os auspícios da UNESCO.

SOBRE O NIC.br

O Núcleo de Informação e Coordenação do Ponto BR – NIC.br (https://nic.br/) é uma entidade civil de direito privado e sem fins de lucro, encarregada da operação do domínio .br, bem como da distribuição de números IP e do registro de Sistemas Autônomos no país. Conduz ações e projetos que trazem benefícios à infraestrutura da Internet no Brasil.

SOBRE O CGI.br

O Comitê Gestor da Internet no Brasil – CGI.br (https://cgi.br/), responsável por estabelecer diretrizes estratégicas relacionadas ao uso e desenvolvimento da Internet no Brasil, coordena e integra todas as iniciativas de serviços Internet no país, promovendo a qualidade técnica, a inovação e a disseminação dos serviços ofertados.

*As ideias e opiniões expressas nos textos dessa publicação são as dos respectivos autores e não refletem necessariamente as do NIC.br e do CGI.br.

unesco
Centro sob os auspícios da UNESCO

cetic.br
Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação

nic.br
Núcleo de Informação e Coordenação do Ponto BR

cgi.br
Comitê Gestor da Internet no Brasil

ISSN - 2965-2642

POR UMA INTERNET CADA VEZ MELHOR NO BRASIL

CGI.BR, MODELO DE GOVERNANÇA MULTISSETORIAL

https://cgi.br

nic.br cgi.br

FOTOS: RICARDO MATSUKAWA E SHUTTERSTOCK