IDENTIDADE DIGITAL E INFRAESTRUTURA PÚBLICA DIGITAL: RECOMENDAÇÕES PARA UMA ARQUITETURA INFORMACIONAL JUSTA

Eduarda Costa Almeida
Pedro Bastos Lobo Martins

REALIZAÇÃO:
DataPrivacyBR Research

APOIO:
ripple

Sobre a Data Privacy Brasil

A Data Privacy Brasil é uma organização que nasce da união entre uma escola e uma associação civil em prol da promoção da cultura de proteção de dados e direitos digitais no Brasil e no mundo.

Fundada em 2018, a Data Privacy Brasil Ensino surge como um espaço para difundir e inovar no conhecimento sobre privacidade e proteção de dados no país. Com conteúdo adaptado para um linguagem mais prática, com exercícios e estudos de caso, esta é uma escola para todos aqueles que se interessam e querem se aprofundar na rica temática da privacidade, proteção de dados e novas tecnologias.

A Associação Data Privacy Brasil de Pesquisa é uma organização da sociedade civil, sem fins lucrativos e suprapartidária, que promove a proteção de dados pessoais e outros direitos fundamentais a partir de uma perspectiva da justiça social e assimetrias de poder.

A partir de 2023, as duas instituições se unem para formar uma única organização, mantendo os mesmos princípios e atividades. Com o apoio de uma equipe multidisciplinar, realizamos formações, eventos, certificações, consultorias, conteúdos multimídia, pesquisas de interesse público e auditorias cívicas para promoção de direitos em uma sociedade datificada marcada por assimetrias e injustiças. Por meio da educação, da sensibilização e da mobilização da sociedade, almejamos uma sociedade democrática onde as tecnologias estejam à serviço da autonomia e dignidade das pessoas.

www.dataprivacy.com.br | www.dataprivacybr.org

Direção

Bruno Bioni, Mariana Rielli e Rafael Zanatta

Coordenação

Carla Rodrigues, Jaqueline Pigatto, Pedro Martins, Pedro Saliba e Victor Barcellos

Equipe

Alicia Lobato, Barbara Yamasaki, Eduarda Costa, Eduardo Mendonça, Gabriela Vergili, Giovana Andrade, Isabelle Santos, Johanna Monagreda, João Paulo Vicente, Larissa Pacheco, Louise Karczeski, Matheus Arcanjo, Natasha Nóvoa, Nathan Paschoalini, Otávio Almeida, Pedro Henrique, Rafael Guimarães, Rennan Willian, Rodolfo Rodrigues e Vinicius Silva.

Imprensa

Para esclarecimentos sobre o documento e entrevistas, entrar em contato pelo e-mail imprensa@dataprivacybr.org

Como citar esse documento

ALMEIDA, Eduarda Costa; MARTINS, Pedro Bastos Lobo. Identidade Digital e Infraestrutura Pública Digital: recomendações para uma arquitetura informacional justa. São Paulo: Associação Data Privacy Brasil de Pesquisa, 2025.

Sumário Executivo

Este relatório examina o impacto de uma Infraestrutura Pública Digital (IPD), especialmente as aplicações de identidade digital, para a proteção de dados pessoais à luz da Constituição Federal brasileira (CF) e da Lei Geral de Proteção de Dados (LGPD). O objetivo é compreender como o ecossistema de IPD e identidade digital se relacionam, tensionam e conformam o exercício de direitos fundamentais, particularmente pela lente da proteção de dados enquanto um direito eminentemente procedimental, que visa estabelecer parâmetros para garantir que o fluxo informacional na IPD seja justo e promotora de direitos.

A crescente digitalização da sociedade e dos serviços governamentais exige a criação de uma IPD robusta e confiável para que as pessoas possam interagir com segurança nas aplicações da infraestrutura. Nesse sentido, a identidade digital funciona como porta de entrada da IPD, e por isso desempenha um papel crucial no acesso a serviços e produtos essenciais. No entanto, o uso de dados pessoais em sistemas de identidade digital levanta preocupações significativas sobre a proteção de dados, a autodeterminação e a potencialização de desigualdades existentes.

Diante da complexidade desse cenário, este relatório funciona como uma ferramenta essencial para a construção de uma IPD que promova um fluxo de dados, inclusive pessoais, justo, inclusivo e com observância do direito fundamental à proteção de dados. O relatório é um chamado à ação para os governos, o setor privado e a sociedade civil, enfatizando a importância da colaboração de vários agentes para garantir que a IPD seja um instrumento de desenvolvimento social e valor público, e não uma ferramenta de controle ou exclusão.

A partir de uma leitura de proteção de dados sobre as aplicações de identidade na IPD, é possível traçar as seguintes conclusões:

- **A proteção de dados é um direito fundamental autônomo no Brasil, reconhecido pelo STF e pela CF, e deve ser considerado no desenho, desenvolvimento e implementação de sistemas de identidade digital na IPD**. Isso não significa a simples coleta de consentimento para qualquer tratamento feito na IPD, por isso a autodeterminação informativa, a proteção contextual dos dados e a separação informacional de poderes

são temas aprofundados neste relatório.

- **A geração de valor público é condição de uma IPD. Só há IPD quando o bem comum e o interesse público é garantido.** Assegurar que as aplicações na IPD atendam às finalidades e direções dessa comunidade garante a legitimidade e sustentabilidade dos resultados alcançados. A simples geração de valor econômico a partir dos dados não garante o alcance do valor público se os direitos dos indivíduos forem negligenciados.

- **A identificação do valor público exige uma compreensão do que a comunidade define como "bem comum".** Esse processo deve ser contextualizado e continuamente atualizado, considerando os princípios, necessidades e objetivos específicos de cada comunidade em um determinado período de tempo a partir de mecanismos de participação cívica. Essa infraestrutura deve ser desenhada e implementada de forma a ser interoperável e beneficiar a sociedade como um todo, e não apenas interesses privados ou setores específicos, permitindo que os diferentes sistemas e atores que integram a IPD possam trocar dados de maneira adequada, sem que haja a captura dessa infraestrutura por um único ou um grupo de atores.

- **Os processos de identificação digital estão em constante mudança, de forma que os riscos associados a uma identidade digital não são apenas a soma dos riscos de identidade e de sua digitalização.** Os processos de identificação podem variar no grau de robustez e contexto de aplicação. Com o avanço tecnológico, foi desenvolvido um modelo de identidade em camadas, onde múltiplos sistemas de identidade se integram e comunicam. Ainda, em processos complexos, a autenticação se baseia em modelos probabilísticos baseados não apenas em dados fornecidos pelo titular, mas também em correlações e dados inferidos. Esse fluxo intenso de dados pode tensionar a compatibilidade entre a finalidade da coleta e os usos posteriores, dos quais o titular não tem conhecimento e possui pouco poder de autodeterminação, exigindo salvaguardas adequadas para que usos secundários sejam compatíveis com os valores normativos da proteção de dados.

- **A autonomia e a autodeterminação informativa asseguram aos indivíduos alguma das condições para exercer a capacidade de desenvolverem suas personalidades livremente**, sem serem submetidos a formas de controle social que anulem sua individualidade. Os titulares devem ter livre acesso aos dados pessoais e a informações claras, precisas e facilmente acessíveis sobre como seus dados estão sendo utilizados para assim, questionarem e se oporem ao tratamento que não estão de acordo. Esses direitos permitem que o fluxo de dados seja co-construído com o titular, podendo gerar bancos de dados de maior qualidade, funcionando, inclusive, como barreiras de contenção a fraude e roubos de identidades.

- **O conceito de privacidade como integridade contextual é crucial para garantir um fluxo informacional justo em sistemas de identidade digital.** A proteção de dados é preservada quando os dados são tratados de acordo com as expectativas razoáveis dos titulares, considerando o contexto específico em que são coletados e utilizados, a pessoa a quem os dados se referem, a entidade que envia os dados e a que recebe, além da natureza dos dados compartilhados.

- **O princípio da separação informacional de poderes deve ser aplicado aos sistemas de identidade na IPD.** O fluxo de dados entre órgãos do Estado deve ser limitado às suas competências e finalidades específicas, evitando a concentração de poder e o desvio de finalidade. O compartilhamento deve atender a uma finalidade específica e que atenda ao valor público, de forma ao tratamento ser condicionado à existência de uma motivação legítima para o outro órgão receber os dados, e deve instaurar procedimento administrativo formal, além de utilizar sistemas eletrônicos de segurança e de registro de acesso.

- **A implementação de mecanismos de proteção de dados e prestação de contas é essencial para garantir um valor público à IPD, além de promover confiança e segurança na infraestrutura.** A proteção de dados, nesse contexto, não se limita ao sigilo e à segurança da informação, mas busca um fluxo de dados seguro e adequado, com uma arquitetura informacional justa e participativa. Isso inclui a observância dos princípios de proteção de dados, direitos dos titulares, e a participação multis-

setorial na construção e manutenção dessa infraestrutura.

- **Na IPD, o consentimento é entendido como uma das bases legais que justificam o tratamento de dados, mas não é a única nem sempre a mais adequada.** Isso ocorre, por exemplo, quando os dados são tratados para operacionalizar políticas públicas, gerar dados para avaliação da efetividade de políticas, promover a transparência pública ou fiscalizar o cumprimento de normas. Nesses casos, o consentimento não pode ser considerado livre, já que o tratamento é necessário para atender a obrigações legais ou interesses de outros agentes, como o Estado. Para além do consentimento, as ferramentas de proteção de dados funcionam como catalisadores de um fluxo informacional justo, garantindo outras bases legais para justificar o tratamento de dados de forma legítima e com as devidas balizas e salvaguardas.

- **A definição de núcleos de responsabilidade no desenvolvimento da IPD evita insegurança e fortalece a confiança na infraestrutura e suas aplicações.** A clareza na definição da responsabilidade de cada agente é fundamental para que os usuários saibam a quem recorrer em caso de danos. A IPD envolve múltiplos atores colaborando em um mesmo ecossistema. Sem a definição de responsabilidades e mecanismos de prestação de contas, pode haver incerteza quanto às regras comuns a todos os atores quando houver necessidade de reparar um dano.

- **A participação ativa de diferentes setores da sociedade é fundamental para o desenvolvimento de uma IPD justa e cidadã, garantindo que os sistemas de identidade atendam ao interesse público.** Ao possibilitar espaços de cocriação, as comunidades podem influenciar ativamente no desenho, implementação e monitoramento dessas infraestruturas. A realização de consultas públicas, a implementação de canais de denúncia e a criação de um conselho de supervisão independente são medidas importantes para promover a participação.

Em resumo, a construção de uma IPD justa, ética e voltada para o interesse público exige uma abordagem colaborativa que envolva os setores público e privado, a sociedade civil e a academia. A implementação de ferramentas de proteção de dados e prestação de contas, além da participação nesse processo, é essencial

para garantir que a IPD seja útil, eficiente e esteja de acordo com os valores da sociedade como um todo. Avaliar riscos, estabelecer regras, ouvir a sociedade, ser transparente e aberto ao escrutínio público gera uma política pública mais assertiva desde o começo e orientada para atender as demandas da sociedade. É diante disso que este relatório contribui para o debate público sobre a IPD no Brasil, oferecendo subsídios para a formulação de políticas públicas que promovam, ao mesmo tempo, a inovação, a inclusão digital e o respeito aos direitos fundamentais.

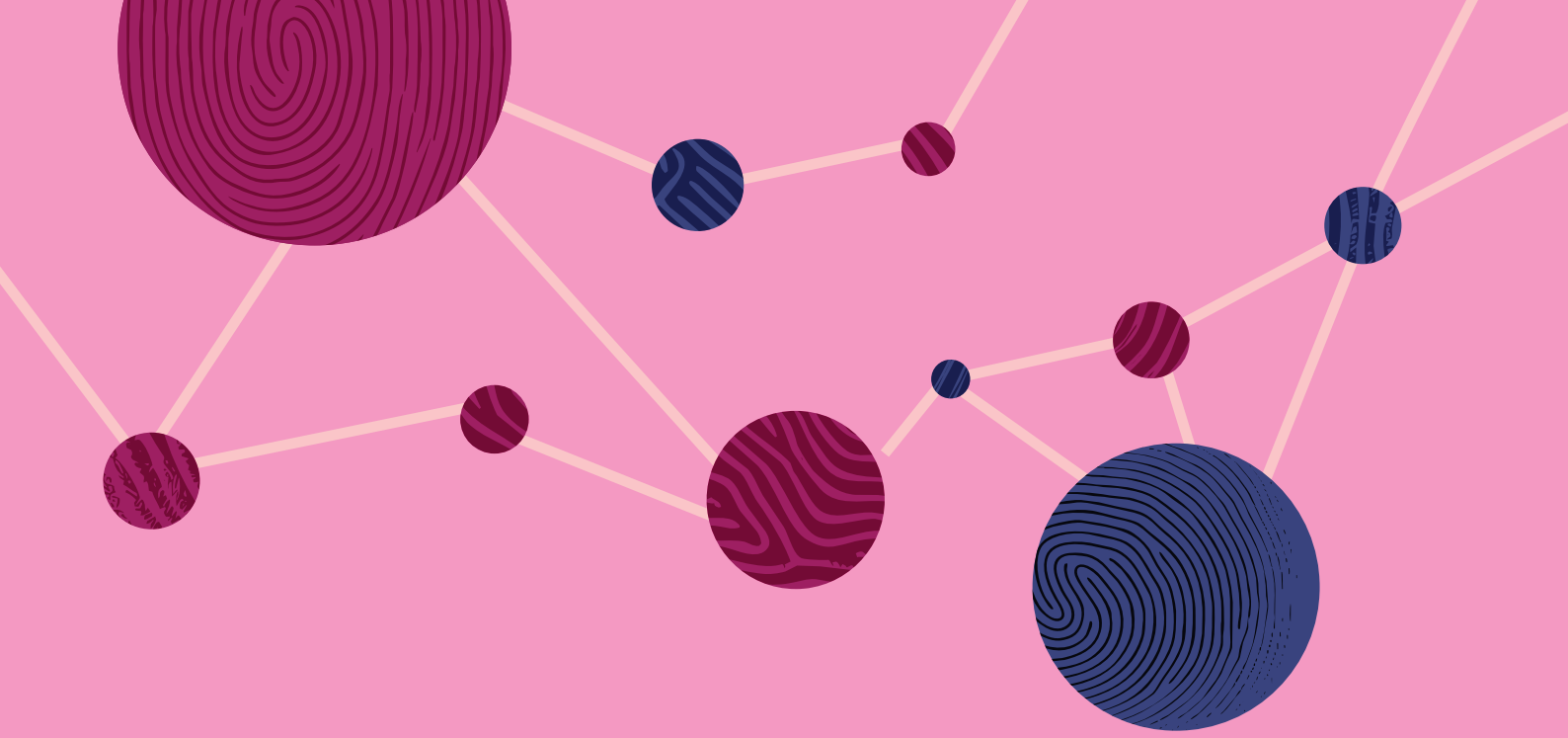
Agradecimentos

Esta pesquisa foi apoiada pela Ripple. O estudo foi enriquecido pela interação com uma comunidade de especialistas e profissionais que têm desempenhado um papel fundamental no debate sobre IPD no Brasil.

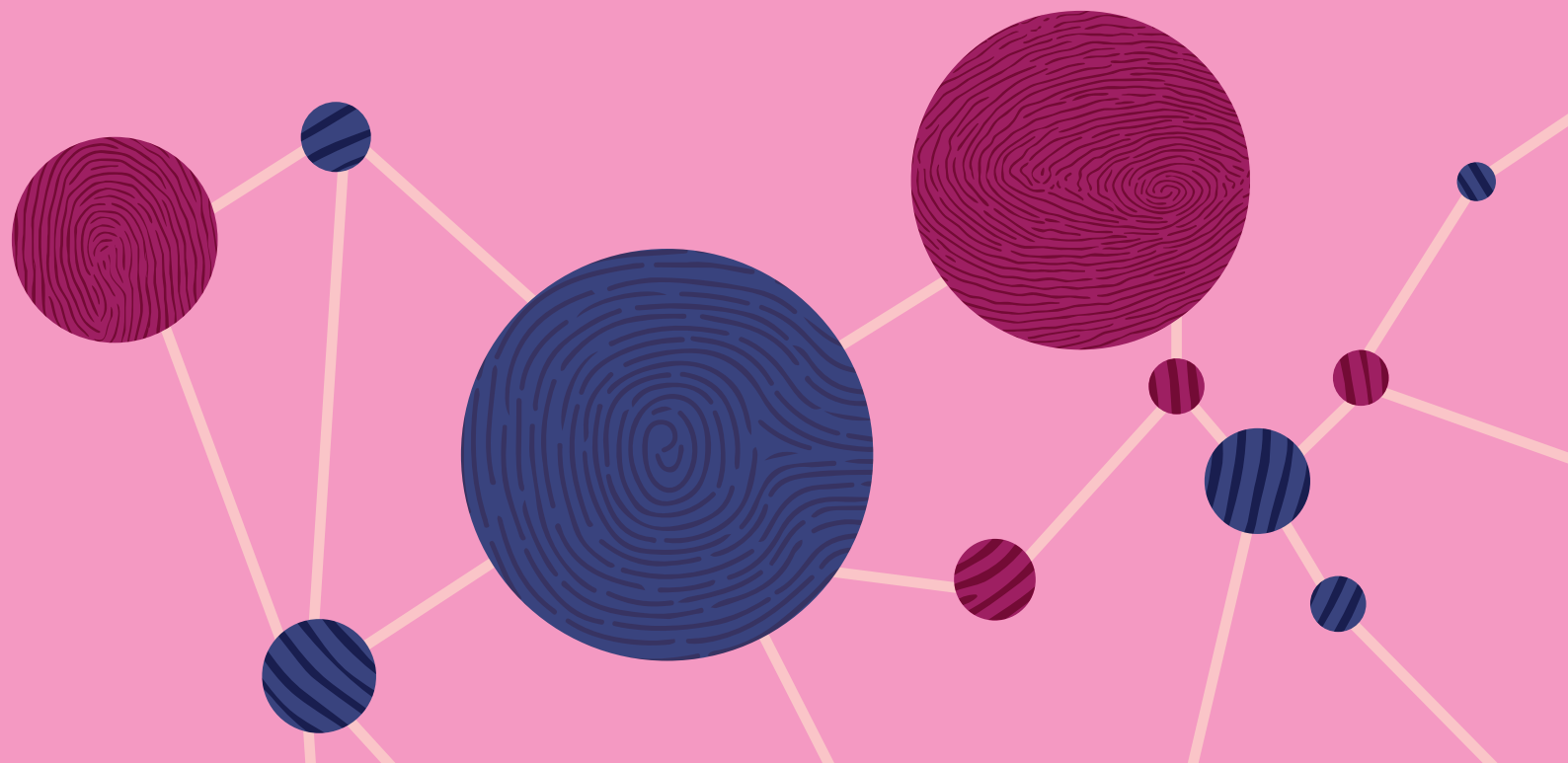
Agradecemos todos os envolvidos nas fases de elaboração deste relatório, especialmente nas entrevistas iniciais de mapeamento de campo, por suas contribuições fundamentais para aprofundamento do tema, além do diálogo aberto e colaboração ao longo deste projeto. Ainda, agradecemos aos especialistas Maria Luciano, Igor Gonçalves, e Hudson Mesquita pelo engajamento e apoio na discussão dos resultados e revisão crítica da versão final do texto.

Também expressamos nossa gratidão aos profissionais que atuam diretamente na área, cuja experiência e perspectivas foram essenciais para o desenvolvimento desta pesquisa. Em especial, agradecemos a todos os participantes da trilha de Identidade Digital, por sua participação no evento "Horizontes Comuns: o papel da infraestrutura pública digital em finanças, identidade e justiça climática" realizado no dia 30 de abril de 2024 e organizado pela Data Privacy, agradecemos os participantes pela generosidade em compartilhar seus conhecimentos e reflexões.

ÍNDICE



01.
CONSIDERAÇÕES INICIAIS



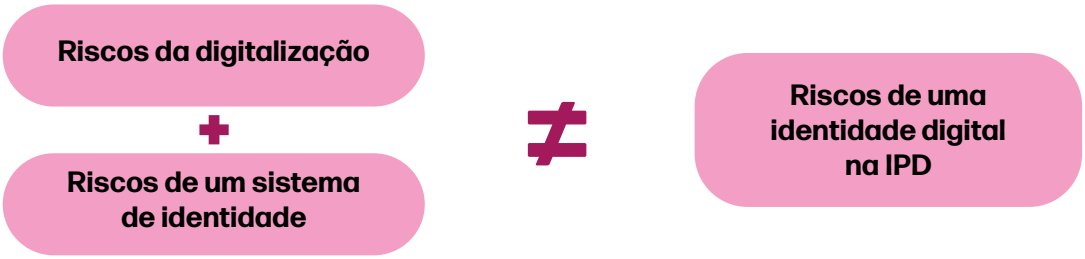
1 Considerações iniciais

A tecnologia tem transformado profundamente as interações humanas, deslocando muitos processos cotidianos analógicos para o digital, incluindo as ferramentas de identificação. Esses processos de identificação digital tornaram-se centrais para o acesso a serviços públicos e privados, a autenticação de transações e participação massiva das pessoas na economia digital, quando necessário.

No entanto, o uso massivo de processos de identificação também amplifica os riscos associados ao uso indevido de dados pessoais, a vigilância massiva e a exclusão digital. A governança de dados emerge, assim, como elemento crucial para equilibrar o adequado uso dos avanços tecnológicos com a proteção dos direitos fundamentais. Por isso, uma governança robusta busca assegurar que os processos de identificação digital respeitem a privacidade, promovam a inclusão e reforcem a confiança dos cidadãos nas infraestruturas digitais para que a IPD possa ser mais uma ferramenta facilitadora à disposição das pessoas.

1.1. Infraestrutura Pública Digital

A partir da moldura de uma infraestrutura pública digital (IPD), este relatório se debruça sobre os obstáculos enfrentados na garantia do direito de proteção de dados desde o desenho até a implementação e acompanhamento de sistemas de identidade digital. Isso porque sistemas de identidade na IPD apresentam riscos para as pessoas que vão além da soma dos riscos de um sistema de identidade e da sua digitalização isoladamente considerados.[1]



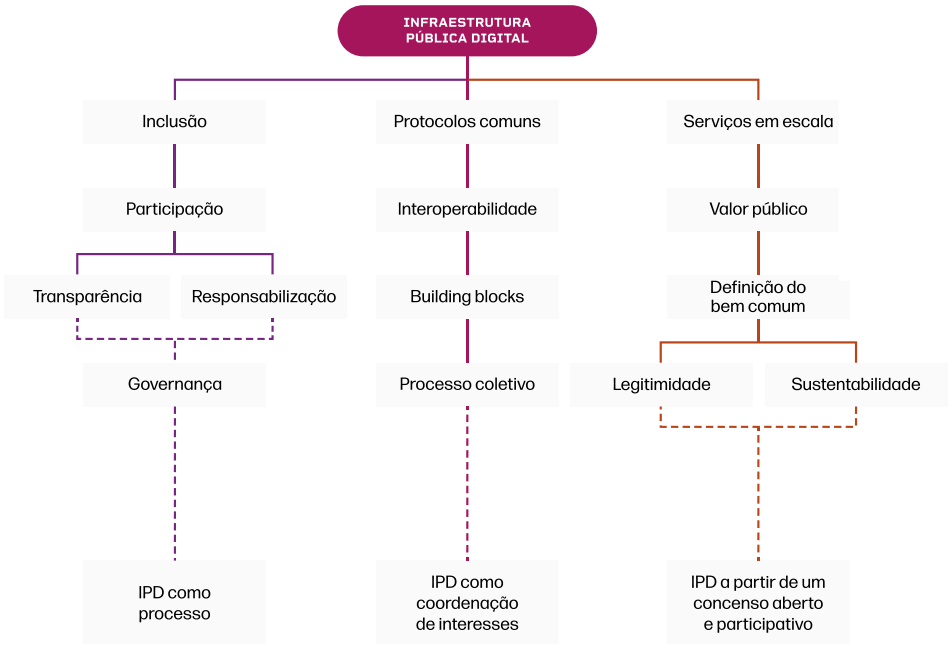
Assim como a infraestrutura física, o desenvolvimento de uma IPD é um caminho possível para garantir o funcionamento de uma organização em acordo com um

1 ALMEIDA, Eduarda Costa; MARTINS, Pedro Bastos Lobo. A Infraestrutura da identidade: os influxos de uma identidade digital como aplicação da IPD. São Paulo: Associação Data Privacy Brasil de Pesquisa, 2024.

valor público, agora também disponível no ambiente digital. É a infraestrutura que garante a disponibilidade dos recursos para apoiar atividades produtivas e promover um desenvolvimento social[2]. Com isso, aplicações de infraestrutura possuem uma maior utilidade enquanto componentes de um conjunto que habilita o funcionamento de um ecossistema digital composto por outras aplicações, como é o caso de soluções de identidade.

Essas aplicações de identidade são elementos fundamentais para uma IPD por garantir a identificação da pessoa que utiliza a infraestrutura e, com isso, permitir que ela acesse qualquer aplicação daquela IPD. Em contextos em que é necessário identificar o usuário na infraestrutura, uma IPD ganha relevância prática por permitir a identificação do usuário de suas aplicações de maneira segura e conveniente.

Enquanto pano de fundo para o desenvolvimento de aplicações de identidade, a noção de IPD mobiliza alguns conceitos chave para compreender as molduras que são criadas nesse processo de digitalização. Apesar de não haver uma definição única sobre o conceito de IPD, este relatório parte do pressuposto de uma IPD como processo construído a partir da coordenação de interesses e de um consenso aberto e participativo. Nesse sentido, uma IPD é definida por concatenar protocolos comuns, interoperabilidade, valor público, bem comum, inclusão e participação a partir de um processo coletivo.



2 CARVALHO, A. C. Infraestrutura sob uma perspectiva pública: instrumentos para o seu desenvolvimento. 2013. 608 f. Tese (Doutorado em Direito) - Faculdade de Direito, Universidade de São Paulo. p. 86.

Um desses conceitos chave da IPD é o da **infraestrutura.** Esse elemento é, por natureza, vago e comporta várias finalidades, isso porque infraestrutura é a fundação que se usa para construir outras aplicações[3]. Exemplos tradicionais de infraestrutura são os sistemas de transporte, composto por rodovias, ferrovias, aeroportos e portos, além dos sistemas de telecomunicação, correio, água ou saneamento básico.

O sentido de infraestrutura também está associado à abordagem de "*building blocks*", ou seja, de blocos de montagens e construção, em que é possível acrescentar aplicações em cima de uma base comum, acomodar mudanças e aumentar as funcionalidades da infraestrutura, permitindo atualizações e aprimoramentos sempre que necessário. Soluções de infraestrutura, em regra, são gerenciadas de forma aberta e acessível, de forma que todos os membros de uma comunidade que desejam usar seus recursos podem fazê-lo em termos iguais e não discriminatórios, mesmo que o acesso não seja gratuito[4].

Ainda, mudanças de infraestrutura são conhecidas por gerarem repercussões significativas, as externalidades positivas, que resultam em grandes ganhos sociais. A ideia tradicional de infraestrutura foi derivada da observação de que os ganhos privados da construção e da expansão das redes de transporte e comunicação também eram acompanhados por grandes ganhos sociais adicionais[5]. Dessa forma, a própria noção de infraestrutura está ligada à produção de um valor que é benéfico aos agentes que a produzem, mas também aos usuários que a acessam, ideia que será destacada neste relatório.

Quando pensada para o contexto de IPD, toda infraestrutura deve permitir que as entidades que participam dela possam interagir livremente [6] e construir módulos independentes. A construção dessa infraestrutura é resultado, majoritariamen-

---

3 ZUCKERMAN, Ethan. What Is Digital Public Infrastructure? Center for Journalism and liberty, 17 nov. 2020. Disponível em: https://www.journalismliberty.org/publications/what-is-digital-public-infrastructure. Acesso em: 27 abril 2024.

4 FRISCHMANN, Brett M., Defining Infrastructure and Commons Management. In: FRISCHMANN, Brett M. Infrastructure: The Social Value of Shared Resources, p. 3, Oxford University Press, 2012, Available at SSRN: https://ssrn.com/abstract=2117460. p. 4

5 FRISCHMANN, Brett M., Defining Infrastructure and Commons Management. In: FRISCHMANN, Brett M. Infrastructure: The Social Value of Shared Resources, p. 3, Oxford University Press, 2012, Available at SSRN: https://ssrn.com/abstract=2117460. p. 5

6 PORTEOUS, David. Is DPI a useful category or a shiny new distraction? 2023. Disponível em: https://www.integralsolutionists.com/is-dpi-a-useful-category-or-a-shiny-new-distraction. Acesso em: 27 abril 2024.

te, da tecnologia utilizada para tanto. Assim, a fim de que essa tecnologia atenda esses sentidos da infraestrutura, é fundamental que ela reflita outros elementos, como escalabilidade, extensividade, abertura e interoperabilidade[7].

O desenvolvimento de uma IPD em protocolos comuns permite que outras funcionalidades possam ser adicionadas a ela e essas possam interagir entre si. A troca de informações entre aplicações da infraestrutura, independentemente das suas origens, pode gerar confiança e facilitar o fluxo seguro de dados. Ao mesmo tempo, a IPD deve poder aumentar suas capacidades e funcionalidades de forma eficiente à medida da demanda, sem comprometer o desempenho ou a qualidade dos serviços oferecidos.

Esses elementos de IPD se traduzem em aplicações de identidade que devem ser reconhecidas por um volume expressivo de agentes do ecossistema da IPD, tornando a solução extensível e escalável. Ainda, em acordo com a interoperabilidade, as informações de identidade e suas validações devem poder transitar entre sistemas, mesmo que em aplicações diferentes. Ou seja, diferentes sistemas devem poder comunicar entre si a partir da definição de padrões comuns e confiáveis.

O **valor público** também é um dos elementos chave da IPD. Isso significa dizer que as aplicações na IPD devem servir ao bem comum maximizando o valor público[8]. No entanto, definir o que é bem comum é um processo contextual e varia de acordo com os princípios, necessidades e objetivos de cada comunidade. A partir do delineamento do que é bem comum, a ideia de valor público ganha objeto e direcionamento específico. Por isso, ainda há bastante disputa sobre o sentido de valor público nas IPD. A título de exemplo, no contexto brasileiro, o valor público da IPD foi apresentado como interesse público, um dos elementos essenciais da IPD, pelo Decreto nº 12.069, de 21 de junho de 2024. O Decreto indica a IPD como solução construída para interesse público, termo explorado pelo direito administrativo brasileiro, que pode ser aproximado do sentido de valor público como construído neste relatório.

---

7 UNDP. The DPI Approach: A Playbook. 21 ago. 2023. Disponível em: https://www.undp.org/publications/dpi-approach-playbook. Acesso em: 27 mar. 2024.

8 MAZZUCATO, Mariana; EAVES, David; VASCONCELLOS, Beatriz. Digital public infrastructure and public value: What is 'public' about DPI? UCL Institute for Innovation and Public Purpose, Working Paper Series (IIPP WP 2024- 05). Disponível em: https://www.ucl.ac.uk/bartlett/public-purpose/publications/2024/mar/digital-public-infrastructure-and-public-value-what-public-about-dpi. Acesso em: 25 abril 2024.

É imprescindível que as aplicações na IPD atendam as finalidades e as direções da comunidade em que estão inseridas. Esse entendimento não só direciona os esforços da construção de uma IPD para demandas concretas, mas também garante a legitimidade e a sustentabilidade dos resultados alcançados[9]. Com isso, a coordenação de interesses no processo é essencial para assegurar que as diversas perspectivas sejam consideradas, promovendo um consenso aberto e participativo sobre o que constitui valor público.

Desvendar o que significa valor público para uma comunidade pressupõe a inclusão e a participação das entidades que a compõem. Isso porque, apenas conhecendo suas necessidades e aspirações, é possível desenhar uma fundação que seja útil para a sociedade. Vale notar que a definição de valor público não é fixada apenas por um grupo que compõe a sociedade e aceita pelos outros, ela é resultado de um processo diverso e coletivo em que há espaços de co-criação e participação efetiva.

Para que o elemento de valor público seja atendido pela IPD, a sociedade deve possuir ferramentas formais e materiais para influenciar no desenvolvimento de suas aplicações, além da sua implementação e acompanhamento. Essa participação é fundamental para impulsionar a inovação e criar soluções centradas nas pessoas e na diversidade dos grupos que compõem essa comunidade. A partir dessa colaboração, objetiva-se garantir que os benefícios do valor público sejam distribuídos de forma equitativa, gerando crescimento inclusivo e compartilhamento dos conhecimentos e das capacidades desenvolvidas no processo[10].

Ainda, o processo de identificar o bem comum perpassa pela implementação de ferramentas de transparência e responsabilização, a fim de se cativar e manter a confiança da comunidade na infraestrutura[11]. A partir desses elementos, é possível controlar e fiscalizar as ações implementadas pelas entidades que compõem a IPD, garantindo que a sociedade possua informações e ferramentas úteis para entender de que forma o valor público está sendo atendido ou não pela IPD.

---

9 MAZZUCATO, Mariana. Governing the economics of the common good: from correcting market failures to shaping collective goals. Journal of Economic Policy Reform, 27(1): 1-24, 2023. DOI: 10.1080/17487870.2023.2280969

10 MAZZUCATO, Mariana; RYAN-COLLINS, Josh. Putting value creation back into "public value": from market-fixing to market-shaping. Journal of Economic Policy Reform, 25(4): 345-360, 2022. DOI: 10.1080/17487870.2022.2053537.

11 UNDP. The DPI Approach: A Playbook. 2023. Disponível em: https://www.undp.org/publications/dpi-approach-playbook. Acesso em: 27 mar. 2024. p. 11.

Também é relevante que as molduras desse valor público sejam revisitadas e definidas em um processo que sofre atualizações. É importante que a mudança dos interesses da sociedade seja refletida no sentido da definição de bem comum e valor público, e, com isso, impacte o direcionamento das aplicações na IPD. É nesse sentido que o desenvolvimento de IPD e de suas aplicações deve ser entendido como processo de coordenação de interesses a partir de elaborações abertas e participativas.

Em vista do potencial transformador da IPD, vários países e entidades internacionais têm se debruçado sobre o tema a fim de criar **conceitos e consensos** para a implementação coordenada e aprendizado mútuo sobre os impactos dessa infraestrutura. O G20 é um dos espaços em que essa discussão tem sido mais frutífera, especialmente durante a presidência da Índia, Brasil e África do Sul.

Diante do impacto dos processos de digitalização, o Governo Federal elaborou a Estratégia Federal de Governo Digital[12] e Estratégia Nacional de Governo Digital[13], já previstas na Lei nº 14.129, a Lei de Governo Digital[14]. A estratégia nacional foi publicada como Decreto nº 12.069, de 2024, responsável por orientar a transformação digital em governos municipais, estaduais e federal, "articular e potencializar as iniciativas de governo digital em todo o país, considerando sua amplitude e diversidade, bem como a redução das desigualdades regionais e com a melhoria do acesso aos serviços públicos"[15].

Esse Decreto indica a Secretaria de Governo Digital (SGD) como responsável por promover o desenvolvimento, a implementação e o uso das IPD, em articulação com vários outros agentes, nomeadamente:

---

12 MINISTÉRIO DA GESTÃO E DA INOVAÇÃO EM SERVIÇOS PÚBLICOS. Estratégia Federal de Governo Digital 2024-2027. Governo Digital. Disponível em: <https://www.gov.br/governodigital/pt-br/estrategias-e-governanca-digital/EFGD>. Acesso em: 7 nov. 2024

13 MINISTÉRIO DA GESTÃO E DA INOVAÇÃO EM SERVIÇOS PÚBLICOS. Estratégia Nacional de Governo Digital. Governo Digital. Disponível em: <https://www.gov.br/governodigital/pt-br/estrategias-e-governanca-digital/estrategianacional>.

14 Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/L14129.htm. Acesso em: 07 nov. 2024.

15 BRASIL. Ministério da Gestão e Inovação. Consulta Pública - Estratégia Nacional de Governo Digital. Brasília, 15 dez. 2023. Disponível em: https://dados.gov.br/dados/conteudo/consulta-publica-estrategia-nacional-de-governo-digital

* Formada por entes federados que aderiram à rede mediante Termo de Adesão assinado pela autoridade máxima do Poder Executivo em nível estadual, distrital ou municipal[16].

Isso mostra uma abertura formal da SGD para que outras entidades sejam ouvidas no processo de desenvolvimento de uma IPD. Essa determinação está diretamente alinhada com as noções de participação pública, elemento chave de uma IPD.

O Decreto também dialoga com outros elementos da IPD no que tange às prioridades da infraestrutura, que podem ser comparadas da seguinte forma:

16 BRASIL. Ministério da Economia. Portaria nº 23, de 4 de abril de 2019. Disponível em: https://www.in.gov.br/materia/-/asset_publisher/Kujrw0TZC2Mb/content/id/70491912/do1-2019-04-08-portaria-n-23-de-4-de-abril-de-2019-70491574#:~:text=Disp%C3%B5e%20sobre%20diretrizes%2C%20compet%C3%AAncias%20e,vista%20o%20disposto%20no%20art. Acesso em 03 de set. de 2024.

Prioridades da IPD segundo o Decreto	Elementos da IPD relacionados
A busca pela universalização do acesso às funcionalidades da IPD, com foco em soluções tecnológicas inovadoras e inclusivas centradas nas necessidades das pessoas.	Infraestrutura escalável, extensiva, aberta, pública, inclusiva e direcionada para valor público.
A adoção de padrões tecnológicos interoperáveis, seguros, escaláveis e economicamente sustentáveis a longo prazo.	Infraestrutura interoperável, escalável e sustentável.
A promoção do compartilhamento seguro de dados, da transparência ativa e da sustentabilidade ambiental, nos termos do disposto na legislação.	Direcionamento para valor público, com parâmetros de transparência e responsabilidade.
A integração de canais digitais e físicos.	Infraestrutura interoperável e escalável, sem abandonar as soluções disponíveis em meio físico[17].
O mapeamento prévio de riscos e a tomada de medidas para sua mitigação, a fim de garantir a adoção de práticas de privacidade, proteção de dados e segurança da informação em todo o ciclo de vida das IPD.	Parâmetros de responsabilidade.

Ainda, o Decreto nº 12.069, de 2024, reconhece como IPD de identificação civil o conjunto de iniciativas do Serviço de Identificação do Cidadão e da Plataforma Gov.br, especificamente quanto à ferramenta de assinatura eletrônica em interações com entes públicos e ao mecanismo de acesso digital único do usuário aos serviços públicos, com nível de segurança compatível ao grau de exigência, natureza e criticidade dos dados e das informações pertinentes ao serviço público solicitado[18].

1.2. Identidade Digital

Um dos pilares do ecossistema da IPD é a identidade digital. Essa forma de identidade é resultado do registro de um conjunto de atributos eletrônicos únicos para atendimento de três funções típicas, dependentes e convergentes entre si, quais

17 UNDP. The DPI Approach: A Playbook. 2023. Disponível em: https://www.undp.org/publications/dpi-approach-playbook. Acesso em: 27 mar. 2024. p. 13.

18 BRASIL. Decreto nº 8.939, de 19 de dezembro de 2016. Disponível em: https://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2016/Decreto/D8936.htm#art3ix. Acesso em 03 de set. de 2024

sejam: identificação, autenticação e autorização.

Para que uma identidade atenda a função de **identificação** é necessário que sejam emitidas credenciais a partir da coleta de informações biográficas. Assim, uma pessoa passa a se identificar com a apresentação e a validação dessas credenciais. É com a identificação que se verifica a existência de alguma duplicidade na emissão da credencial. Em regra, coleta-se algum registro biométrico e emite-se um documento de identificação.

Essa etapa é crítica, já que, se houver alguma barreira ou fricção nela, as próximas funções ficam prejudicadas. Se uma pessoa não é identificada, ela não pode ter sua identidade validada e, consequentemente, passa a não acessar espaços ou serviços destinados a pessoas que passaram pelo processo de identificação.

As outras duas funções da identidade partem do pressuposto que foi possível identificar uma pessoa, e isso destrava as atividades de autenticação e autorização. A autenticação é a funcionalidade de se confirmar ou rejeitar a indicação de que uma pessoa é quem ela diz ser. Em regra, essa verificação acontece baseada em fatores que a pessoa titular de uma determinada identidade diz ter, conhecer ou ser, ou até mesmo na combinação de mais de um fator.

A partir da autenticação da identidade portada, essa identidade permite que a pessoa receba **autorização** para acessar produtos ou serviços específicos, adequados e limitados para o seu nível de acesso. Assim, diante dessas funções da identidade, é possível que entidades que precisam identificar pessoas confirmem, seja durante a integração inicial de um novo identificado, seja de forma contínua, que a pessoa é elegível para acessar um determinado direito, serviço, informação ou funcionalidade do sistema[19]. Dessa forma, é evidente que as funções de sistemas de identidade são exercidas em diferentes momentos para garantir confiança na aplicação utilizada.

19 WORLD BANK. ID4D Practitioner's Guide: Version 1.0. Washington: World Bank License, out. 2019, p. 20. Disponível em: https://documents1.worldbank.org/curated/en/248371559325561562/pdf/ID4D-Practitioner-s-Guide.pdf. Acesso em: 28 jan. 2024.

Informações complementares

Pretensões da ID Digital[20]

Um tipo de identidade digital pode ser um arquivo em uma carteira digital que armazena várias informações confiáveis sobre alguém, ou seja, os seus atributos. Nesse cenário, o titular pode escolher quando e com quem compartilhá-las, sem precisar compartilhar toda a carteira digital. Isso pode incluir a divulgação de detalhes do governo, como nome legal, data de nascimento, direito de residir, trabalhar ou estudar, bem como detalhes de outras organizações, como suas qualificações profissionais ou histórico de emprego.

Outro tipo de identidade digital pode fornecer autenticação de um usuário da internet quando as pessoas precisam provar sua identidade para uma organização terceira. É possível que uma pessoa faça login com segurança em seu provedor de serviços de identidade e, com isso, autorize o compartilhamento de informações apropriadas com a organização terceira. Por exemplo, quando uma pessoa compra produtos com restrição de idade de um varejista on-line sem dizer a sua idade, mas apenas provando que tem mais de 18 anos.

As identidades digitais também podem ser usadas na Internet para provar quem está envolvido em uma transação. Elas eliminariam a necessidade de enviar cópias de documentos para provar quem as pessoas são, com todos os riscos dos dados serem perdidos ou roubados. Em vez disso, as pessoas poderiam usar uma identidade digital para provar algo sobre si mesmas quando estiverem on-line. Também seria possível usar identidades digitais para garantir que a pessoa ou organização com a qual se está lidando seja quem ela diz ser antes de compartilhar qualquer informação.

Em geral, a pretensão da ID digital é colocar as pessoas no controle de quais e quantas informações elas gerenciam e compartilham. Ela proporciona uma maneira de proteger os dados pessoais e pode impedir que as organizações obtenham informações que a pessoa prefira não compartilhar.

20 GOV.UK. UK Digital Identity and Attributes Trust Framework Alpha v1 (0.1). GOV.UK. Disponível em: https://www.gov.uk/government/publications/the-uk-digital-identity-and-attributes-trust-framework/the-uk-digital-identity-and-attributes-trust-framework#introduction. Acesso em: 2 dez. 2024.

Um dos pontos fundamentais da transformação impulsionada por uma IPD é a implementação de uma identidade digital. A IPD e a identidade digital possuem uma relação bastante imbricada: a IPD fornece a base tecnológica e de governança necessária para o funcionamento de sistemas e serviços digitais, ao passo que algumas das aplicações da infraestrutura só podem funcionar se for possível identificar o usuário de maneira segura e conveniente.

Já que parte das relações passa a ser digital, o desafio de se saber com quem essas relações e obrigações estão sendo firmadas ganha novo fôlego. Ou seja, em alguns casos, passa a ser relevante saber se a pessoa que está atrás da tela é realmente quem diz ser. Em algumas aplicações, a identidade é a porta de entrada para o mundo digital, de forma a aumentar a demanda por um processo de validação robusto e confiável.

Soluções de identidade não necessariamente se confundem com processos de *log in* ou *sign on* em um site, diferente desses processos, a identidade visa ser única[21] e está restrita a apenas pessoas reais, o que pode não ser uma regra em outros sistemas[22].

A depender do contexto, os processos de identificação podem variar em graus de robustez. Apesar de objetivarem a identificação, não é comum que, para uma simples compra online, se verifique a identidade do consumidor por meio de um documento expedido pelo Estado. Já para uma transferência bancária, é esperado que se garanta alguns requisitos de segurança e integridade para confirmar a identidade dos sujeitos envolvidos no processo.

Dessa forma, processos de autenticação, e até mesmo identificação, têm sido cada vez mais complexificados, de forma que a identidade passa a se basear não apenas em dados pessoais fornecidos pelo titular, mas tratados a partir de compartilhamentos e cruzamentos de dados advindos de outras fontes.

---

21 OECD. OECD/LEGAL/0491. Recommendation of the Council on the Governance of Digital Identity. 8 jun. 2023. Disponível em: https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0491. Acesso em: 27 jan. 2024.

22 GOV.UK. UK Digital Identity and Attributes Trust Framework Alpha v1 (0.1). GOV.UK. Disponível em: https://www.gov.uk/government/publications/the-uk-digital-identity-and-attributes-trust-framework/the-uk-digital-identity-and-attributes-trust-framework#introduction. Acesso em: 2 dez. 2024.

Primeiras reflexões

Identificação e autenticação em camadas

Com a complexificação dos processos de identidade, a autenticação deixa de ser entendida apenas como a verificação da identidade de uma pessoa, validando se ela é quem diz ser com base nas informações que ela apresenta. Os mecanismos de autenticação passam a influenciar a própria identificação. Ou seja, a autenticação passa a ser um processo de *disclosure* (desvendar a partir do compartilhamento) de informações pessoais entre uma pessoa identificada e os agentes do ecossistema de identidade que visam identificar.

Esse disclosure permite a complexificação do processo de identidade, não mais apenas validando a identidade de alguém com base nos dados biográficos registrados em uma credencial, mas autorizando, por exemplo, uma transação financeira com base na falta de indícios de fraude a partir de outras informações pessoais e padrões comportamentais coletados por outros agentes em contextos e finalidades distintas.

O fluxo intenso de dados está relacionado a um modelo de **identidade em camadas,** em que há a integração de múltiplos sistemas de identidade, os quais o titular se relaciona de forma individualizada, em contextos específicos e para finalidades determinadas. Porém esses sistemas se somam e se comunicam para formar camadas de identidade de alguém. Essas camadas tensionam a compatibilidade entre a finalidade da coleta e os usos posteriores os quais o titular não conhece.

Um dos desafios enfrentados no desenvolvimento de identidade como IPD é a manutenção e promoção da autonomia das pessoas identificadas. Com a integração das bases e a troca de informações entre agentes diversos, as pessoas, gradualmente, perdem seu **poder de agência** intencional sobre elas próprias, com isso, perdem a capacidade de se auto identificar e ser autoral nas suas ações de forma individual ou coletiva[23].

23 ROUVROY, Antoinette. The end(s) of critique: data behaviourism versus due process. In: HILDEBRANDT, Mireille; DE VRIES, Katja (eds.). Privacy, Due Process and the Computational Turn: the philosophy of law meets the philosophy of technology. NewYork: Routledge, 2013. p. 143-167.

O **ecossistema de agentes** que atuam em soluções de identidade também passa a ser complexo e o provedor de identidade deixa de ser o único agente que pode validá-las. Isso porque não necessariamente os dados que compõem a identidade foram apenas aqueles coletados pelo provedor em um primeiro momento. Outros dados, que não o do provedor da identidade, passam a formar a identidade de alguém. Ainda as partes e entidades confiantes passam a autenticar as credenciais emitidas sobre um titular mesmo sem diálogo direto com o provedor, mas apenas com base em outros dados de identificação advindos de outras fontes.

No modelo tradicional, a identificação era baseada em uma lógica binária: a identidade de uma pessoa era validada como sendo "sim, ela é a titular da credencial que está apresentando" ou "não, ela não é a titular da credencial que está apresentando", com base em informações fornecidas diretamente, como um documento ou senha.

Porém, nesses processos complexos, a lógica é de um modelo probabilístico, ou seja, a autenticação não se baseia mais em uma validação direta, mas em percentuais de confiança calculados a partir de diversos dados e correlações. Por exemplo, um sistema pode concluir que há 92% de chance de uma pessoa ser quem ela afirma ser, com base no cruzamento de informações como padrões de comportamento online, biometria e geolocalização.

Nesse cenário, há a prevalência do **compartilhamento** e do cruzamento de dados pessoais coletados pelos mais diversos agentes, em contextos e para finalidades variadas. Um fluxo mais intenso de dados faz com que a atribuição de uma característica a uma pessoa possa também ser facilmente transmissível e usada em outros processos de identificação não relacionados com o inicial. Em uma IPD, esse processo atinge escalas significativas ampliando os potenciais riscos associados a essa lógica do compartilhamento, inclusive permitindo que esses riscos sejam transmitidos entre sistemas diferentes de identificação.

Exemplo hipotético

Identidade como resultado de uma análise probabilística

Maria mora em uma região periférica de São Paulo e está em busca de um empréstimo para abrir seu pequeno negócio de costura. Ela trabalha informalmente e depende de suas redes sociais para vender suas peças de roupa e interagir com potenciais clientes. Como parte de sua vida cotidiana, ela também compartilha detalhes sobre sua vida pessoal, incluindo postagens sobre dificuldades financeiras temporárias e problemas de saúde que enfrentou no passado. Maria utiliza a conta bancária da sua filha para receber transferências relativas aos pagamentos das vendas das roupas, já que ela não possui conta em banco.

Sem saber, os dados que Maria publica em suas redes sociais são compartilhados pela rede com uma empresa de análise de crédito, que os utiliza para definir o score de crédito de indivíduos. Esses dados incluem informações sobre sua localização, suas interações, conteúdo de postagens e comentários que faz em publicações de outras pessoas. A empresa de análise de crédito utiliza um algoritmo que associa postagens de pessoas em áreas economicamente vulneráveis e menções a dificuldades financeiras a um baixo score de crédito. Maria, que já enfrenta desafios por não ter um histórico de crédito formal, acaba sendo prejudicada por essas associações. Ao solicitar o empréstimo em banco que possui recente vínculo, Maria é surpreendida ao ser negada, com o argumento de que seu score de crédito é insuficiente para aprovação.

Mesmo com as contas em dia e com uma ideia promissora de negócio, Maria é penalizada pela forma como seus dados foram interpretados em conjunto. Para tomar a decisão final, o banco somou aspectos da sua identidade, como a localização registrada pelo seu celular, os posts da rede social, conta bancária que é vinculada ao seu celular, além de outros dados como aqueles fornecidos por Maria no momento da solicitação do crédito. O sistema automatizado não levou em consideração a totalidade de sua realidade financeira, mas apenas os dados coletados de forma enviesada disponíveis na infraestrutura digital.

Para garantir autonomia, a estrutura das aplicações de identidade têm sido pensadas, indicando, inclusive, para arranjos descentralizados e modelos de identidade auto soberana. Em observância a essas premissas, as pessoas têm maior poder sobre seus próprios dados de identidade e podem compartilhá-los seletivamente com outras entidades sem depender de uma autoridade central provedora da identidade e de suas validações.

Essa estrutura tem como objetivo garantir um verdadeiro controle do usuário sobre sua identidade, aumentando sua **autonomia**. Para tanto, uma identidade auto soberana deve poder transitar e ser validada, e ela deve permitir que o titular escolha quando deseja divulgar seus dados para um terceiro, quais dados deseja compartilhar, para qual entidade, e para qual finalidade[24].

Para concretizar esses elementos, os **sistemas descentralizados** geralmente utilizam tecnologias de blockchain, um tipo de registro distribuído *(distributed ledger*), para permitir a troca segura de credenciais verificáveis. O *blockchain* fornece essencialmente um domínio descentralizado não controlado por nenhuma entidade individual. Os dados armazenados em qualquer blockchain estão prontamente disponíveis (propriedade de disponibilidade) para qualquer entidade autorizada (propriedade de acesso)[25]. Diante dessas características, uma estrutura descentralizada de identidade estaria vinculada a ferramentas de registro distribuídas.

Além de sistemas descentralizados, outra ferramenta considerada para promover autonomia na IPD que utiliza soluções de identidade é a disseminação de mecanismos de **participação** no desenvolvimento e implementação da infraestrutura e suas aplicações. Desde o desenho da IPD, para que o valor público seja delimitado, até sua concretização e acompanhamento, a participação ativa de diferentes setores da sociedade é uma das chaves para um desenvolvimento seguro e que traduza o bem comum.

Esse engajamento é reconhecido pela Estratégia de Governo Digital, já que o Decreto nº 12.069, de 2024, determina um trabalho conjunto entre a SGD e diversos

---

24 ALLEN, Christopher. The Path to Self-Sovereign Identity. 2016. Disponível em: http://www.lifewithalacrity.com/2016/04/the-path-to-self-soverereign-identity.html. Acesso em: 28 jun. 2024.

25 FERDOUS, Md Sadek; CHOWDHURY, Farida; ALASSAFI, Madini. In Search of Self-Sovereign Identity Leveraging Blockchain Technology. IEEE Access, v. 7, 2019. Disponível em: https://ieeexplore.ieee.org/document/8776589. Acesso em: 28 jun. 2024.

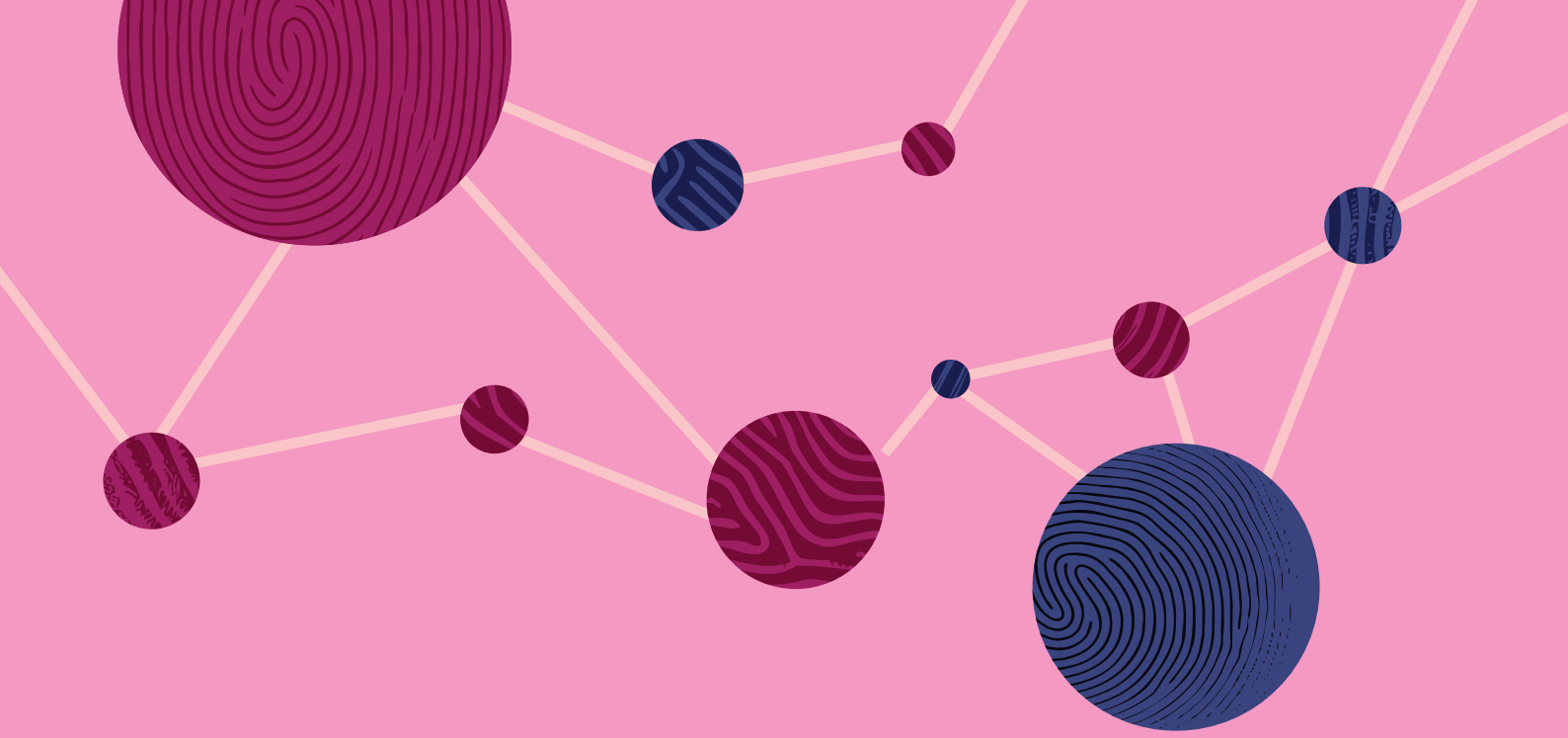
outros setores para a construção de uma IPD. Por meio do engajamento de diversos setores, a relevância da inovação no mercado e a prestação de serviços para potencializar as experiências das pessoas recebem destaque.

É apenas por meio da participação de grupos de empresas, entidades da sociedade civil, associações, consumidores, pesquisadores, acadêmicos e qualquer agente impactado que será possível desenvolver soluções centradas no cidadão, usuário da IPD. A cooperação entre atores permite o desenvolvimento de soluções inovadoras e a sustentabilidade do sistema[26]. Ao permitir que outros grupos contribuam ativamente, é possível que os governos possam criar um ecossistema digital mais dinâmico, sustentável e inclusivo, além de voltado para as necessidades da sociedade em que a IPD está inserida.

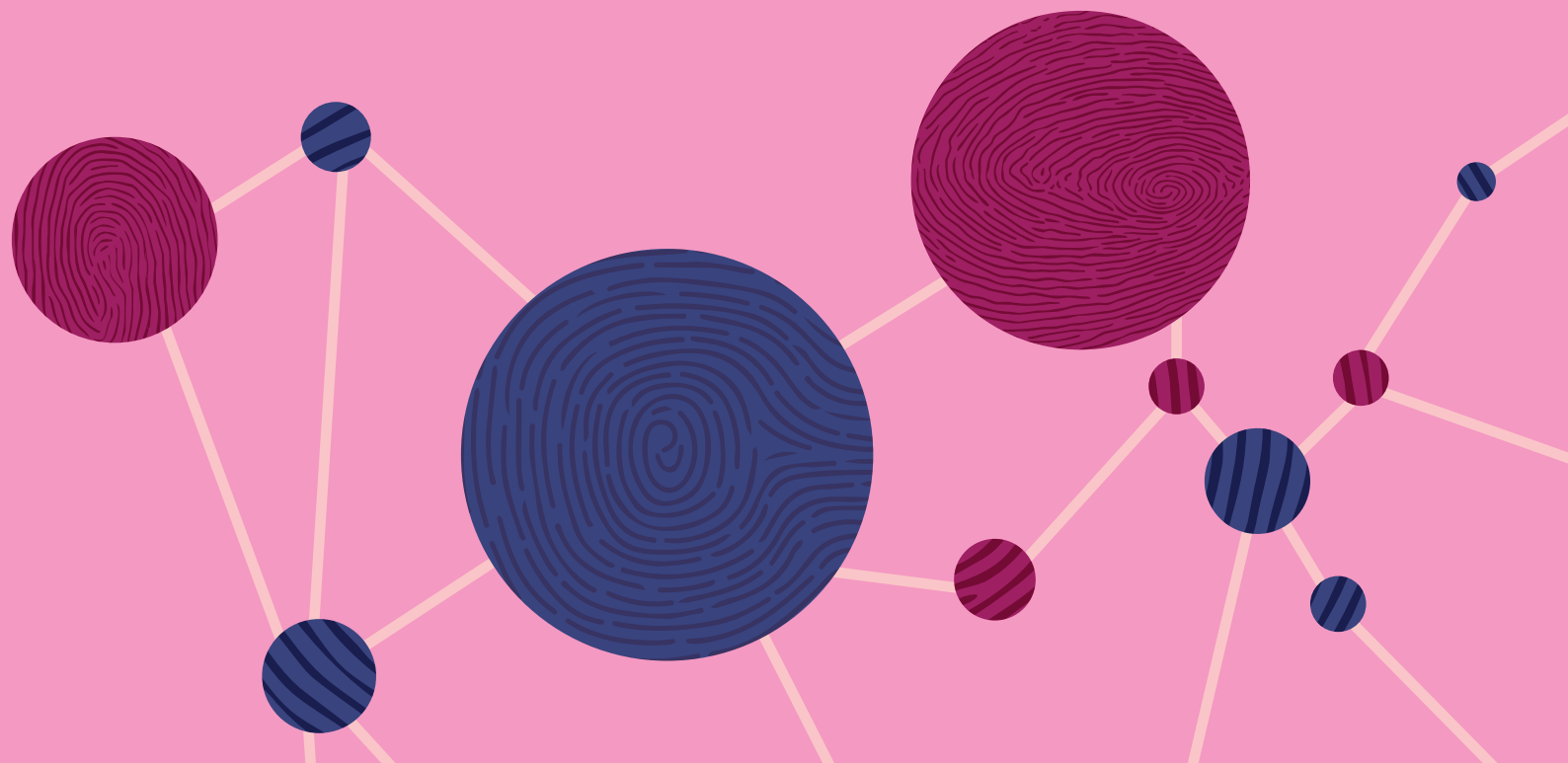
O desenvolvimento de IPD traz diversos benefícios e desafios que devem ser enfrentados para a minimização dos riscos aos direitos das pessoas frente às oportunidades criadas por uma infraestrutura digital. É nesse contexto que este relatório abordará de que forma o ecossistema de IPD e de identidade é percebido pela perspectiva de defesa de direitos constitucionais, especialmente de proteção de dados pessoais.

Para tanto, serão analisadas a gramática constitucional brasileira de proteção de dados pessoais, os elementos normativos que concretizam o direito de proteção de dados, bem como as práticas que orientam o desenvolvimento de aplicações de identidade digital em uma IPD. A partir dos conceitos jurídicos sedimentados na doutrina e na jurisprudência brasileira, é possível identificar balizas e direcionamentos concretos na implementação de aplicações de identidade digital em qualquer nível de uma infraestrutura pública. Essas balizas são fundamentais para garantir um valor público na identidade digital, uma prestação de contas no uso de dados pessoais e uma participação efetiva na IPD.

26 MASSALLY, Keyzom Ngodup, MATTHAN, Rahul, CHAUDHURI, Rudra. What is the DPI Approach? Carnegie Endowment for International Peace, 15 maio 2023. Disponível em: https://carnegieindia.org/2023/05/15/what-is-dpiapproach-pub-89721. Acesso em: 27 jan. 2024.



02.
METODOLOGIA



2 Metodologia

Este relatório busca explorar de que forma a gramática de proteção de dados, especialmente por meio da jurisprudência constitucional brasileira e da lei de proteção de dados, impacta no desenvolvimento de aplicações de identidade em uma IPD.

A hipótese é de que a gramática criada pelo direito de proteção de dados pessoais apresenta parâmetros úteis para garantir um fluxo informacional justo, estabelecendo, a partir de seus princípios, um desenho de arquitetura informacional com parâmetros adequados de governança e *accountability*.

Para compreender a extensão dessa hipótese, esta pesquisa se debruça sobre a gramática de proteção de dados e os conceitos de IPD em vista de três questões complementares:

- A falta de articulação entre os conceitos de uma identidade digital, IPD e a gramática de proteção de dados, especialmente em acordo com a jurisprudência constitucional brasileira;

- O risco de sistemas de identidade serem desenhados de forma a reforçar e ampliar injustiças e assimetrias históricas;

- A necessidade de se implementar os parâmetros normativos de proteção de dados pessoais na construção de IPD como parte de sua estrutura fundante.

Diante disso, este relatório busca compreender os delineamentos da seguinte pergunta: a partir de uma leitura constitucional do direito à proteção de dados, quais medidas de governança devem ser implementadas em um contexto de IPD? Para tanto, são utilizados casos fictícios a fim de ilustrar as tensões existentes em uma IPD com base em situações não reais, mas que guardam alguma semelhança com a realidade e, por isso, podem ser concretizadas no futuro.

Estamos passando por uma janela de oportunidade para o desenvolvimento de identidade digital, diante da disseminação de soluções como o Gov.br e a nova Carteira de Identidade Nacional (CIN). Durante a presidência do G20, o Brasil passou por um momento geopolítico propício para o aprofundamento de temas re-

lacionados à IPD e à digitalização de serviços essenciais. Ainda, não é possível ignorar o impacto massivo de soluções de identidade digital no dia a dia das pessoas, que devem, cada vez mais, passar por processos de identificação e validação de identidade no ambiente digital.

Este documento é o relatório final do projeto de pesquisa "Arquiteturas Cidadãs em Identidade Digital", em que a Data Privacy Brasil buscou mapear a interseção entre uma identidade digital e a proteção de dados em um contexto de desenvolvimento de uma IPD. Por isso, a metodologia deste relatório se confunde com o próprio processo de desenvolvimento da pesquisa.

As seguintes atividades direcionaram o caminho desta pesquisa:

- ***Cards* para o público geral:** para firmar conceitos fundamentais a respeito de IPD e identidade digital, foram produzidos cartões (*cards*) para que qualquer pessoa, mesmo com pouco acúmulo sobre os temas, pudesse entender e situar o debate iniciado pela pesquisa. Com os *cards*, foi possível solidificar os conceitos iniciais e basilares do projeto de pesquisa e publicar um material acessível e de baixa complexidade.

- **Entrevistas exploratórias:** foram conduzidas quinze entrevistas exploratórias junto a especialistas, tanto do setor privado, quanto público, academia e terceiro setor, para mapear estruturas que já estão sendo utilizadas para construir uma identidade digital. As entrevistas foram feitas por videoconferência, não foram gravadas e foram organizadas de forma semi-estruturada. Essa abordagem permitiu insights valiosos sobre os desafios e as oportunidades da interseção entre IPD, proteção de dados, governança de dados, transparência e acesso a uma identidade digital.

- **Evento com especialistas:** iniciou-se um trabalho de construção de campo e construiu-se pontes entre os espaços de desenvolvimento de aplicações de identidade públicos e privados, reunindo tomadores de decisão, especialistas, representantes da sociedade civil e acadêmicos no evento "Horizontes Comuns: o papel da infraestrutura pública digital em finanças, identidade e justiça climática" realizado no dia 30 de julho de 2024, em Brasília. No evento, a Data pode testar os principais pontos de questionamento em uma trilha dedicada ao tema de identidade digital. A trilha contou

com a participação de profissionais que se dividiram em grupos menores para discussões orientadas por perguntas produzidas pela Data Privacy Brasil.

- **Revisão de bibliografia nacional e internacional:** foram analisados os casos concretos já correntes de identidade digital, os benefícios que a identidade digital gera, os riscos a direitos fundamentais, e as possíveis recomendações para o desenvolvimento e a ampliação de uma identidade digital em acordo com os valores de uma IPD. Para tanto, foram analisados conteúdos citados nas entrevistas, além de outros produzidos por atores chave no desenvolvimento de uma IPD e de aplicações de identidade digital.

- **Chamada pública da ONU para o relatório *"Leveraging DPI for Safe and Inclusive Societies"*:** o Secretário-Geral das Nações Unidas para a Tecnologia (ODET) e o Programa das Nações Unidas para o Desenvolvimento (PNUD) publicaram o relatório "Alavancando a IPD para Sociedades Seguras e Inclusivas". A Aapti e a Data Privacy Brasil engajaram no processo para fornecer um feedback sobre o relatório e iniciar um diálogo levando em consideração algumas contribuições sobre proteção de dados e direitos humanos de forma mais ampla. Nessa oportunidade, identificou-se que faltam parâmetros para garantir a participação significativa de diversas partes interessadas ao longo do ciclo de vida da IPD. A versão final do relatório foi publicada em DPI Safeguards.

- **Cartilha "A Infraestrutura da identidade: os influxos de uma identidade digital como aplicação da IPD":** o objetivo era mapear e elaborar sobre a intersecção de conceitos chave que seriam inevitavelmente usados por agentes que atuam no ecossistema de identidade. Eles poderiam reconhecer e aplicar os fundamentos, as aplicações e as funcionalidades de uma identidade digital no contexto de IPD. Na cartilha, a Data Privacy Brasil começou a traçar interpretações próprias sobre IPD e identidade a partir de conexões e parâmetros da organização.

- **Episódio do podcast, Dadocracia, sobre o tema:** o episódio buscou identificar, a partir da percepção dos entrevistados, os principais desafios no debate sobre identidade e infraestrutura pública digital. Para tanto, o

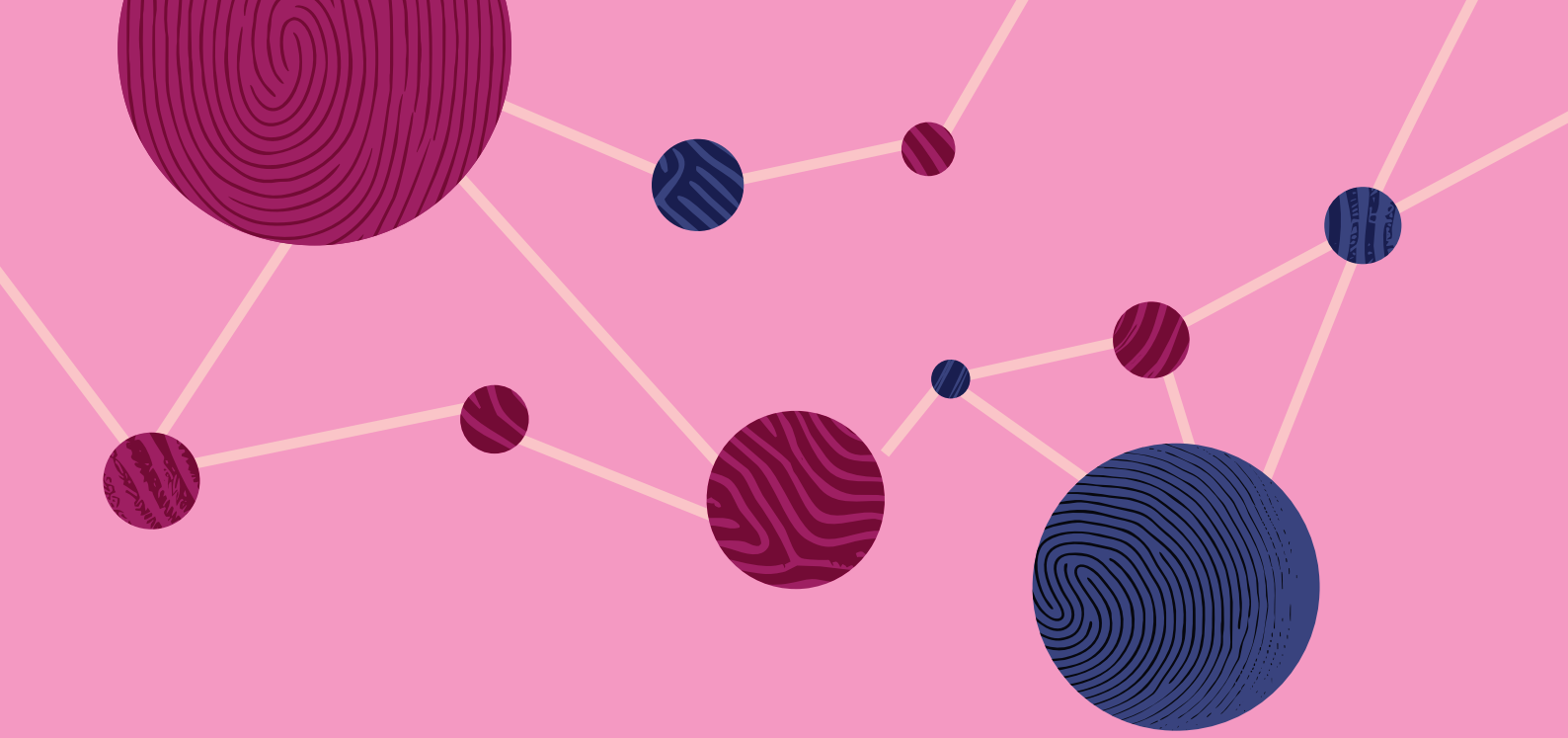
podcast contou com entrevistas com Eduardo Lacerda, coordenador-geral de Identificação Civil da Secretaria de Governo Digital, Pedro Martins, coordenador acadêmico da Data Privacy Brasil, Janaína Costa, especialista em identidade digital e consultora independente, e Yasodara Córdova, especialista em identidade digital e privacidade da Único e parte do board de investimentos do Co-Develop Fund.

A partir desses acúmulos, este relatório foi produzido a partir de uma abordagem proativa da proteção de dados, concebendo-a não como uma regra de sigilo, mas como um componente que fomenta o fluxo informacional justo a partir da fixação de procedimentos e parâmetros pautados na promoção de direitos fundamentais.

Ao envolver os stakeholders-chave, seja do setor privado e do terceiro setor, seja do Poder Público e academia, vinculados à criação de uma IPD, a Data aspira influenciar diretamente o desenvolvimento de políticas públicas no campo. A incidência nesse espaço também é resultado de elaborações e aprofundamentos a partir de publicações de outros agentes sobre o tema. Portanto, e partindo de todo o caminho traçado até aqui, este relatório está dividido em duas grandes seções:

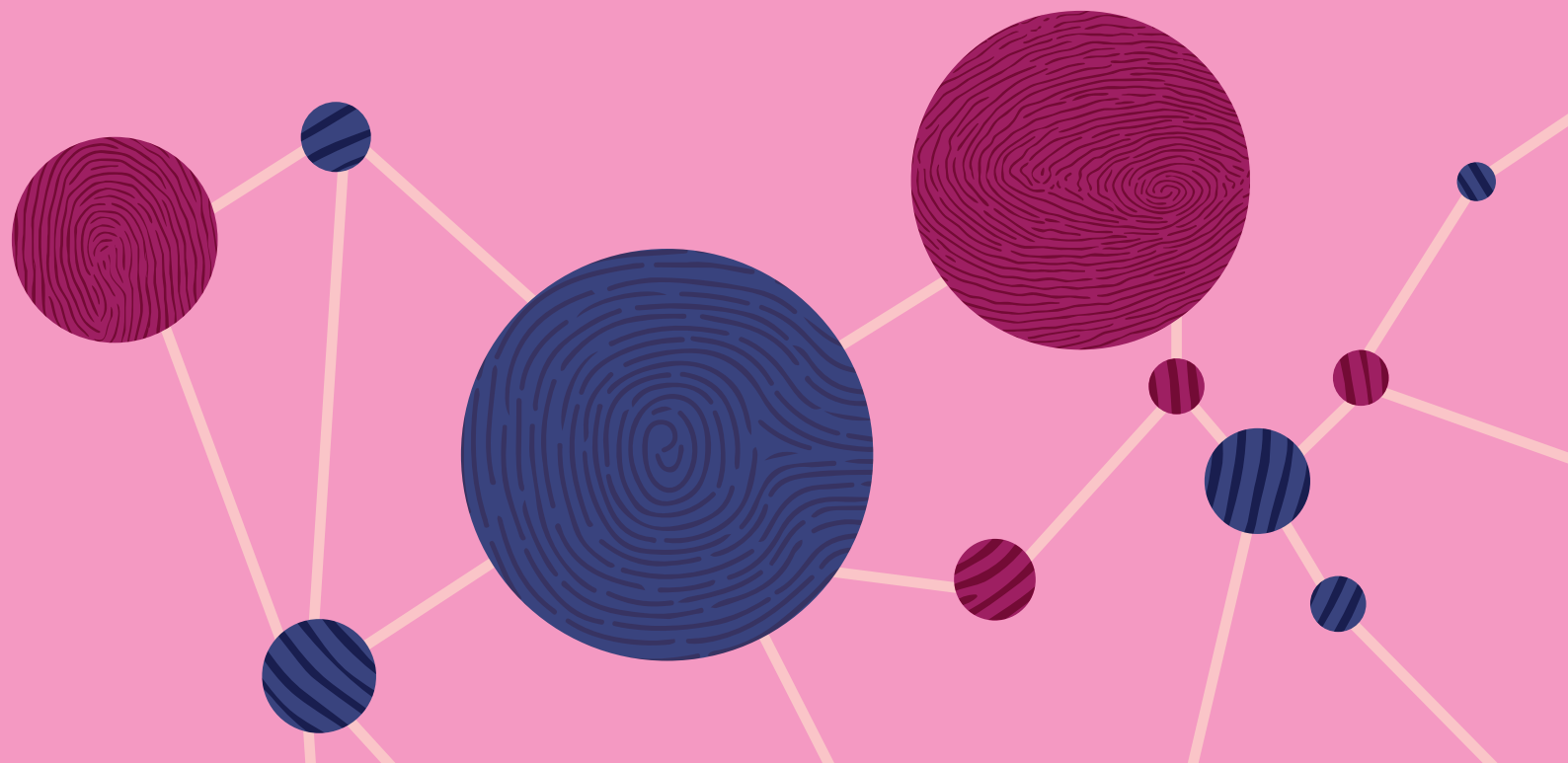
- A primeira versa sobre a gramática de proteção de dados, com atenção à jurisprudência constitucional brasileira, que permeia conceitos de privacidade e proteção de dados, privacidade como integridade contextual e separação informacional de poderes;

- A segunda seção propõe caminhos de procedimentalização das normas em uma IPD voltada para o bem comum a partir de uma leitura constitucional de proteção de dados sobre as aplicações na IPD, especialmente na garantia de um fluxo informacional justo.



03.

GRAMÁTICA CONSTITUCIONAL BRASILEIRA EM PROTEÇÃO DE DADOS



3 Gramática constitucional brasileira em proteção de dados

3.1. Privacidade e Proteção de Dados

O começo das discussões sobre a proteção de dados pessoais encontra raízes na histórica assimetria de poder entre o Estado e o cidadão, onde o avanço das tecnologias impõe desafios ao direito à privacidade. As primeiras gerações de leis de proteção de dados surgiram como resposta a essa disparidade de poder, visando estabelecer limites claros à coleta e ao uso de dados pessoais por autoridades públicas. Com o avanço tecnológico e o crescente processamento de dados, essa assimetria se intensificou, e a compreensão dos direitos fundamentais se expandiu, exigindo novas abordagens e mecanismos de proteção.

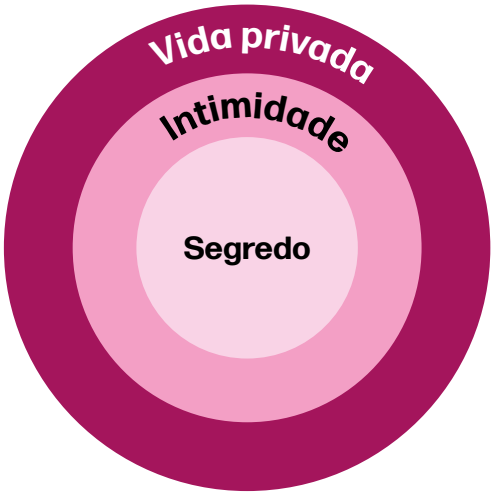
No Brasil, a Lei Geral de Proteção de Dados - Lei 13.709/18 (LGPD) representa uma resposta regulatória para garantir que o uso de dados pessoais ocorra em consonância com os direitos fundamentais de privacidade e proteção de dados, estabelecendo um novo equilíbrio na relação entre Poder Público, entes privados e cidadãos. A própria Constituição Federal (CF), desde sua promulgação, determina um direito à privacidade como direito fundamental relacionado à proteção da intimidade.

O direito de privacidade visa proteger o sujeito para que ele estabeleça um espaço no qual ele "tenha condições de desenvolver a própria personalidade, livre de ingerências externas"[27]. Em um sentido tradicional, o direito à privacidade é associado à manutenção do sigilo de um esfera privada da vida das pessoas, que se opõe à esfera pública. Esse direito à privacidade é uma garantia **individual** de **não intervenção** do Estado, em que o sujeito escolhe não disponibilizar para outras pessoas algumas informações sobre ela mesma, ou seja, é a possibilidade do sujeito escolher deixar informações suas fora do domínio público[28], do conhecimento de terceiros.

27 DONEDA, Danilo. Da privacidade à proteção de dados pessoais. Renovar: Rio de Janeiro, 2006, p. 96

28 BIONI, Bruno Ricardo. Proteção de dados pessoais: a função e os limites do consentimento. São Paulo: Editora Gen, 2019, p. 95.

Nesse contexto, a extensão do direito à privacidade, previsto no art. 5º, X, da CF, estaria limitada a garantir que dados da esfera privada não circulassem em outras esferas sem que o titular tenha dado causa para tanto[29]. Esse âmbito de proteção mais restrito está associado à doutrina de Hubmann, em que três círculos concêntricos representam diferentes graus de manifestação da privacidade, todos sujeitos à proteção.



Nesse esquema, a informação conhecida na esfera pública não poderia ser protegida pelo direito à privacidade. Essa doutrina está alinhada a uma interpretação que reforça a dicotomia entre informação pessoal e informação pública, de forma que a informação pessoal não poderia ser pública e, se o fosse, ela não poderia ser protegida enquanto tal.

No entanto, com o avanço da tecnologia e das formas de processamento de dados, o âmbito de incidência do direito à privacidade foi tensionado, inclusive reinventado[30]. O debate sobre privacidade cada vez mais toca outros conceitos, que ganham relevância própria, como a proteção de dados e a autodeterminação informativa, por exemplo.

O objetivo desse direito passa a ser garantir que a pessoa tenha autonomia para **desenvolver sua personalidade** e não seja "submetida a formas de controle social que, em última análise, anularia sua individualidade, cercearia sua autonomia

29 DONEDA, Danilo. Da privacidade à proteção de dados pessoais. Renovar: Rio de Janeiro, 2006, p. 81

30 RODOTÀ, Stefano. A vida na sociedade da vigilância: a privacidade hoje. Rio de Janeiro: Renovar, 2008, p. 15.

privada e inviabilizaria o livre desenvolvimento da sua personalidade"[31]. Essa proteção é feita a partir de uma ação positiva do Estado que cria regulamentações sobre a forma adequada de se tratar dados em observância aos direitos das pessoas.

Com o tempo, a proteção de dados ganha relevância como uma ferramenta de **distribuição de poder na sociedade**[32]. Ela indica para a incidência de princípios e diretrizes que devem nortear todo tratamento de dados, especialmente garantindo ferramentas de transparência e publicidade, com especificação de propósito legítimos e não abusivos, e regras de compartilhamento de dados, buscando a limitação do tratamento ao mínimo necessário.

A partir de uma noção de proteção de dados, o objeto de tutela não é mais um grupo de dados relacionados à vida privada de um sujeito, mas qualquer dado, inclusive aquele que ele compartilha com outros agentes e que terceiros trocam entre si. Nesse sentido, dados de identificação, como nome, CPF, filiação, endereço, entre outros, apesar de difundidos em formulários, coletados por agentes sem vínculo com o titular, ou mesmo disponibilizados publicamente, estão sujeitos à proteção jurídica. Ainda, mesmo aqueles dados que não identificam unicamente o titular mas podem levar a sua identificação, como localização do dispositivo móvel, hábitos e dados de identificação na internet, passam a ser tutelados.

Diante desse arcabouço apresentado pela proteção de dados, a corte constitucional brasileira se viu em face de debates justamente sobre a tensão entre a privacidade e a proteção de dados. Em maio de 2022, o Supremo Tribunal Federal (STF), no julgamento da Ação Direta de Inconstitucionalidade (ADI) nº 6387, reconheceu **a proteção de dados como um direito fundamental autônomo**. Essa ação teve como objeto a declaração de inconstitucionalidade da Medida Provisória (MP) 954/2020[33]. Essa MP determinava que todas operadoras de telefonia disponibilizassem ao IBGE, em meio eletrônico, os nomes, números de telefone e endereços de milhões de usuários de serviços de telecomunicação.

---

31 DONEDA, Danilo. Da privacidade à proteção de dados pessoais. Renovar: Rio de Janeiro, 2006, p. 141-142.

32 DONEDA, Danilo. Da privacidade à proteção de dados pessoais. Renovar: Rio de Janeiro, 2006, p. 334.

33 PRESIDÊNCIA DA REPÚBLICA. Medida Provisória no 954, de 17 de abril de 2020. Planalto.gov.br. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/mpv/mpv954.htm. Acesso em: 2 dez. 2024.

À época, a intenção era que esses dados pudessem ser utilizados pelo IBGE para que o instituto pudesse produzir estatísticas oficiais durante a situação de emergência de saúde pública do coronavírus. O período de pandemia impedia que o IBGE pudesse realizar pesquisa de campo, diante do isolamento social, e a justificativa do IBGE era de que, com os dados tratados pelas empresas de telecomunicações, seria possível alcançar os cidadãos e realizar entrevistas por telefone.

No entanto, já no julgamento da medida cautelar da ação, a ministra Rosa Weber, relatora, indicou preocupação sobre a conformidade da MP com direitos fundamentais[34]. Um dos maiores riscos identificados pelo tribunal era o de vigilância, em que o compartilhamento de dados pessoais realizado para atingir-se uma finalidade inicial acabasse sendo base para outras atividades de tratamento diferentes desse primeiro propósito. Esse contexto foi suficiente para chamar atenção dos magistrados sobre um possível desvio de finalidade no uso dos dados e o impacto do compartilhamento para os direitos dos cidadãos.

Nesse sentido, o plenário reconheceu que **não existem dados pessoais desprovidos de tutela**, de forma a haver proteção jurídica inclusive para os dados não considerados íntimos ou sensíveis[35]. Ou seja, o direito à proteção de dados é diferente do direito à proteção à intimidade e privacidade justamente por tutelar objeto distinto[36], mais amplo. Com isso, o STF reconheceu o surgimento de um novo direito com dimensão subjetiva e objetiva, em que há deveres de proteção do Estado em garantir que o sujeito mantenha sua esfera de liberdade individual.

Após o julgamento e em acordo com a posição do tribunal, o Congresso Nacional aprovou a **Emenda à Constituição nº 115/2022** para prever expressamente a proteção de dados como direito fundamental elencado no rol do art. 5º da CF. Assim, a proteção de dados pessoais, mais do que uma matéria regulada por norma infraconstitucional, passou a ser direito fundamental de todas as pessoas e, por isso, deve ser observada por todos os agentes que se submetem à Constituição

---

34 SUPREMO TRIBUNAL FEDERAL. Medida Cautelar na Ação Direta de Constitucionalidade 6.387 Distrito Federal. Disponível em: https://portal.stf.jus.br/processos/downloadPeca.asp?id=15342959350&ext=.pdf. Acesso em: 2 dez. 2024.

35 SUPREMO TRIBUNAL FEDERAL. Referendo na Medida Cautelar na Ação Direta de Inconstitucionalidade 6.387 Distrito Federal. Disponível em: https://portal.stf.jus.br/processos/downloadPeca.asp?id=15344949214&ext=.pdf. Acesso em: 2 dez. 2024.

36 MENDES, Laura Schertel. Decisão histórica do STF reconhece direito fundamental à proteção de dados pessoais. JOTA Jornalismo. Disponível em: https://www.jota.info/artigos/decisao-historica-do-stf-reconhece-direito-fundamental-a-protecao-de-dados-pessoais. Acesso em: 2 dez. 2024.

Federal, sejam órgãos públicos, sejam empresas ou organizações privadas.

Isso significa que o desenvolvimento de soluções na IPD, inclusive de identidade, por serem serviços e atividades intensamente ligadas ao tratamento de dados pessoais, também estão no guarda-chuva de atividades que devem observar o direito constitucional à proteção de dados. Diferentemente da privacidade tradicional, esse direito não impõe uma barreira e condições de sigilo ou vedação ao tratamento de dados, mas delimita parâmetros concretos para que o fluxo de dados seja adequado aos princípios da proteção de dados, especialmente o da finalidade, como será analisado neste documento.

3.2. Desenvolvimento da personalidade e autonomia

Associado ao direito fundamental à proteção de dados, outro conceito tensionado pela disseminação de aplicações na IPD é o da **autodeterminação informativa**. Ele também foi citado pela decisão do STF sobre a MP 954/2020 e é um dos fundamentos da LGPD expresso no art. 2º, II. O objeto de proteção jurídica da autodeterminação é o livre desenvolvimento da personalidade em acordo com subjetividade e autonomia de alguém.

Por mais que relacionada à ideia de controle, é importante notar que, assim como o direito à proteção de dados, a autodeterminação não se resume ao processo de tomada de decisão materializada no consentimento do titular. A autorização dada pelo titular para que um terceiro processe seus dados pessoais não é suficiente, adequada ou a única forma de garantir que o titular esteja exercendo sua autodeterminação, ainda mais em contextos de constante fluxo de dados pessoais. Veridiana Alimonti especifica que o fluxo de dados "não depende necessariamente da capacidade do indivíduo de controlá-lo desde o início. Refere-se à sua compatibilidade com disciplina de proteção mais abrangente que estabelece princípios, limites e instrumentos que atentam à perspectiva individual, mas que vão além"[37].

Assim, apesar de "tradicionalmente associada ao aspecto de controle individual sobre dados pessoais, a autodeterminação vai além da possibilidade de reco-

37 ALIMONTI, Veridiana. Autodeterminação informativa na LGPD: antecedentes, influências e desafios. In: DONEDA, Danilo; MENDES, Laura Schertel; CUEVA, Ricardo Villas Bôas (coord.). Lei Geral de Proteção de Dados. A caminho da efetividade: contribuições para a implementação da LGPD. São Paulo: Thomson Reuters Brasil, 2020, p. RB-11.2.

nhecer o titular de dados como mero fornecedor de informações sobre si e seu contexto em contrapartida ao acesso a bens, serviços, políticas públicas e benefícios sociais"[38]. Não é ônus do titular apenas autorizar, consentir com o tratamento de dados, nem mesmo o seu compartilhamento com terceiros, o objeto da autodeterminação vai além do titular agir como agente responsável por controlar seus dados.

Para Rodotà, "a possibilidade de controlar não serve apenas para assegurar ao cidadão a exatidão e o uso correto das informações a ele diretamente relacionadas, mas pode se tornar um instrumento de equilíbrio na nova **distribuição de poder** que vai se delineando"[39]. A autodeterminação justifica um esforço que não é individual, "[r]aramente o cidadão é capaz de perceber o sentido que a coleta de determinadas informações pode assumir em organizações complexas e dotadas de meios sofisticados para o tratamento de dados, podendo escapar a ele próprio o grau de periculosidade do uso destes dados por parte de tais organizações"[40].

Em um mundo digital, se a autodeterminação informativa não é objeto de proteção, outros direitos como o **livre desenvolvimento da personalidade** e a **autonomia** restam comprometidos. Isso porque, esse fundamento visa justamente proteger a capacidade dos indivíduos definirem, por si mesmos, quais são seus interesses e necessidades e como eles devem ser protegidos em uma sociedade justa[41]. A disseminação do uso de tecnologias coloca em risco justamente a capacidade da pessoa ou de grupos não se prenderem a amarras externas que não conseguem superar quando desenvolvem e descobrem suas preferências, características, identidades e interesses.

Essa capacidade das pessoas se auto determinarem é "precondição para uma ordem comunicacional livre e democrática"[42]. Isso porque, enquanto um direito de

---

38 ALMEIDA, Eduarda Costa. Diga-me os seus dados, que eu lhe direi quem você vai ser: o Direito à explicação como garantia da autodeterminação informativa na Lei Geral de Proteção de Dados Pessoais. 2023. 168 f., il. Trabalho de Conclusão de Curso (Bacharelado em Direito) – Universidade de Brasília, Brasília, 2023.

39 RODOTÀ, Stefano. A vida na sociedade da vigilância. A privacidade hoje. Rio de Janeiro: Renovar, 2008, p. 37.

40 RODOTÀ, Stefano. A vida na sociedade da vigilância. A privacidade hoje. Rio de Janeiro: Renovar, 2008, p. 37.

41 QUELLE, Claudia. Not just user control in the General Data Protection Regulation. On the problems with choice and paternalism, and on the point of data protection, Karlstad: Springer, 2017. In: LEHMANN, A.; et al. (orgs.). Privacy and Identity Management - Facing up to Next Steps. Karlstad: Springer, 2017.

42 SARLET, Ingo Wolfgang; SALES SARLET, Gabriele. Separação informacional de poderes no direito constitucional brasileiro. São Paulo: Associação Data Privacy Brasil de Pesquisa, 2022. p. 24

personalidade, é por meio da autodeterminação que uma pessoa passa a ter ferramentas para decidir sobre a disponibilidade de suas informações a terceiros e a desenvolver sua própria personalidade, inclusive diante da noção de grupo, para interagir na sociedade e nos espaços públicos, que também estão sendo digitalizados.

Essa possível limitação da autonomia está vinculada com a definição de perfis a partir do tratamento de dados pessoais em diferentes contextos, conhecidas como práticas de *profiling*. O objetivo dessa prática é garantir que, a partir do tratamento massivo de dados, seja possível **prever e antecipar** acontecimentos, como o próprio comportamento e a identidade humana. O termo *"data behaviourism"* traduz justamente esse processo de produzir conhecimento sobre preferências, atitudes, comportamentos ou eventos futuros sem considerar as motivações psicológicas, os discursos ou as narrativas do sujeito, mas sim com base unicamente em dados[43].

Como consequência, esse processo de profiling com base em dados afeta as oportunidades que estão disponíveis para nós e, consequentemente, o campo de possibilidades que nos define: não apenas o que já fizemos ou estamos fazendo, mas também o que poderíamos ter feito ou poderíamos fazer no futuro[44].

Assim, em um contexto de compartilhamento de dados e IPD, especialmente em relação a estruturas de atribuição e autenticação de identidade, o potencial de uso das correlações entre essas informações abre uma janela para um aumento exponencial na troca, compartilhamento, cruzamento e uso desses dados. Isso porque aplicações na IPD e outras formas de tecnologia estão associadas a um cenário de fluxo de dados, justamente para que as funções de identidade possam ser concretizadas, mas que deve ser justo do ponto de vista de estrutura e implementação.

Ao mesmo tempo em que há intenso fluxo de dados, um dos efeitos desse processo é a lógica probabilística da identificação, em que não é mais necessário ou

---

43 ROUVROY, Antoinette. The end(s) of critique : data-behaviourism vs. due-process. In: HILDEBRANDT, Mireille; DE-VRIES, Katja. Privacy, Due Process and the Computational Turn The philosophy of law meets the philosophy of technology. Oxon: Routledge, 2013. p. 143

44 ROUVROY, Antoinette. "Of Data and Men". Fundamental Rights and Freedoms in a World of Big Data. University of Namur, 2016. p. 22.

viável garantir que a pessoa foi devidamente identificada. Aceita-se uma margem de erro que permite inferir com certo grau de certeza que uma pessoa corresponde a um determinado perfil ou categoria. Essa lógica, embora útil em contextos de alta escala de dados e velocidade no fluxo, como no uso de sistemas automatizados para prevenção de fraudes ou personalização de serviços, pode apresentar riscos significativos para os direitos fundamentais. Isso porque as pessoas passam a ser determinadas com base em pressupostos sobre seus comportamentos ou características que não necessariamente correspondem à realidade, mas que são derivados de correlações estatísticas.

Exemplo hipotético

Identidade como uma probabilidade

Isabela usa o seu cartão de crédito para realizar todas as suas compras diárias. O banco em que Isabela tem conta e concede o cartão coleta metadados das transações financeiras, como o horário da compra, a frequência de compras naquele mesmo estabelecimento, a região da cidade do estabelecimento, o valor das compras, o setor de comércio, entre outros dados. Essas informações podem ser usadas pelo banco para identificar indícios de fraude. Se houver, e essa sinalização for combinada com vários outros indícios, como o perfil de consumo, perfil socioeconômico do titular, o local, horário e valor da compra, é possível que a transação seja identificada como possível fraude, e Isabela seja identificada a partir de uma característica atribuída a ela como provável fraudadora.

Por mais que a característica final atribuída possa ser transmitida para outros agentes, as inferências intermediárias também são, de forma se poder propagar por outros espaços a inferência feita para um contexto específico de detecção de fraude. Em um contexto de IPD, sem as devidas salvaguardas técnicas e de governança, é possível que os dados coletados sobre o uso de cartão de crédito feito por Isabela, bem como dados que indicam fraude, sejam usados para outras finalidades, como o aumento do valor do seguro de cartão ofertado por uma empresa de seguros não vinculada ao banco responsável pelo cartão ou o agravamento dos fatores que indicam a probabilidade da Isabela ser considerada como fraudadora para acesso a um programa de assistência social.

Com a digitalização, as pessoas passam a cada vez menos exercer plenamente o seu **poder de agência** sobre elas próprias. Com o fluxo intenso de dados, os titulares perdem visibilidade sobre quem processa seus dados e para quais finalidades. Isso impede que as pessoas tenham a capacidade de se auto identificar e ser autoral nas suas ações individuais ou coletivas, já que elas passam a ser identificadas com base em dados pessoais transmitidos por elas, mas também dados infra-individuais e de perfis que foram usados para inferir àquela característica.

A identidade digital não é a transposição de uma identidade analógica para o mundo digital. Ela possui suas próprias nuances e significados que vão além de dados biográficos e passam a ser resultado de uma soma de características que fluem na infraestrutura digital.

Nesse novo contexto, há uma mudança na lógica de identificação e posterior validação. A lógica anterior era de que a pessoa teria uma parcela de poder para revelar e saber quais informações sobre ela estão sendo reveladas, como nome completo, CPF, foto de perfil, endereço, etc. Ainda, a pessoa também conhecia e participava do contexto em que aquelas informações seriam usadas. Com a digitalização e automação, a pessoa perde o papel ativo no processo de identificação, passando a ser um objeto a ser identificado por dados que ela não necessariamente conhece e que não são exatamente unicamente sobre ela.

Exemplo hipotético

Controle de acesso a eventos culturais

Luciana deseja assistir a um show em uma grande arena na sua cidade. No passado, o controle de acesso seria feito de forma simples: ela compraria o ingresso, apresentaria um documento de identidade na entrada (se necessário) e teria sua presença confirmada por meio do ingresso físico ou digital. Nesse modelo, Luciana sabia exatamente quais informações estavam sendo reveladas, como por exemplo, nome, número do documento e um comprovante de compra.

Com a digitalização, esse processo foi substituído por sistemas avançados de reconhecimento facial. Ao comprar o ingresso, a empresa que vende o in-

gresso solicita que Luciana envie uma foto que será usada para identificação na entrada. No dia do evento, câmeras instaladas na arena capturam imagens de todos os visitantes, inclusive de Luciana, com sistemas automatizados analisando as características faciais e verificando-as no banco de dados dos ingressos vendidos.

Nesse modelo, Luciana não tem controle sobre quais dados adicionais podem estar sendo coletados além de sua imagem facial. Por exemplo, o sistema pode associar sua presença no evento a dados de geolocalização, horários de entrada e saída, ou até mesmo cruzar essa informação com outros eventos que ela frequentou no passado. Além disso, o sistema pode usar algoritmos de análise que identificam padrões comportamentais, como a forma de andar ou expressões faciais, ou para validar a presença usando informações que a Luciana não forneceu ativamente e pode nem está ciente de que estão sendo usadas.

Esse processo torna a pessoa um objeto de identificação, com base em dados que ela não controla e que podem incluir inferências estatísticas ou correlacionais que extrapolam sua intenção original de apenas assistir ao show.

Essa nova lógica de identificação está próxima de práticas de profiling, em que se tem uma noção da pessoa ser identificada por dados infra-individuais para, a partir disso, formar um perfil supra-individual. Os dois processos posicionam a pessoa como **objeto**, não mais sujeito, em que os dados e o seu perfil não necessariamente são representativos da sua identidade auto declarada. Essa "identidade" é produzida de forma agregada, a partir de dados estatísticos, em que a pessoa perde a capacidade de se autodeterminar e passa a ser um perfil em que é possível predizer seus interesses e comportamentos.

Há uma mudança de posição da pessoa identificada, que antes era alguém que revela informações passando a ser alguém que tem informações reveladas e associadas a ela. No desenvolvimento de IPD e de suas aplicações de identidade, é fundamental que haja mecanismos de subjetivação e reivindicação de uma identidade a fim de garantir uma autodeterminação para a pessoa identificada e, com isso, o exercício do livre desenvolvimento de sua personalidade.

3.3. Proteção contextual

Em um cenário de *big data*, digitalização e desenvolvimento de infraestruturas públicas digitais, além da disseminação de ferramentas de ciência de dados, inteligência artificial, cruzamento e mineração de dados, o impacto do tratamento de informações na vida das pessoas é expressivo.

Informações complementares

Direito de acesso à informação no STF

Para garantir acesso à informação e publicidade dos atos do Estado, o Poder Público passou a disponibilizar na internet informações e documentos para acesso amplo de qualquer interessado. Isso tornou o direito de acesso à informação mais acessível que antigamente, quando os dados eram manipulados fisicamente, mas também possibilitou que outros agentes acessassem e processassem esses documentos e as utilizassem para outras finalidades. Essa disponibilização de registros públicos pelo Poder Judiciário é tema do Recurso Extraordinário com Agravo 1307386, Tema 1141, que será julgado pelo STF.

Diante da alta produção e disponibilidade de dados pessoais, especialmente em um contexto de IPD, quais tipos de proteção e salvaguardas precisam ser desenvolvidas nesse cenário para que esse fluxo informacional traga impactos positivos para a sociedade? Segundo a **teoria da privacidade[45] como integridade contextual[46]**, a proteção da privacidade não é sobre restringir o acesso ao dado pessoal, torná-lo secreto, ou assumir que o titular exerça controle sobre suas próprias informações.

Para essa teoria, a privacidade é preservada quando os fluxos de dados gerados estão em conformidade com as **normas contextuais de informação** aplicáveis

45 Nota-se que no contexto norte-americano, não há diferença expressa entre privacidade e proteção de dados, como apresentado no início deste capítulo. Nesse sentido, a ideia de privacidade contextual, como apresentado pela professora Nissenbaum, deve ser entendida como em linha com a perspectiva de proteção de dados brasileira, não apenas da privacidade em si.

46 Nissenbaum, Helen. Privacy in context: Technology, Policy and the Integrity of Social Life. Stanford: Stanford Law Books, 2010. p. 2

àquele cenário. O pressuposto é de que cada esfera da vida é governada por normas específicas sobre os fluxos de informações adequados, como os âmbitos de atuação de uma pessoa como mãe, estudante e cidadã, que em cada esfera transmite informações específicas e pertinentes àquele contexto. Mas o que seriam essas normas?

Normas contextuais são aquelas que estabelecem **expectativas** para comportamentos característicos a depender de cinco elementos[47]:

- Qual a esfera social do titular? Pessoa a que o dado se refere, se uma professora, candidato a cargo político, criança, mãe, médica, consumidora, policial, amiga, idosa, devedora, religiosa, entre outros.

- Qual a esfera social do remetente? Entidade que inicia o fluxo de dados, se empresa de telecomunicações, órgão público de assistência social, órgão público de saúde, delegacia de polícia, instituição financeira, entre outros.

- Qual a esfera social do destinatário? Entidade que recebe o fluxo de dados, podendo ser do mesmo grupo ou não da entidade remetente.

- Qual o tipo de informação? Dado pessoal que é colocado em fluxo, se o nome da pessoa, endereço, e-mail, gostos pessoais, biometria, filiação, entre outros.

- Há restrições à transmissão? Impedimentos que o fluxo pode ter a depender de outros elementos, como o consentimento ou normas definidas em lei, resolução, práticas, ou contratos.

Assim, os fluxos de informações são considerados adequados na medida em que estão em conformidade com essas normas ou, pelo menos, não as violam. Todos os cinco elementos devem ser levados em consideração em uma avaliação de conformidade do fluxo, já que conformam a norma contextual que indica a viabilidade do fluxo ocorrer.

---

47 Nissenbaum, Helen. Contextual Integrity Up and Down the Data Food Chain, 20 Theoretical Inquiries L. 221 (2019). p. 229.

Por outro lado, a análise sobre esses cinco fatores resolveria também situações novas em que não há uma permissão ou restrição à transmissão tão clara? Diante de uma interpretação dura, essa teoria levaria para uma presunção sempre favorável apenas aos fluxos de dados já consolidados pela sociedade. Novas formas de trocar informações poderiam ser entendidas como inadequadas[48].

A teoria indica que, para além do mapeamento desses cinco elementos, é necessário analisar o interesse das partes afetadas, os valores políticos e éticos, além dos propósitos e valores contextuais, para que seja possível perceber se o fluxo de dados está adequado à privacidade ou não.

Da perspectiva dos **interesses**, valores éticos e políticos, passa-se a ser necessário analisar elementos como quem é beneficiado e quem é prejudicado com o tratamento, como os interesses e preferências dessas pessoas são atendidos, além de se identificar quais são os custos e quais são os benefícios. Essas questões objetivam entender se há risco de roubo de identidade, constrangimento, ou desbalanceamento de poder ou diminuição da capacidade de modular seus relacionamentos ou de se autodeterminar.

Quanto aos **propósitos e valores contextuais**, deve-se levar em conta as legítimas expectativas do titular sobre o fluxo de informação no contexto em que são tratados. Nesse sentido, é importante frisar que o tráfego de dados não ocorre no vácuo, mas sim sob um conjunto de circunstâncias que orientam a integridade do fluxo[49]. Assim, mesmo após a consideração dos cinco parâmetros sobre a adequação do fluxo de dados, deve-se analisar a **legitimidade** do fluxo a partir dos interesses, valores sociais e fins e valores contextuais do tratamento que iniciou o fluxo. Isso porque a privacidade contextual tem como premissa confrontar os tratamentos de dados pessoais em que há uma distância expressiva entre uma expectativa contextual e a prática daquele agente que trata os dados.

---

48 BIRNHACK, Michael D. A quest for a theory of privacy: context and control. Disponível em http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1824533. Acesso em 08 set. 2024. p. 21.

49 BIONI, Bruno Ricardo. Proteção de dados pessoais: a função e os limites do consentimento. Rio de Janeiro: Forense, 2019. p. 216

Exemplo hipotético

Fluxo de dados de saúde

Joana está procurando auxílio médico para investigar sintomas de uma infecção alimentar após ter comido em uma grande rede de restaurantes de sua cidade. Para tanto, ela realizou uma consulta com a médica do posto de saúde do seu bairro, agendada pela plataforma de saúde da União.

A médica solicitou que Joana realizasse uma série de exames em uma clínica conveniada e que retornasse assim que os resultados fossem obtidos. Joana realizou os exames em uma clínica que possui serviço de envio de resultados para os médicos solicitantes do exame, mas a paciente não autorizou o compartilhamento direto e preferiu buscar os resultados. Na consulta de retorno, Joana apresentou os resultados para a médica, que constatou a intoxicação alimentar.

A paciente, mantendo comportamento cuidadoso com o compartilhamento dos seus dados, pediu os exames para a médica, após o diagnóstico. Apesar do pedido, os resultados do exame foram enviados para o órgão responsável pela vigilância sanitária para que fosse possível fiscalizar o restaurante que deu causa ao diagnóstico de Joana e para que a disseminação da doença fosse contida. Assim, tendo em vista que o tratamento foi adequado e que não haveria necessidade de coletar o consentimento da titular, o contexto do tratamento permitiu o fluxo de dados de Joana entre a médica e o órgão sanitário para atender uma finalidade para além dos interesses da titular, mas que era próxima à sua expectativa na relação paciente e médica.

A partir de uma leitura de integridade contextual da privacidade, é possível que o direito à proteção de dados seja instrumento para que as pessoas desenvolvam sua personalidade livremente. A disponibilidade de dados não indica nem para um fluxo irrestrito de dados que ignora as circunstâncias do tratamento, mas também não impede qualquer trânsito de dados em nome de uma lógica de que o titular deve controlar qualquer troca de dados a seu respeito.

O fluxo informacional possui um valor fundamental para que os entes que o com-

põem desempenhem seus papéis sociais já esperados[50]. É diante dessas perspectivas, seja com o mapeamento dos cinco elementos, seja com a observância dos interesses e valores éticos e contextuais do caso, que o **fluxo informacional** deve ser entendido como **íntegro**. O direcionamento desses parâmetros éticos e contextuais dão a flexibilidade necessária a um cenário de mudança constante e digitalização da vida, em que vários elementos dela passam a estar no mundo digital.

Ainda de acordo com a teoria da privacidade como integridade contextual, a definição dessas expectativas contextuais dos titulares está relacionada também com elementos de **transparência, prestação de contas** e ônus da prova[51]. Isso porque o titular não é surpreendido quando ele conhece o fluxo em que está inserido e tem alinhados os seus valores contextuais. Com essas informações, o titular, bem como toda sociedade, passam a ter as ferramentas necessárias para questionar e responsabilizar os agentes de tratamento que realizam determinadas etapas do fluxo de forma inadequada.

O fluxo de dados pessoais em uma IPD deve ser analisado a partir de uma perspectiva de privacidade contextual, a fim de se garantir que a troca de informações está de acordo com os valores de privacidade e, mais especificamente, com o direito fundamental à proteção de dados pessoais. Por essa abordagem, o direito não visa colocar barreiras ou travar o fluxo de dados pessoais, esse trânsito de informações passa a ser guiado por considerações regulamentares específicas de acordo com a **relação contextual** estabelecida entre os agentes afetados pelo fluxo.

A partir dessa teoria, a integridade do trânsito de dados passa a ser percebida de acordo com o contexto em que o próprio fluxo está inserido[52]. Se existem dúvidas sobre **quem são os agentes e quais as informações que compõem o fluxo e sobre os valores éticos e contextuais que são promovidos ou obscurecidos pelo tratamento[53]**, o fluxo passa a não ser percebido como íntegro e deve ser

---

50 BIONI, Bruno Ricardo. Proteção de dados pessoais: a função e os limites do consentimento. Rio de Janeiro: Forense, 2019. p. 216

51 NISSENBAUM, Helen. Contextual Integrity Up and Down the Data Food Chain, 20 Theoretical Inquiries L. 221 (2019). p. 256.

52 BIONI, Bruno Ricardo. Proteção de dados pessoais: a função e os limites do consentimento.Rio de Janeiro: Forense, 2019. p. 212.

53 RODRIGUES, Amaury de Matos. A controvérsia sobre a divulgação de remuneração dos servidores públicos: uma análise à luz da privacidade como integridade contextual. Dissertação (mestrado) – Instituto Brasiliense de Direito Público – IDP, Brasília, 2014. p. 60.

reavaliado. Por isso, o compartilhamento de dados, inclusive de dados de identidade em uma infraestrutura, podem ocorrer desde que observem o contexto em que estão inseridos.

3.4. Separação informacional

A digitalização da vida também afeta a forma com que as informações são estruturadas, organizadas e disponibilizadas para os agentes que compõem esse espaço digital. Por isso, para além do contexto em que esses dados foram coletados, o conceito de separação informacional se mostra como mais uma outra chave para a leitura do direito constitucional de proteção de dados.

A separação informacional guarda origem no conceito de separação informacional de poderes e, por consequência, na teoria da separação dos poderes. O objetivo dessa teoria é **repartir o poder político** em pessoas distintas para impedir a concentração desse poder[54]. Essa divisão de poderes está relacionada ao princípio da divisão de tarefas no Estado, em que os órgãos estatais, que compõem o Estado, possuem funções, **competências** próprias e podem exercê-las com relativa autonomia, sem a interferência e dependência dos outros[55]. Ao mesmo tempo em que há divisão de poderes em esferas de competência limitadas, os poderes atuam conjuntamente para a consecução de objetivos constitucionais comuns[56].

A luz do constitucionalismo digital, esses princípios clássicos foram ressignificados a um contexto de digitalização, inclusive do Estado, em que se deve garantir uma separação informacional de poderes. Ou seja, o Estado não deve ser entendido como uma unidade informacional em que todos os seus órgãos têm às suas disposições os mesmos dados, como o Estado é organizado em poderes, em competências, essas devem limitar inclusive as informações que seus órgãos podem acessar.

---

54 MENDES, Gilmar Ferreira; BRANCO, Paulo Gustavo Gonet. Curso de Direito Constitucional, 7ª Ed. São Paulo, Saraiva, 2012.

55 SILVA, Virgílio Afonso da. Direito Constitucional Brasileiro. São Paulo: Editora da Universidade de São Paulo, 2021. p. 33

56 SARLET, Ingo Wolfgang; SALES SARLET, Gabriele. Separação informacional de poderes no direito constitucional brasileiro. São Paulo: Associação Data Privacy Brasil de Pesquisa, 2022. p. 28

Como consequência, o fluxo e o compartilhamento de dados pessoais entre órgãos do Estado devem observar as competências, funções e poderes dos agentes envolvidos nesse ecossistema. Ainda, o tratamento de dados realizado por um ente deve estar em acordo com suas competências, sob risco de possibilitar uma concentração de poder.

Esse conceito foi debatido pelo STF em diversas decisões exaradas pelo tribunal, três desses casos merecem destaque.

ADI nº 6529/DF - Caso Abin

Em outubro de 2021, o plenário do STF proferiu acórdão na **ADI nº 6529/DF** e decidiu pela constitucionalidade, com interpretação conforme, do parágrafo único, do art. 4º, da Lei n. 9.883/1999[57]. Este dispositivo permite que o Sistema Brasileiro de Inteligência (SISBIN) compartilhe dados relacionados à defesa das instituições e dos interesses nacionais com a Agência Brasileira de Inteligência (Abin).

Para os requerentes da ADI, essa permissão legal não estava em acordo com a manutenção dos direitos e garantias fundamentais, com acordos internacionais, até mesmo com as normas brasileiras. A lei objeto da ação estaria em oposição às normas que previam dever de motivação, razoabilidade e proporcionalidade no compartilhamento de informações, além de deveres de sigilo gravados por reserva de jurisdição. Isso porque, segundo os requerentes, "houve, recentemente, um paulatino aumento do poder requisitório de informações pela Abin" e "não é de se desprezar a possibilidade de desvirtuamento da finalidade da Abin".

Toda a lide se baseou na possibilidade do SISBIN fornecer ou não dados para a Abin sem as devidas balizas constitucionais. Nesse sentido, o STF afirmou que, apesar do caráter sigiloso das atividades de inteligência exercidas pela Abin, elas não podem se afastar do controle externo do poder Legislativo (inc. X, do art. 49, da Constituição) e do Poder Judiciário (inc. XXXV, do art. 5º, da Constituição) para se verificar as estritas finalidades públicas a que o tratamento de dados se dirige.

Assim, o tribunal fixou entendimento de que "o fornecimento de informação entre órgãos que não cumpra os rigores formais do direito nem atenda estritamente ao

57 https://portal.stf.jus.br/processos/downloadPeca.asp?id=15348384228&ext=.pdf

interesse público, rotulado legalmente como defesa das instituições e do interesse nacional, configura abuso do direito, contrariando a finalidade legítima posta na norma legal".

Como pano de fundo, o STF argumenta que o compartilhamento de dados, pessoais ou não, deve atender uma finalidade específica e pública, ou seja, se o órgão que recebe os dados não tem uma motivação para tanto, o tratamento não deve ser feito. Há uma separação de competências entre os órgãos públicos, que deve ser respeitada também a nível informacional, de forma que apenas as autoridades pertinentes devem tratar determinados dados.

A partir da decisão do STF, o seguinte infográfico pode ser feito:

Esse julgado não torna rígido qualquer compartilhamento de dados entre os órgãos do Poder Público. Ele pode ocorrer desde que haja:

- observância do interesse público;
- motivação dos atos administrativos;
- análise da necessidade de sigilo e reserva de jurisdição.

Nesse sentido, a ministra relatora, Cármen Lúcia, afirma que a "possibilidade de fornecimento de informações harmoniza-se com o federalismo cooperativo e não consubstancia invasão à autonomia política". Dessa forma, quando esses requisitos forem preenchidos, os dados podem e devem fluir entre agentes públicos.

ADI nº 6649/DF e ADPF nº 695/DF - Caso Cadastro Base do Cidadão

Em setembro de 2022, o STF teve oportunidade de julgar caso similar na **ADI nº 6649/DF e na Arguição de Descumprimento de Preceito Fundamental (ADPF) nº 695/DF**, em que a constitucionalidade do Decreto nº 10.046/2022 foi questionada[58].

O Decreto nº 10.046/2019 dispõe sobre a governança no compartilhamento de dados no âmbito da administração pública federal, e institui o Cadastro Base do Cidadão (CBC) e o Comitê Central de Governança de Dados[59]. O objetivo do Decreto era facilitar o processo de compartilhamento de dados, inclusive pessoais, realizado entre entidades da administração pública federal direta, autárquica e fundacional e dos demais Poderes da União. Segundo o art. 1º do Decreto, sua finalidade era simplificar a oferta de serviços públicos, otimizar a formulação e o monitoramento de políticas públicas, além de promover a qualidade dos dados custodiados pelos órgãos federais.

Para tanto, o art. 5º, do Decreto, determinou que seria dispensada a celebração de convênio, acordo de cooperação técnica ou instrumentos congêneres para a

58 SUPREMO TRIBUNAL FEDERAL. Ação Direta de Inconstitucionalidade 6.649 Distrito Federal. Disponível em: https://portal.stf.jus.br/processos/downloadPeca.asp?id=15358978491&ext=.pdf. Acesso em: 2 dez. 2024.

59 PRESIDÊNCIA DA REPÚBLICA. Decreto n 10.046, de 9 de outubro de 2019. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/decreto/d10046.htm. Acesso em: 2 dez. 2024.

efetivação do compartilhamento de dados entre os órgãos regidos pelo decreto.

Assim que publicado, o Decreto foi utilizado para justificar o compartilhamento de dados pessoais da Carteira Nacional de Habilitação, gerida pela Secretaria Nacional de Trânsito (Senatran), antigo Denatran, entre o Serviço Federal de Processamento de Dados (Serpro) e a Abin. Esse foi um dos fatos que motivou a propositura da ADPF em questão. Com a judicialização do caso, o Denatran revogou o Termo de Autorização que permitia o compartilhamento de dados com a Abin. Mesmo com a possível perda de objeto da ADPF, o ministro Gilmar Mendes, relator, manteve o julgamento, tendo em vista que o "ato do Poder Público impugnado nesta ADPF abrangia todo um quadro de insegurança jurídica gerado por interpretações distorcidas do Decreto 10.046/2019"[60].

O voto do relator, que foi o voto condutor do julgamento, conferiu uma interpretação conforme ao Decreto para apresentar parâmetros orientativos para o compartilhamento de dados.

Para o STF, se, por um lado, a celebração de convênios e acordos de cooperação técnica poderia ser uma barreira para o compartilhamento, uma de suas finalidades era justamente garantir a publicidade do compartilhamento. O tribunal reforça o compromisso do Poder Público em dar transparência sobre os compartilhamentos que realiza, sendo dever do órgão dar "a devida publicidade às hipóteses em que cada entidade governamental compartilha ou tem acesso a banco de dados pessoais"[61].

O STF determinou que o compartilhamento de dados entre órgãos e entidades da Administração Pública só pode acontecer quando publicizado e diante:

- da eleição de propósitos legítimos, específicos e explícitos para o tratamento de dados (art. 6º, inciso I, da Lei 13.709/2018);

60 SUPREMO TRIBUNAL FEDERAL. Arguição de Descumprimento de Preceito Fundamental 695 Distrito Federal. p. 5. Disponível em: https://portal.stf.jus.br/processos/downloadPeca.asp?id=15358978671&ext=.pdf. Acesso em: 29 jul. 2024.

61 SUPREMO TRIBUNAL FEDERAL. Arguição de Descumprimento de Preceito Fundamental 695 Distrito Federal. p. 3. Disponível em: https://portal.stf.jus.br/processos/downloadPeca.asp?id=15358978671&ext=.pdf. Acesso em: 29 jul. 2024.

- da compatibilidade do tratamento com as finalidades informadas (art. 6º, inciso II);

- da limitação do compartilhamento ao mínimo necessário para o atendimento da finalidade informada (art. 6º, inciso III);

- do cumprimento integral dos requisitos, garantias e procedimentos estabelecidos na Lei Geral de Proteção de Dados, no que for compatível com o setor público.

Esses requisitos são bastante similares aos da decisão do tribunal no julgamento da ADI 6529/DF. Por um lado, nesta ADI, os requisitos do compartilhamento de dados são fundamentados nos conceitos de interesse público e desvio de finalidade delimitados na própria constituição. Por outro lado, na ADI 6649/DF, o diálogo com os dispositivos da LGPD são expressos, de forma a complementar os elementos trazidos pela constituição. De acordo com os dois julgados, o compartilhamento de dados deve observar requisitos comuns à proteção de dados para a análise de constitucionalidade do compartilhamento de informações pessoais, explicitando o diálogo entre as matérias.

Na ADI em questão, o STF reforça, de forma explícita, o entendimento da ADI 6529, e retoma argumentos em linha com o princípio da separação informacional de poderes. Como resumo dos dois julgados, para o tribunal, esse tipo de compartilhamento deve observar:

- a adoção de medidas proporcionais e estritamente necessárias ao atendimento do interesse público;

- a instauração de procedimento administrativo formal, acompanhado de prévia e exaustiva motivação, para permitir o controle de legalidade pelo Poder Judiciário;

- a utilização de sistemas eletrônicos de segurança e de registro de acesso, inclusive para efeito de responsabilização em caso de abuso; e

- a observância dos princípios gerais de proteção e dos direitos do titular previstos na LGPD, no que for compatível com o exercício dessa função estatal.

Vale notar que o interesse público não deve ser analisado como um bem jurídico superior e em confronto com outros valores constitucionais, como a proteção de dados e a privacidade. Isso porque, se a privacidade for analisada como um interesse individual, ela sucumbiria ao interesse coletivo, em que o Poder Público poderia tratar dados de forma irrestrita para finalidades públicas, consideradas superiores[62]. Assim, a proteção de dados deve ser entendida como uma ferramenta para atingimento de objetivos coletivos de estruturação dos regimes democráticos, ao mesmo tempo que garantidora da autonomia das pessoas[63].

Outro elemento fundamental considerado pela decisão final do STF foi a composição do Comitê Central de Governança de Dados previsto no Decreto. Essa composição foi considerada inconstitucional pelo tribunal porque ele era composto apenas de representantes da administração pública federal, mas deveria ter uma "composição independente, plural e aberta à participação efetiva de representantes de outras instituições democráticas".

O Comitê seria responsável por estabelecer limites ao compartilhamento de dados entre órgãos da administração pública federal, fato que produz efeitos transversais nas atividades do setor público. Por isso, o STF reconhece a necessidade do mesmo ser representativo e demonstrar uma abertura para a pluralização do debate para além de representantes do Poder Público para a garantia da eficácia do direito fundamental. A **participação cívica**, como reconhecida pelo STF, é uma **ferramenta central para legitimação das atividades feitas pelo Estado**, por isso ela será objeto de análise mais específica no capítulo seguinte.

MS nº 36.150/DF - Caso Inep x TCU

Por fim, o STF, em dezembro de 2021, julgou o **Mandado de Segurança (MS) nº 36.150/DF**, sobre a possibilidade de compartilhamento de dados pessoais entre órgãos do Poder Público.[64] O MS foi impetrado pelo Instituto Nacional de Estudos e Pesquisas Educacionais Anísio Teixeira (INEP) contra acórdão do Tribunal

62 BLACK, Gillian e STEVENS, Leslie. "Enhancing Data Protection and Data Processing in the Public Sector: The Critical Role of Proportionality and the Public Interest" . In: Scripted. Vol. 10, n. 1, 2013, p. 95.

63 SUPREMO TRIBUNAL FEDERAL. Ação Direta de Inconstitucionalidade 6.649 Distrito Federal. p. 33. Disponível em: https://portal.stf.jus.br/processos/downloadPeca.asp?id=15358978491&ext=.pdf. Acesso em: 2 dez. 2024

64 SUPREMO TRIBUNAL FEDERAL. Mandado de Segurança 36.150 Distrito Federal. Disponível em: https://portal.stf.jus.br/processos/downloadPeca.asp?id=15349322719&ext=.pdf. Acesso em: 2 dez. 2024.

de Contas da União (TCU) que determinou a entrega de dados individualizados do Censo Escolar e do ENEM para auditoria do Programa Bolsa Família.

Por parte do INEP, o compartilhamento de informações com o TCU para controle externo seria contrária às expectativas dos estudantes que fornecem seus dados, colocando em risco a capacidade do INEP em fazer pesquisa e monitorar as políticas públicas de educação, e afrontaria direitos de terceiros que têm a garantia de sigilo sobre os seus dados pessoais. Já o TCU afirma que o item 16.3 do Edital ENEM 2017 permite o uso da informação pessoal no âmbito de programas governamentais e que os seus auditores possuem competência prevista em lei para acessar informações pessoais, mesmo que sigilosas.

Por um lado, o STF reconhece o caráter sigiloso dos dados tratados pelo INEP, por outro o TCU tem competência de realizar auditorias e a atribuição dessa competência supõe o reconhecimento dos meios necessários ao cumprimento desse encargo. Por isso, a "questão controvertida está em saber se o dever de sigilo imposto ao INEP seria quebrado com a transmissão ao TCU dessas bases de dados individualizados do Censo Educacional e do ENEM". Essa análise de competência dos órgãos públicos está diretamente vinculada ao debate de separação informacional dos poderes, de forma que o órgão poderia e deveria acessar todos aqueles dados necessários para realizar suas atribuições.

Em seu voto, ainda na medida cautelar do MS, o ministro relator Barroso entende que o compartilhamento de dados pessoais a outro órgão público "para uma finalidade diversa daquela inicialmente declarada subverte a autorização daqueles que forneceram seus dados pessoais, em aparente violação do dever de sigilo e da garantia de inviolabilidade da intimidade".[65] Assim, o compartilhamento de dados minaria a confiança dos estudantes no INEP, o que poderia violar o sigilo estatístico entre o INEP e os estudantes e poderia colocar em risco a continuidade das atividades desempenhadas pelo próprio INEP.

Neste julgado, o ministro Barroso retoma expressamente a decisão do tribunal na ADI 6649 e ADPF 695 diante do "impacto do regime de compartilhamento de dados entre órgãos públicos para a proteção de direitos fundamentais".

---

65 SUPREMO TRIBUNAL FEDERAL. Medida Cautelar em Mandado de Segurança 36.150 Distrito Federal. Disponível em: https://portal.stf.jus.br/processos/downloadPeca.asp?id=15339236967&ext=.pdf. Acesso em: 2 dez. 2024.

A partir de uma análise dos três casos em questão, é evidente a posição do STF pela necessidade de temperar o compartilhamento de dados entre órgãos do Poder Público, justificado pela **eficiência e digitalização** da administração, com **valores constitucionais** que indicam para delimitação de uma **finalidade específica e compatível** para o tratamento, além do **interesse público** e **publicidade** imbricada. Esse cuidado com a finalidade do compartilhamento de dados está em consonância direta com o princípio da separação informacional dos poderes.

Essa separação de informações pessoais que podem ser tratadas é justificada pela ideia de uma divisão funcional de competência e atribuições para que sejam estabelecidos **limites para o exercício do poder** político. No contexto digital, isso significa que o Estado "deve estabelecer, mediante a utilização de parâmetros de atuação forjados com base no princípio da separação de poderes, um regime organizacional pautado na divisão por competências, envidando todos os esforços para evitar o compartilhamento abusivo, desproporcional, irrestrito e, portanto, inconstitucional de dados pessoais". [66]

Assim, os julgados do STF indicam para a interpretação já consolidada de que o Estado não é uno, inclusive diante das informações pessoais que ele estabelece e conhece. Seguindo a lógica da separação de poderes, a divisão de competências definidas na constituição deve guiar inclusive a forma e os parâmetros do compartilhamento de dados pessoais. No limite, esses dados não podem ser compartilhados irrestritamente pelos entes que formam o Poder Público, especialmente quando não houver finalidade para tanto ou essa for diversa, sob pena de desvio de finalidade.[67]

Uma forma de evitar possíveis abusos no compartilhamento de dados é pautar o fluxo de dados pela **divisão de competências** dos agentes que enviam e recebem dados pessoais. Essa separação de competências, de poderes, dos órgãos públicos está diretamente relacionada com a identificação de finalidades específicas do tratamento que determinados agentes realizam com base em sua

66 SARLET, Ingo Wolfgang; SALES SARLET, Gabriele. Separação informacional de poderes no direito constitucional brasileiro. São Paulo: Associação Data Privacy Brasil de Pesquisa, 2022.

67 SARLET, Ingo Wolfgang; SALES SARLET, Gabriele. Separação informacional de poderes no direito constitucional brasileiro. São Paulo: Associação Data Privacy Brasil de Pesquisa, 2022.

competência.[68] Essa avaliação dos parâmetros para compartilhamento de dados indicadas pelo STF é complementar ao já apresentado pela ANPD no Guia Orientativo de Tratamento de dados pessoais pelo Poder Público.[69] Os parâmetros das duas fontes podem ser comparados da seguinte forma:

STF	ANPD[70]
Cumprimento integral dos requisitos, garantias e procedimentos estabelecidos na LGPD, no que for compatível com o setor público.	Documentação da operação de tratamento por meio de uma análise técnica e jurídica que discipline o compartilhamento.
Instauração de procedimento administrativo formal, acompanhado de prévia e exaustiva motivação, para permitir o controle de legalidade pelo Poder Judiciário.	Formalização da operação de tratamento por meio da celebração de contrato, convênio ou instrumento congênere.
Avaliação da compatibilidade do compartilhamento de dados, verificando se o compartilhamento de dados pessoais a outro órgão público para uma finalidade diversa daquela inicialmente declarada subverte a autorização dos titulares.	Identificação dos dados pessoais objeto do compartilhamento e a finalidade específica dos dados tratados, verificando a compatibilidade entre a finalidade original e a finalidade do compartilhamento.
Cumprimento integral dos requisitos, garantias e procedimentos estabelecidos na LGPD, no que for compatível com o setor público.	Atribuição de uma base legal adequada para a atividade de compartilhamento, bem como o termo inicial e final do tratamento.
Obrigação do órgão público dar a devida publicidade às hipóteses em que cada entidade governamental compartilha ou tem acesso a banco de dados pessoais.	Informação, de forma clara e acessível, ao titular de dados sobre o compartilhamento e os meios para o exercício de seus direitos.
Utilização de sistemas eletrônicos de segurança e de registro de acesso, inclusive para efeito de responsabilização em caso de abuso.	Adoção de medidas de prevenção e segurança da informação, inclusive as medidas técnicas e administrativas para proteger os dados pessoais de incidentes de segurança.

68 SARLET, Ingo Wolfgang; SALES SARLET, Gabriele. Separação informacional de poderes no direito constitucional brasileiro. São Paulo: Associação Data Privacy Brasil de Pesquisa, 2022. p. 34.

69 ANPD. Guia Orientativo de Tratamento de dados pessoais pelo Poder Público. 2023. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/documentos-de-publicacoes/guia-poder-publico-anpd-versao-final.pdf. Acesso em: 20 dez. 2024.

70 MARTINS, Pedro Bastos Lobo; SANTOS, Pedro Henrique; CRUZ, Sinhue Nascimento. Guia ANPD: Tratamento de Dados pelo Poder Público. 2022. Data Privacy Brasil.

Cumprimento integral dos requisitos, garantias e procedimentos estabelecidos na LGPD, no que for compatível com o setor público.	Caso necessário, adoção de medidas adicionais, como a elaboração de um relatório de impacto à proteção de dados, definição do ônus financeiro do compartilhamento de dados e a possibilidade de novo compartilhamento ou transferência posterior.
Adoção de medidas proporcionais e estritamente necessárias ao atendimento do interesse público.	Avaliação da compatibilidade entre a finalidade original e a do uso secundário que considere o interesse público e a finalidade pública específica do tratamento posterior, bem como o seu vínculo com as competências legais dos órgãos ou entidades envolvidos.

Para além do primeiro momento em que o controlador coleta do próprio titular seus dados pessoais, a LGPD apresenta algumas ferramentas a serem utilizadas pelos agentes de tratamento quando ele não tiver contato direto com o titular, ou em cenários de reuso dos dados. Qualquer tratamento de dados deve ocorrer para atingir-se "propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades".[71]

É bastante comum que em casos de compartilhamento e fluxo intenso de dados, comuns a cenários de IPD, a arquitetura do tratamento de informações seja complexo e, para além do titular, as informações sejam **validadas** com base em outros agentes. Isso é bastante evidente em aplicações de identidade, especialmente nas funções de autenticação e autorização, em que validade da informação apresentada pelo titular é confirmada com outros agentes, inclusive com o emissor da credencial. Nesse processo de verificação, podem ser consultados dados tratados por entidades privadas ou públicas, em diferentes contextos.

No contexto de separação informacional dos poderes, "a intervenção do Estado não pode comprometer o objetivo e tampouco a finalidade pública que deu ensejo ao processamento, justificando a coleta dos dados pessoais sob pena de desvio de finalidade". [72]O compartilhamento de dados garante importância ao dever de transparência, desde a coleta, do agente de tratamento perante o titular, já que é "condição objetiva para o exercício de direitos como o de oposição ao novo

71 PRESIDÊNCIA DA REPÚBLICA. Lei n 13.709, de 14 de agosto de 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 2 dez. 2024.

72 SARLET, Ingo Wolfgang; SALES SARLET, Gabriele. Separação informacional de poderes no direito constitucional brasileiro. São Paulo: Associação Data Privacy Brasil de Pesquisa, 2022. p. 34.

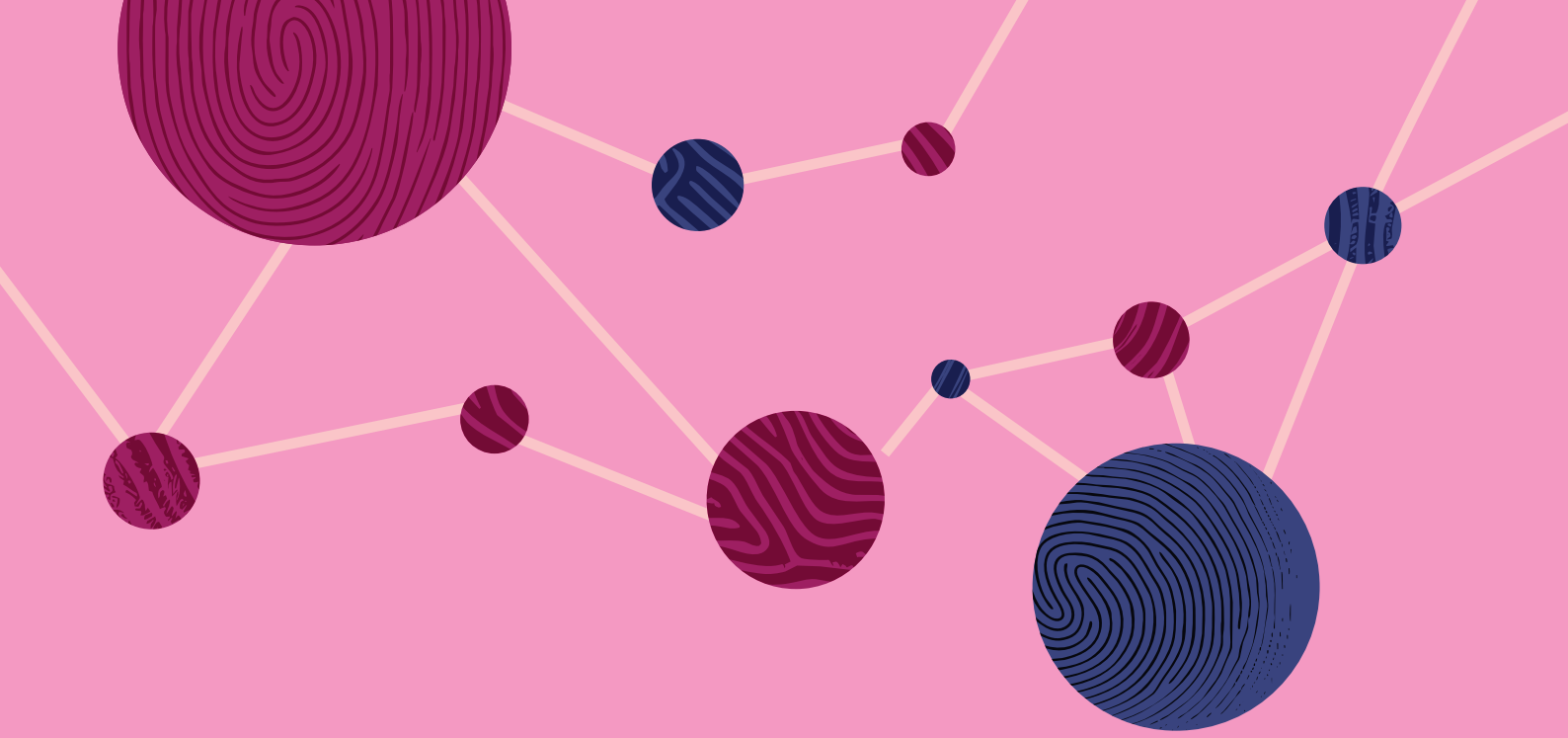
tratamento"[73]. Assim, o uso de dados para **finalidades secundárias** depende de:

- indicação de base jurídica apropriada para sustentar o novo tratamento;
- compatibilidade da finalidade secundária com a finalidade do tratamento de dados no momento da coleta dos dados, a finalidade primária;
- previsão de finalidade suficientemente especificada, que permita a avaliação do interesse público a ser atingido;
- observância dos princípios de proteção de dados e direitos dos titulares, em especial o princípio da transparência, necessidade, adequação e prestação de contas e o direito de informação e acesso.

Portanto, o direito fundamental à proteção de dados, diferente do sentido tradicional de privacidade, não está relacionado com um dever do Estado ou outros agentes se abster de conhecer o sujeito. Ao contrário, os dados pessoais podem fluir e, quando isso ocorre, o fluxo de informações deve observar **parâmetros contextuais e de separação informacional** dos poderes de acordo com a finalidade do tratamento.

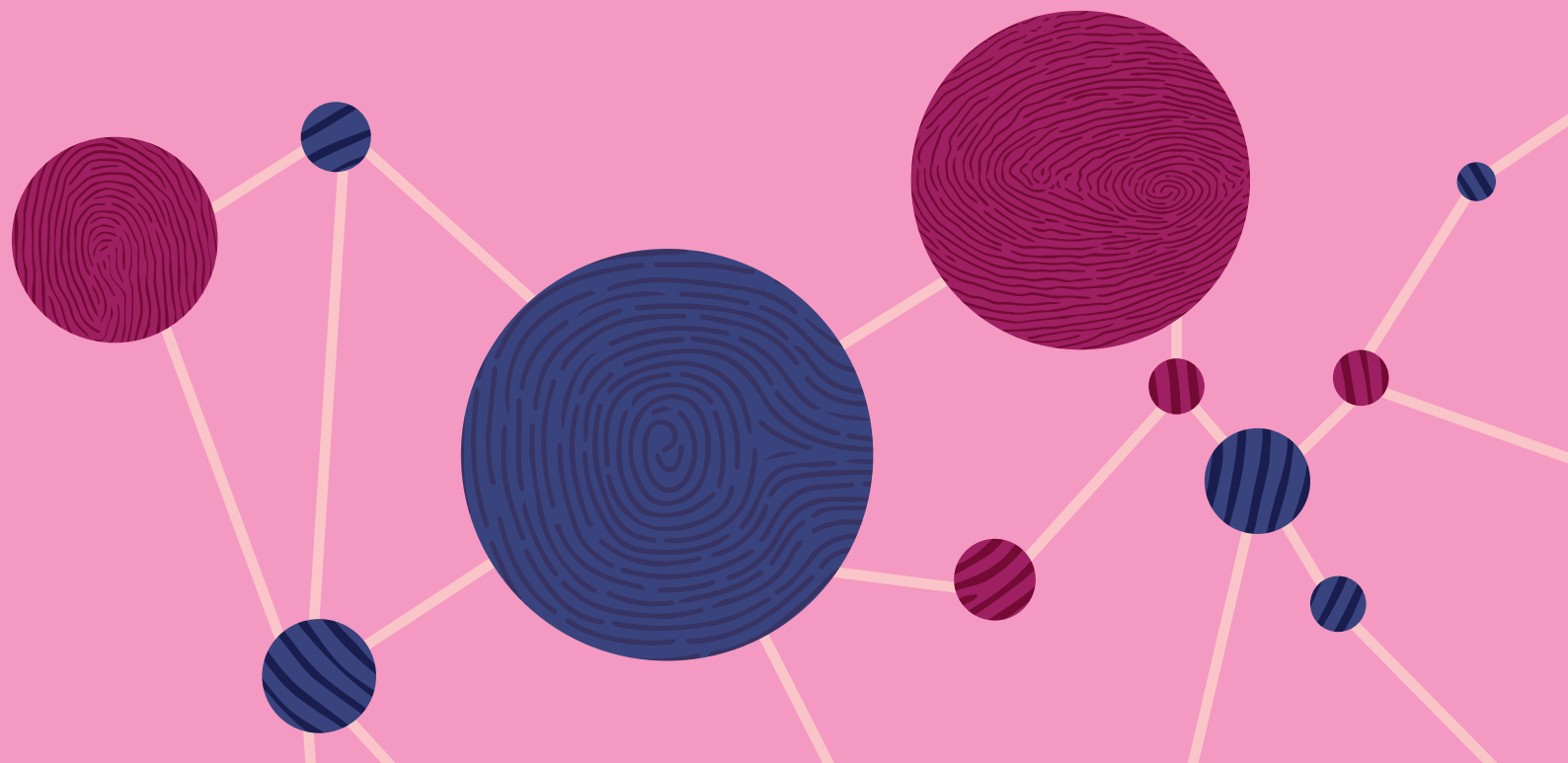
Isso porque desenvolver uma IPD e soluções de identidade cria risco de violação de direitos, especialmente o de proteção de dados pessoais, tratado neste documento. Ainda, em um contexto de infraestrutura, é possível que os riscos gerados em uma IPD passem a se manifestar em **outras aplicações**, diante do intenso fluxo de dados. Assim, a introdução de **arranjos robustos** é fundamental para garantir que esse compartilhamento de informações ocorra de maneira segura, informada e rastreável.

73 WIMMER, Miriam. Limites e possibilidades para o uso secundário de dados pessoais no poder público: lições da pandemia. Revista Brasileira de Políticas Públicas, Brasília, v. 11, n. 1. p.122-142, 2021. p. 137.



04.

PROCEDIMENTALIZANDO UMA IPD PARA O BEM COMUM: PROTEÇÃO DE DADOS E PRESTAÇÃO DE CONTAS



4 Procedimentalizando uma IPD para o bem comum: proteção de dados e prestação de contas

Os processos de digitalização ressignificam diversas relações, inclusive entre o cidadão e o Estado, entre o consumidor e as empresas e as pessoas entre si. A tecnologia, incorporada nos processos cotidianos, inclusive de governança pública, traz novos desafios para a sociedade em vista da assimetria de forças entre esses grupos[74]. A tecnologia, especialmente quando relacionada a mudanças de infraestrutura, como na IPD, está associada a um interesse que não é apenas das partes que a integram, mas envolve também um bem comum.

Nesse cenário digital, como evidenciado no capítulo anterior, novos desafios surgem para a sociedade da informação, já que, de um lado os dados são "insumo essencial ao desenvolvimento das mais variadas atividades econômicas e governamentais"[75], e de outro o seu tratamento indevido pode colocar em risco a proteção de direitos fundamentais. Este relatório visa justamente olhar esses desafios por uma lente de proteção de dados pessoais enquanto um direito fundamental.

A partir dos conceitos chave relacionados a IPD e a identidade digital, nota-se que um dos pilares da IPD é o que significa essa infraestrutura ser pública para o próprio sistema e para suas aplicações. O sentido de "pública" da IPD pode variar a depender de vários elementos responsáveis por dar sentido a esse termo em acordo com o praticado pelos agentes envolvidos na construção e manutenção de uma infraestrutura digital. Por isso, não se pode perder de vista o objeto de análise (identidade como aplicação na IPD) a fim de que as práticas indicadas neste relatório sejam aderentes e implementáveis ao caso concreto.

No que tange a identidade, a sua principal funcionalidade é permitir que uma pes-

74 COMITÊ GESTOR DA INTERNET NO BRASIL. TIC Governo Eletrônico 2019 Pesquisa Sobre o Uso das Tecnologias de Informação e Comunicação no Setor Público Brasileiro. São Paulo: Núcleo de Informação e Coordenação do Ponto BR, 2020. p. 28. Disponível em: https://cetic.br/media/docs/publicacoes/2/20200707094309/tic_governo_eletronico_2019_livro_eletronico.pdf. Acesso em: 2 dez. 2024.

75 COMITÊ GESTOR DA INTERNET NO BRASIL. TIC Governo Eletrônico 2019 Pesquisa Sobre o Uso das Tecnologias de Informação e Comunicação no Setor Público Brasileiro. São Paulo: Núcleo de Informação e Coordenação do Ponto BR, 2020. p. 30. Disponível em: https://cetic.br/media/docs/publicacoes/2/20200707094309/tic_governo_eletronico_2019_livro_eletronico.pdf. Acesso em: 2 dez. 2024.

soa seja reconhecida, compartilhe suas credenciais ou prove quem ela é, quando necessário às interações e transações no mundo digital ou offline. A identidade é uma das principais aplicações na IPD, porque, em muitos contextos, é necessário identificar quem está utilizando aplicações na infraestrutura para depois oferecer os serviços devidos a ela. Como parte das relações passa a ser digital, o desafio de se saber com quem essas relações e obrigações estão sendo firmadas é posto novamente. Esse tipo de demanda é bastante evidente nas atividades de identificação e autenticação de uma pessoa feitas pelo setor bancário para garantir que a pessoa que realiza transação bancária é o titular da conta, ou mesmo quando a pessoa utiliza espaços online para solicitar acesso a benefício previdenciário.

Informações complementares

Framework de confiança de atributos e identidade digital do Reino Unido alpha v1[76]

No contexto de identidade digital, o governo do Reino Unido publicou seu framework com uma série de parâmetros para o estabelecimento de uma identidade digital segura e confiável na região. No cenário do Reino Unido, esse framework de confiança seria administrado por um órgão governamental estabelecido pelo governo. Porém, a estrutura foi criada para agentes além do Poder Público, ou seja, para organizações que desejam fornecer ou consumir produtos e serviços de identidade e atributos digitais.

Para tanto, o governo publicou um documento que define os procedimentos gerais para aderir ao framework. O órgão regulador é responsável por garantir que as organizações terceiras sigam as regras e decidirá o que fazer se não o fizerem, fornecendo certificados às organizações que seguirem o framework. Sendo certificada, isso significa que uma organização pode confiar que as informações que ela fornece são precisas e confiáveis.

Cada vez mais essa identificação é conduzida em sistemas na IPD enquanto soluções estruturantes para uma sociedade digital. Como indicado no primeiro capítulo deste relatório, diversas entidades estão apresentando descrições e en-

76 GOV.UK. UK Digital Identity and Attributes Trust Framework Alpha v1 (0.1). GOV.UK. Disponível em: https://www.gov.uk/government/publications/the-uk-digital-identity-and-attributes-trust-framework/the-uk-digital-identity-and-attributes-trust-framework#introduction. Acesso em: 2 dez. 2024.

foques diversos e específicos para delimitar o conceito de uma IPD. Apesar da difusão de sentidos, a definição na IPD permite traçar diretrizes para o desenvolvimento dessa infraestrutura.

Por isso, as definições do G20 e da Estratégia Nacional de Governo Digital, publicada no Decreto nº 12.069, de 21 de junho de 2024, são relevantes para perceber os movimentos locais e globais sobre o tema de IPD.

DEFINIÇÃO G20

Um conjunto de sistemas digitais compartilhados, seguros, interoperáveis. Esses sistemas devem poder ser construídos com base em normas e padrões abertos para entregar e fornecer acesso equitativo a serviços públicos e/ou privados em escala. Esses sistemas devem ser regidos por quadros jurídicos aplicáveis e regras que permitam conduzir desenvolvimento, inclusão, inovação, confiança e concorrência e respeito aos direitos humanos e as liberdades fundamentais.

Conceito explícito apenas na definição do G20. É importante que se reconheça o caráter de interoperabilidade e segurança dos sistemas para que eles possam ser utilizados como base para outras aplicações a partir dessa base, infraestrutura.

Um dos pilares da IPD é seu elemento de tecnologia aberta, mas essa característica não é reforçada na definição do decreto.

"Acesso equitativo em escala" é similar a ideia de "escala universal" na definição do Decreto.

Parte final igual. IPD deve promover respeito aos direitos humanos e liberdades fundamentais, por isso deve haver esforço de se compreender de que forma as aplicações de IPD afetam os direitos das pessoas

DEFINIÇÃO DECRETO

Infraestruturas públicas digitais - IPD: soluções estruturantes, transversais a várias políticas públicas, que adotam padrões de tecnologia em rede construídos para o interesse público, que permitam escala universal, e viabilizam a orquestração de usos por diversos intervenientes, dos setores públicos e privados, de forma integrada em canais físicos e digitais, governados por arcabouços legais aplicáveis e regras habilitadoras para promover desenvolvimento, inclusão, inovação, confiança, competição, respeito aos direitos humanos e liberdades individuais.

Conceito explícito apenas na definição do Decreto, ele reforça o compromisso com o "público" de IPD, que esta cartilha associa como o termo "valor público", como será descrito neste tópico.

O conceito do Decreto garante abertura para outros agentes formadores da IPD, não apenas o setor público. Essa compreensão está alinhada com os conceitos apresentados por esta Cartilha.

As duas definições reconhecem o uso da IPD para serviços públicos e privados

Parte final igual ao G20.

As duas definições reconhecem o uso da IPD para serviços públicos e privados

Ao mesmo tempo que governos e organizações amadurecem os conceitos e aplicações na IPD, ainda há influxos e questionamentos sobre qual o benefício será criado por uma infraestrutura digital e como avaliá-la perante aos riscos que também podem surgir a partir de um cenário de digitalização e fluxo intensificado de dados entre atores públicos e privados. Dessa forma, o significado de "público" no conceito de IPD ainda é tema de discussão, tanto para a academia, quanto para os agentes que desenvolvem e implementam as aplicações na IPD. Em um primeiro momento, os especialistas em transformação digital do setor público se debruçaram sobre os temas relacionados à digitalização dos serviços públicos e aos ganhos de eficiência possibilitados pela tecnologia[77].

Porém, com o avanço tecnológico e o reconhecimento da importância de incorporar as noções de valor público nas soluções tecnológicas para o setor público, aumentou-se o interesse por definir e direcionar o sentido dos termos de uma IPD, especialmente o que faz dela "pública". Sobre isso, Mazzucato e outros afirmam que uma IPD pode ser pública por ter atributos técnicos (i) interoperáveis, (ii) com padrão aberto, (iii) licenças *open-source*, ou (iv) com uma abordagem "building-blocks", em que os blocos são utilizados para gerar soluções escaláveis e aprimoráveis de forma independente.

Por outro lado, uma infraestrutura digital também pode ser pública por conta de suas finalidades funcionais em (i) fomentar relações inter e intra comunitárias, (ii) melhorar a inclusão financeira e mobilizar as potencialidades dos agentes econômicos, (iii) criar as capacidades para que indivíduos, empresas e agentes da sociedade participem e prosperem em todas as dimensões da vida, ou (iv) garantir as necessidades essenciais para a vida humana, melhorando o bem-estar geral por meio de impactos na área de saúde, educação e enriquecimento cultural. No entanto, implementar os atributos técnicos e as funções do valor público não é suficiente para compreender o que faz uma infraestrutura digital ser pública[78].

Na tentativa de responder às lacunas percebidas, Mazzucato afirma que, para

77 Meijer, A. and Bekkers, V., 'A metatheory of e-government: Creating some order in a fragmented research field.' Government Information Quarterly, 32 (3), 237-245.

78 MAZZUCATO, Mariana; EAVES, David; VASCONCELLOS, Beatriz. Digital public infrastructure and public value: What is 'public' about DPI? UCL Institute for Innovation and Public Purpose, Working Paper Series (IIPP WP 2024- 05). Disponível em: https://www.ucl.ac.uk/bartlett/public-purpose/publications/2024/mar/digital-public-infrastructure-and-public-value-what-public-about-dpi. Acesso em: 25 abril 2024. p. 18

além do valor público, a IPD deve se ocupar em promover a noção de bem comum enquanto forma de maximizar esse valor público criado pelos atributos técnicos ou por suas funções. Isso quer dizer que, além de definir os valores públicos que visa atingir, sejam eles técnicos ou funcionais, uma IPD que busca efetivamente ser "pública" deve seguir parâmetros de governança alinhados com metas sociais claramente articuladas entre atores da sociedade[79]. O desenvolvimento de uma IPD está diretamente ligado à noção de uma estrutura que facilita a entrada novos players e a competição, mecanismos fomentados em parcerias público-privadas.

A partir da leitura proposta por Mazzucato, esses parâmetros de governança versam sobre (i) a capacidade de co-criação e participação no desenvolvimento da infraestrutura, (ii) o direcionamento de prioridades e a função exercida pelo Poder Público, (iii) a existência de mecanismos de transparência e prestação de contas, (iv) a disponibilidade de acesso e dos benefícios da IPD ao público geral, bem como (v) ferramentas de compartilhamento aprendizado[80].

A criação e a maximização do valor público é resultado de um processo coletivo e construído em colaboração entre os setores da sociedade, ou seja, não criado por apenas um setor e fixado pelo outro[81]. É a partir da definição do bem comum que o valor público ganha sentido e direcionamento. Assim, as tecnologias e aplicações de IPD passam a atender finalidades e objetivos específicos da comunidade em que estão inseridas.

Como consequência, é possível afirmar que o significado de "público" na IPD é preenchido também por outras condições, como a implementação de mecanismos de proteção de dados pessoais na própria infraestrutura e a definição dos procedimentos para garantir a promoção do valor público na IPD. Isso porque a preservação do bem comum é concretizada pela garantia do direito fundamental à proteção de dados, seja no conteúdo da aplicação na IPD, seja no procedimento

---

79 MAZZUCATO, Mariana; EAVES, David; VASCONCELLOS, Beatriz. Digital public infrastructure and public value: What is 'public' about DPI? UCL Institute for Innovation and Public Purpose, Working Paper Series (IIPP WP 2024- 05). Disponível em: https://www.ucl.ac.uk/bartlett/public-purpose/publications/2024/mar/digital-public-infrastructure-and-public-value-what-public-about-dpi. Acesso em: 25 abril 2024. p. 22

80 MAZZUCATO, Mariana; EAVES, David; VASCONCELLOS, Beatriz. Digital public infrastructure and public value: What is 'public' about DPI? UCL Institute for Innovation and Public Purpose, Working Paper Series (IIPP WP 2024- 05). Disponível em: https://www.ucl.ac.uk/bartlett/public-purpose/publications/2024/mar/digital-public-infrastructure-and-public-value-what-public-about-dpi. Acesso em: 25 abril 2024. p. 22

81 MAZZUCATO, Mariana; RYAN-COLLINS, Josh. Putting value creation back into "public value": from market-fixing to market-shaping. Journal of Economic Policy Reform, 25(4): 345-360, 2022. DOI: 10.1080/17487870.2022.2053537.

para definição dos seus elementos.

Vale notar que esse entendimento de valor público e de bem comum não se confunde com a identificação ou a mensuração de um valor econômico. De forma prática, a simples geração de valor econômico a partir dos dados em fluxo na IPD não garante o alcance do valor público, especialmente se os direitos dos indivíduos forem negligenciados. Como resultado do processamento de dados e a promoção do bem comum, é importante que os **benefícios** gerados pelo uso dos dados sejam distribuídos de forma justa e equitativa, e não concentrados nas mãos de empresas ou governos poderosos[82].

Nesse sentido e a partir dos aspectos constitucionais reconhecidos pela doutrina e jurisprudência brasileira no que tange o direito de proteção de dados pessoais, o desenvolvimento de uma aplicação na IPD, como os sistemas de identidade, e da própria infraestrutura passa a pressupor uma série de requisitos para a criação e promoção de um bem comum, de um valor público.

Se, por um lado, a complexificação de sistemas de identidade busca aumentar a confiança no resultado final, por outro, a falta de parâmetros pode fazer com que esse sistema coloque em risco a concretização de direitos fundamentais. Por isso, a implementação da infraestrutura requer abordagens cuidadosas para garantir que a IPD promova o bem comum. É nesse sentido que este capítulo visa apresentar **parâmetros de proteção de dados** que asseguram que as aplicações de IPD estejam alinhadas ao próprio conceito de IPD por meio da garantia do direito à proteção de dados e da participação e prestação de contas sobre a infraestrutura.

82 VEALE, Michael. Reasons for Concern around Mariana Mazzucato's Proposals for Data Governance. Michael Veale. Disponível em: https://michae.lv/mariana-mazzucatos-proposals-for-data-governance-are-concerning/#fn7. Acesso em: 2 dez. 2024.

4.1. Proteção de dados como garantia do bem comum

4.1.1. Introdução

Um dos principais efeitos do estabelecimento de uma IPD é o intenso fluxo de dados, sejam eles pessoais ou não, transitando pela infraestrutura digital. A IPD fornece justamente a base tecnológica necessária para permitir a troca eficiente e segura de informações entre diferentes sistemas, facilitando um fluxo contínuo e um processamento intensivo de dados. Esse trânsito de informações está no escopo das regulações de proteção de dados, especialmente enquanto um direito fundamental que orienta a construção de uma arquitetura informacional adequada.

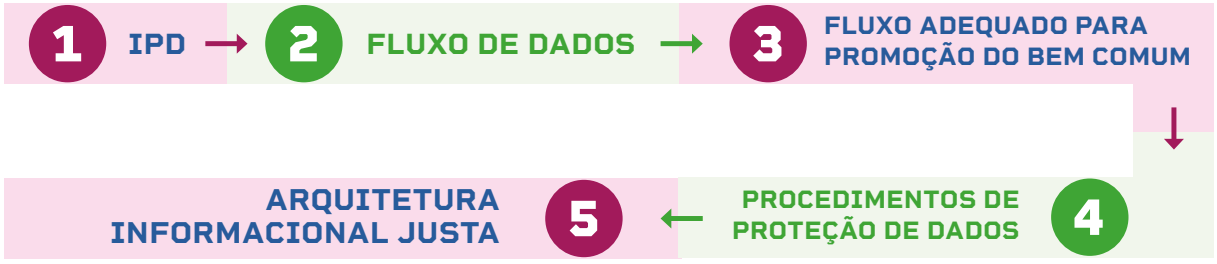
Nesse sentido, em um contexto de IPD, os principais objetos de proteção não são centrados unicamente nos parâmetros de sigilo e vida privada. Parte-se do pressuposto de que os dados pessoais devem circular de maneira segura e adequada, sem impor uma barreira, à priori, aos tratamentos de informações relacionadas à vida privada das pessoas. Ainda, essa circulação adequada de dados também não é limitada a apenas dados da esfera íntima das pessoas, como se era pensado em um conceito restrito de privacidade. A proteção de dados como direito autônomo tem como consequência garantir que apenas aqueles agentes pertinentes tratem dados pessoais de uma pessoa, mas também entende que toda informação pessoal é passível de tutela, inclusive dados conhecidos por terceiros ou mesmo disponíveis publicamente, já que o objetivo, ao final, é proteger o titular, inclusive da violação de outros direitos, como a sua autonomia e o livre desenvolvimento da sua personalidade.

Diante do objetivo desse ecossistema regulatório de proteção de dados em preservar outros direitos das pessoas, nota-se que passam a estar abarcados por esse arcabouço normativo todo dado pessoal que o tratamento vai impactar o titular, não apenas informações privadas, íntimas, ou sensíveis. Ou seja, estão sujeitos às normas de proteção de dados os tratamentos que versem sobre dados vinculados a uma pessoa que possam afetar sua esfera de direitos e interesses. Não se fala mais em uma proteção restrita a um conceito de dado pessoal reducionista, se limitando a apenas aquelas informações com vínculo imediato, direto e exato a uma pessoa identificada. No ecossistema de um direito à proteção de dados, utiliza-se um conceito expansionista de dado pessoal que abarca informa-

ções com vínculo mediato ou inexato a uma pessoa identificável, mesmo que indeterminada, em um primeiro momento, mas que pode ser identificada e afetada a partir da agregação de informações.

Nesse sentido, fica evidente que o fio condutor do arcabouço de proteção de dados é a mensuração e a análise do impacto que o titular estará sujeito quando seus dados forem tratados. Em uma IPD, por mais que sejam conduzidos processos de identificação diretos, a proteção de dados é bastante tensionada, e por isso deve ser observada, no tratamento de dados que impactam o acesso das pessoas a direitos e serviços, mesmo que versem sobre dados anonimizados ou de grupos.

As etapas de implementação de uma IPD estão relacionadas às ferramentas de proteção de dados pessoais, já que as normas de proteção de dados endereçam diversos procedimentos para o estabelecimento de um fluxo seguro, mesmo que intenso, de dados e, com isso, uma arquitetura informacional justa. Uma das facetas desse fluxo adequado é justamente a promoção de um interesse público, em vista que, como estabelecido pelo Supremo Tribunal Federal na ADI 6649, não há "uma visão dicotômica que coloque o interesse público como bem jurídico a ser tutelado de forma totalmente distinta e em confronto com o valor constitucional da privacidade e proteção de dados pessoais"[83]. O interesse público é promovido na concretização do direito à proteção de dados, com seus direitos e princípios próprios.



As obrigações legais descritas na LGPD e na interpretação constitucional do direito fundamental à proteção de dados procedimentalizam as formas de se promover o interesse público e dá os instrumentos necessários para que elas ocorram com segurança jurídica, e justamente abandonando a ideia de sigilo e

83 SUPREMO TRIBUNAL FEDERAL. Ação Direta de Inconstitucionalidade 6.649 Distrito Federal. p. 33. Disponível em: https://portal.stf.jus.br/processos/downloadPeca.asp?id=15358978491&ext=.pdf. Acesso em: 2 dez. 2024.

consentimento como parâmetros únicos ou centrais para um adequado fluxo de dados. Dessa forma, é fundamental a observância dos parâmetros procedimentais previstos na lei para que as aplicações na IPD atendam a um interesse público. Em acordo com o terceiro capítulo deste relatório, o desenvolvimento da IPD deve estar em acordo com os parâmetros de autonomia e autodeterminação informativa, proteção contextual e separação informacional.

Um dos desafios de se estabelecer e implementar soluções inovadoras, como uma IPD, é justamente a definição das ferramentas de prestações de contas, isso porque, mesmo que ainda não estejam consolidadas as suas responsabilidades, os agentes que estão envolvidos na infraestrutura devem ser accountables pelas práticas que realizam. Sem a definição de **núcleos de responsabilidade**, instala-se um cenário de insegurança, o que enfraquece sobremaneira o uso da IPD. É pouco provável que as pessoas utilizem e confiem em sistemas que não sabem com quem estão se relacionando e se serão prejudicadas por ele.

Ainda, por contar em sua definição com a multiplicidade de atores colaborando em um mesmo ecossistema, a falta de definição de responsabilidades e mecanismos de prestação de contas pode criar um vácuo e insegurança quanto às regras comuns a todos atores. Um exemplo disso é a abrangência de regras de transparência, que são mais rígidas para órgãos públicos. No contexto de IPD's, essas regras mais elevadas também deveriam ser compartilhadas e estendidas a atores privados que desenvolvem serviços nessa infraestrutura?

Os usuários da IPD devem ter mecanismos de reparação dos danos que eles venham a sofrer por meio do uso da infraestrutura. Por isso, é fundamental que as pessoas saibam com quem estão se relacionando ao usar as aplicações de uma IPD. A responsabilidade de cada agente deve ser clara para o usuário, a fim de que ele saiba quem procurar quando precisar ter seu direito reparado. Vale destacar que a identificação dos responsáveis pela IPD não transfere às pessoas o ônus de garantir reparação no caso de dano, especialmente em um cenário de baixo letramento digital. A definição da cadeia de responsabilidade em uma IPD é complexa pela multiplicidade de agentes envolvidos, mas a definição de quem é responsável por qual funcionalidade é fundamental para que o dever de reparar surja apenas para aqueles que deram causa ao dano.

Por um lado, os agentes envolvidos na IPD devem definir quando e de que forma

são responsáveis pela IPD, mesmo que contratualmente, por outro lado elas não podem escapar de uma responsabilidade legal diante da violação de um direito do usuário que cause dano. A definição da responsabilidade na infraestrutura é especialmente relevante diante do vínculo entre a IPD e o Poder Público, que pode dar causa a uma responsabilidade solidária ou subsidiária do Estado[84], além da diferença do regime de responsabilidade civil aplicável ao Estado e os particulares.

Por meio de uma definição robusta dos níveis de responsabilidade, os usuários passam a confiar[85] na infraestrutura e nos seus agentes, de forma a compreender suas funcionalidades e incentivar que outras pessoas também as utilizem. O sucesso da IPD também depende da **confiança** que as pessoas depositam nela, de forma que se agentes mal-intencionados participam do sistema e obtém informações autênticas, as pessoas poderiam parar de usar a IPD para se proteger[86].

Por meio de uma procedimentalização da proteção de dados, busca-se chegar em uma arquitetura informacional que promova justiça de dados e, com isso, permite a maximização do valor público. Ou seja, no fim e ao cabo, a geração de o bem comum depende de uma avaliação contextual da arquitetura informacional que demonstre a sua adequação às regras de proteção de dados, não apenas descritos na LGPD, mas como um direito fundamental.

A título de exemplo, para identificar e avaliar o valor público gerado pela IPD, é fundamental que o **fluxo informacional** de suas aplicações, como a identidade digital, seja mapeado e desenhado de acordo com os parâmetros de proteção de dados. Apenas com uma governança de dados robusta, transparente e pautada na promoção de direitos fundamentais é possível verificar se o interesse público está sendo promovido ou não[87]. Isso porque o valor dos dados é altamente dependente do contexto e da finalidade para a qual eles são usados. A mera posse de

---

84 Disponível em: https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias-antigas/2017/2017-11-19_08-00_A-responsabilidade-do-Estado-e-das-concessionarias-de-servicos-publicos.aspx. Acesso em: 20 jan. 2025.

85 UNDP. The DPI Approach: A Playbook. 21 ago. 2023, p. 10. Disponível em: https://www.undp.org/publications/dpi-approach-playbook. Acesso em: 27 mar. 2024.

86 EPICENTER.WORKS. Analysis of Privacy-by-Design EU Legislation on Digital Public Infrastructures. 2024. Disponível em: https://epicenter.works/fileadmin/medienspiegel/user_upload/epicenter.works_-_DPI_Safeguards.pdf. Acesso em: 17 out. 2024. p. 5

87 VEALE, Michael. Reasons for Concern around Mariana Mazzucato's Proposals for Data Governance. Michael Veale. Disponível em: https://michae.lv/mariana-mazzucatos-proposals-for-data-governance-are-concerning/#fn7. Acesso em: 2 dez. 2024.

dados não garante a geração de valor público. É crucial considerar como os dados são tratados, analisados e utilizados para gerar benefícios sociais tangíveis.

Ao mesmo tempo, o fluxo de dados pessoais não é considerado justo apenas com o consentimento dos usuários da IPD, a essa arquitetura por onde essas informações vão transitar é um fator componente e condicionante do caráter de justiça e autodeterminação informacional das pessoas. Assim como o arcabouço de proteção de dados não incide apenas sobre os dados privados e íntimos, a participação e a autodeterminação informacional não se restringem à coleta do consentimento do titular dos dados.

Como será destacado nesta seção, em diversos momentos na IPD sequer será possível pedir o consentimento do titular para uma determinada atividade de tratamento dada a sua necessidade para execução de uma política pública, cumprimento de uma obrigação legal, ou interesse legítimo do agente. Ainda assim, mecanismos de salvaguarda e mitigação dos riscos a direitos fundamentais devem estar presentes para que o titular preserve sua autodeterminação e o desenvolvimento de sua personalidade, de forma geral. A manutenção da sua capacidade de se autodeterminar não é garantida em um momento pontual e isolado de interação do titular com a IPD, esse pressuposto deve estar embarcado no desenvolvimento da própria infraestrutura.

Ao mesmo tempo, como será destacado a seguir, em situações em que o titular é chamado a consentir com uma determinada atividade, para que seja possível coletar um consentimento livre, informado e inequívoco, são igualmente necessários parâmetros de proteção que sustentem essa escolha e ofereçam proteção para garantir que esse consentimento não seja usado para outra finalidade, que pode ser incompatível, por exemplo.

Nem sempre a autodeterminação da pessoa vai ser concretizada por seu consentimento em deixar que determinado agente trate determinado dado. Ou seja, a ideia de autonomia do titular no tratamento de seus dados não é materializada apenas quando este consente com o tratamento, isto é, quando cabe ao titular decidir se o tratamento deve ser feito ou não[88]. Isso em vista da hipervulnerabili-

88 MENDES, Laura Schertel; FONSECA, Gabriel Campos Soares. Proteção de dados para além do consentimento: tendências de materialização. In: DONEDA, Danilo, et al. Tratado de Proteção de Dados Pessoais. Editora Forense. 2023.

dade do titular frente aos agentes de tratamento como o Poder Público e empresas privadas em decidir como os seus dados devem ser tratados, de forma a ser necessário empoderá-lo e dar a ele ferramentas suficientes para emancipá-lo[89].

4.1.2. Bases Legais

Um dos elementos do ecossistema da proteção de dados pessoais é a definição de uma hipótese legal que fundamente a atividade de tratamento de dados. Cada base legal apresenta seus requisitos de validade, cabendo ao agente responsável pelo tratamento adotar as medidas pertinentes para garantir a observância dos critérios que assegurem a legitimidade do tratamento.

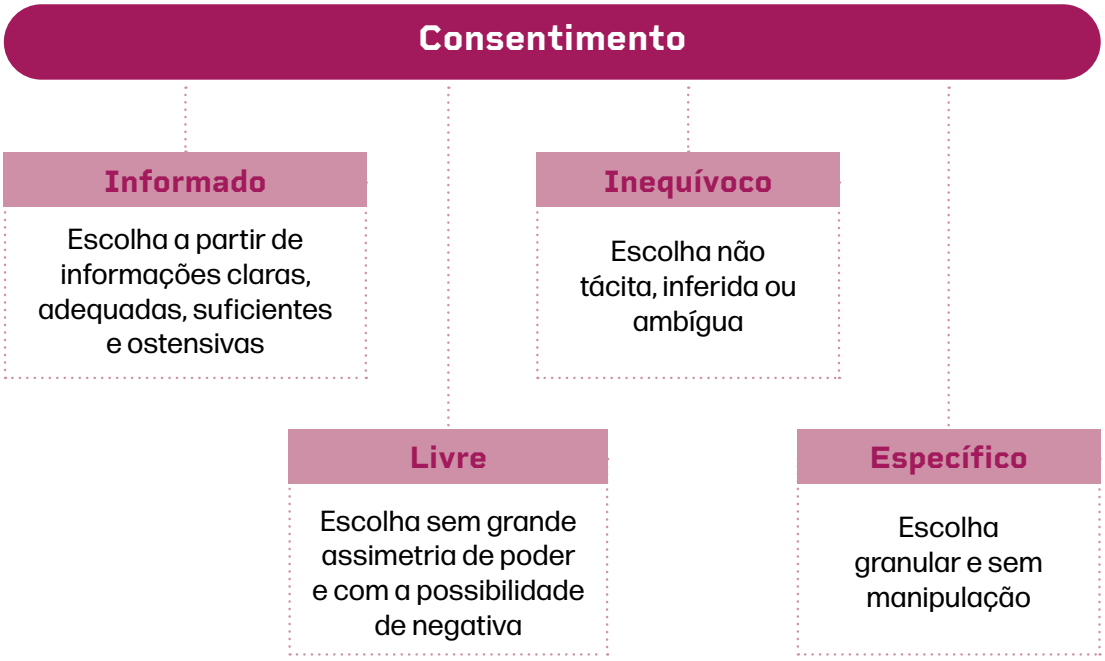
Dentre as hipóteses previstas na LGPD, as opções mais pertinentes ao cenário de IPD são as do consentimento, execução de política pública e cumprimento de obrigações legais ou regulatórias. Cada uma dessas bases possuem peculiaridades próprias que devem ser observadas no caso concreto para avaliar se são aplicáveis ou não, como será analisado a seguir. Ainda, cada atividade de tratamento deve ser justificada por uma base legal, ou seja, para cada finalidade que um grupo de dados é tratado, deve-se haver a indicação de uma hipótese legal adequada a esta finalidade.

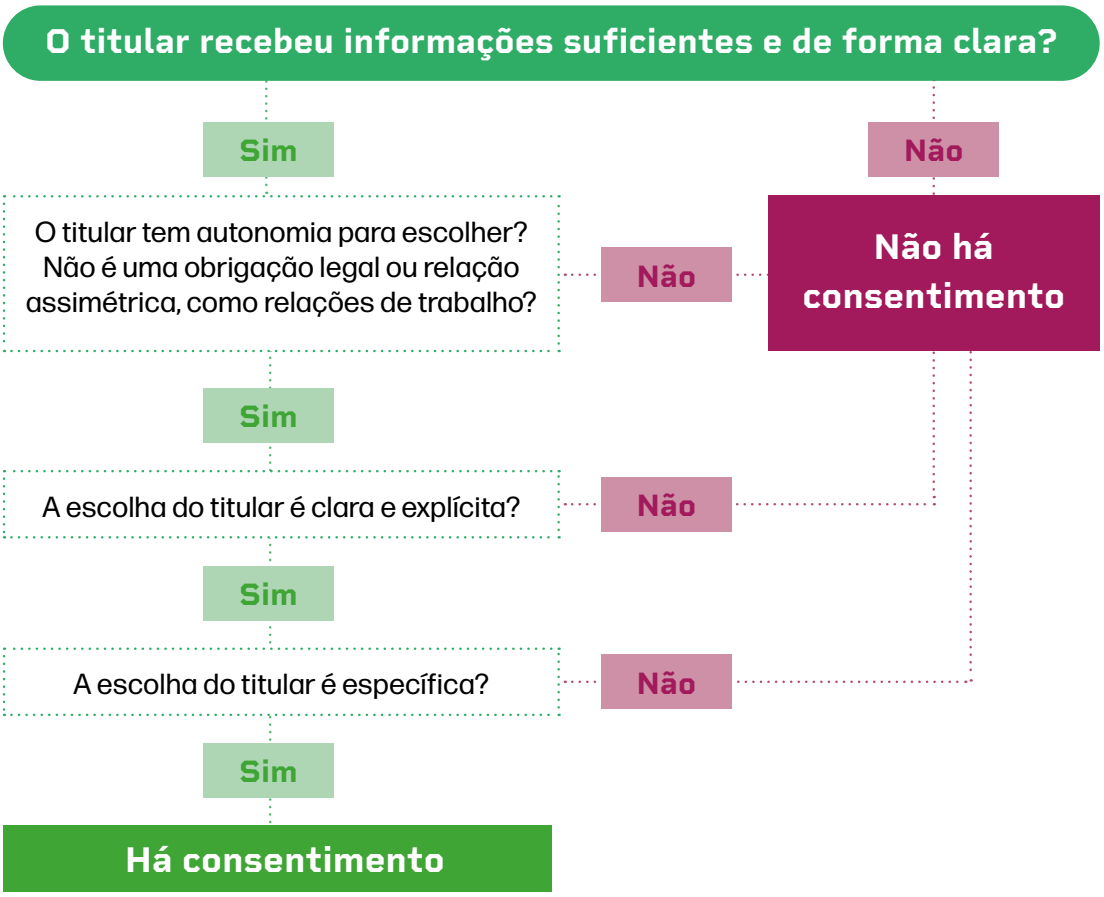
Consentimento

O consentimento é a hipótese que justifica atividades de tratamento de dados em que o titular tem o poder de autorizar ou recusar. Porém, para ser válido, o consentimento deve ser livre, informado e inequívoco, permitindo que o titular tome uma decisão não condicionada e consciente sobre o uso dos seus dados para uma finalidade determinada e informada a ele. Dessa forma, caso a finalidade mude ao longo do tratamento, o titular deve ser informado e ter a oportunidade de fornecer ou não um novo consentimento. Sempre que o consentimento for a base legal escolhida para tratar dados, o titular deve ter a oportunidade de revogar o consentimento, a qualquer momento, fazendo com que o agente deixe de realizar aquela atividade de tratamento de dados.

89 BIONI, Bruno. Proteção de dados pessoais: a função e os limites do consentimento. 2021. Editora Forense. pág. XXVII.

Com isso, a coleta do consentimento do titular é um processo complexo em que o agente responsável pelo tratamento passa a ter o ônus de comprovar que ele é válido e foi obtido em conformidade com a LGPD. Apesar dos requisitos para o consentimento, ele pode ser aplicado em alguns casos relacionados à IPD.





Exemplo hipotético

Consentimento na IPD

A Receita Federal do país do futuro lançou um novo sistema que visa facilitar o processo de declaração de imposto de renda, oferecendo aos contribuintes uma versão pré-preenchida com base em dados já disponíveis em diferentes bases governamentais.

Ao acessar o portal da Receita Federal pela primeira vez naquele ano, a contribuinte Paula se deparou com a seguinte mensagem:

"Cara contribuinte,
A Receita Federal está oferecendo um novo serviço de declaração simplificada. Para utilizar este serviço, precisamos do seu consentimento para acessar e utilizar informações de outras bases de dados governamentais, incluindo:

- Informações salariais (Ministério do Trabalho)
- Dados bancários (Banco Central)
- Informações sobre propriedades (Cartórios de Registro de Imóveis)
- Dados de planos de saúde (Agência Nacional de Saúde Suplementar)

Estas informações serão usadas exclusivamente para pré-preencher sua declaração de imposto de renda, facilitando o processo e reduzindo erros.
Você concorda com o uso dessas informações para este fim?

- ☐ Sim, eu concordo em compartilhar essas informações para o pré-preenchimento da minha declaração de imposto de renda.
- ☐ Não, eu prefiro preencher minha declaração manualmente.

Você pode alterar esta preferência a qualquer momento nas configurações da sua conta. Caso você concorde, as informações serão armazenadas até você submeter a sua declaração de imposto de renda."

Paula, após ler cuidadosamente a mensagem e considerar os benefícios e implicações, decidiu concordar com o uso de suas informações para o pré-preenchimento da declaração.

Este caso ilustra como o consentimento pode ser solicitado de maneira clara e específica, dando ao titular dos dados a opção de escolher se deseja ou não compartilhar suas informações para um fim específico, neste caso, a simplificação do processo de declaração de imposto de renda.

Ao mesmo tempo, existem diversos outros cenários dentro do fluxo informacional de uma IPD em que o consentimento não é a base legal mais adequada para justificar o tratamento de dados, já que muitas vezes as aplicações de IPD não podem depender da autorização do titular. Isso é comum nos casos em que os dados são tratados para operacionalizar políticas públicas e assistenciais, gerar dados para avaliação da efetividade de políticas, promover transparência pública, ou fiscalizar o cumprimento das normas. Nesses casos, o consentimento não pode ser livre, já que o tratamento é necessário para atender obrigação prevista em lei ou para atender interesses do Estado. Por isso, como a coleta do consentimento não é pertinente, outras bases devem fundamentar o tratamento e, junto com elas, outras salvaguardas devem ser concretizadas.

Exemplo hipotético

Uso de dados sem consentimento

Maria recebeu uma mensagem em seu celular. A notificação informou que ela poderia ter direito ao novo Programa de Apoio Familiar (PAF). O texto explicou que o PAF oferecia auxílio financeiro mensal e acesso a cursos de capacitação profissional para famílias em situação de vulnerabilidade. A mensagem ainda explicava que Maria estaria apta a receber o benefício porque os seus dados pessoais cadastrais foram compartilhados pelo órgão do governo que ela tinha vínculo anterior apenas para checar a possibilidade dela também se beneficiar desse programa, informando que após a checagem os dados não estavam mais disponíveis para o órgão gestor do PAF. A mensagem sugeriu que Maria acessasse o portal oficial ou visitasse o Centro de Referência de Assistência Social mais próximo para obter mais informações e confirmar sua elegibilidade.

Por um lado, Maria ficou surpresa com a mensagem, já que ela não havia se inscrito em nenhum programa governamental recentemente. Porém, ela logo lembrou das informações que forneceu ao governo ao longo dos anos relacionados a cadastros para programas sociais, seus dados no último censo e seus registros de trabalho informal. A mensagem apresentava informações sobre de que forma o órgão gestor do PAF encontrou Maria, o que a deixou mais tranquila sobre o ocorrido.

Essa informação deixa claro que a dispensa de consentimento do titular não significa a dispensa de informação adequada a ele. Ainda, a perspectiva de receber auxílio e ter acesso a cursos de capacitação trouxe alívio a Maria. Maria decidiu visitar o centro de assistência social na semana seguinte para obter mais detalhes.

Ainda, mesmo que o consentimento não seja a hipótese justificadora do tratamento, os titulares devem receber uma série de informações sobre o tratamento. Para além do consentimento, a proteção de dados busca, por meio da autonomia e autodeterminação do titular, uma redistribuição de poder entre os titulares e os agentes que desenvolvem a infraestrutura. Esse objetivo não está unicamente associado a uma capacidade individual da pessoa consentir ou não com o tratamento, é importante que se reconheça o caráter coletivo para a proteção de dados na IPD, diante de seu impacto escalar em diversos grupos.

Execução de políticas públicas

Já a base legal de execução de política pública autoriza qualquer tratamento de dados pessoais feito pela administração pública quando necessário para a execução de políticas públicas previstas em leis, regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres. Nesse caso, conforme previsto no artigo 23 da LGPD, o tratamento deve observar o interesse público e atender à finalidade pública do órgão público. Mesmo que não seja necessário coletar o consentimento da pessoa, os órgãos públicos devem informar claramente quais dados serão compartilhados e com quem, além de respeitar os princípios e direitos de proteção de dados.

Exemplo hipotético

Dados de saúde na IPD

O Ministério da Saúde implementou um sistema nacional de prontuário eletrônico chamado "SaúdeConecta". Este sistema integrou dados de saúde de cidadãos de diversas fontes, incluindo hospitais públicos, clínicas particulares conveniadas e farmácias. O objetivo do SaúdeConecta foi melhorar a eficiência do sistema de saúde e a qualidade do atendimento aos pacientes.

O sistema utilizou os seguintes dados dos cidadãos: nome completo e data de nascimento, número de identificação nacional, histórico médico, incluindo diagnósticos e tratamentos, prescrições médicas e registros de compra de medicamentos e resultados de exames laboratoriais e de imagem.

Com base nesses dados, o SaúdeConecta criou alertas para médicos sobre possíveis interações medicamentosas perigosas para cada cidadão, o sistema também otimizou a distribuição de medicamentos em farmácias públicas com base no consumo regional e gerou relatórios anônimos para planejamento de políticas de saúde pública.

O tratamento desses dados pessoais foi realizado sem a necessidade de consentimento dos titulares, baseando-se na base legal de execução de políticas públicas prevista na lei de proteção de dados. No entanto, o Ministério da Saúde implementou rigorosas medidas de segurança e privacidade, incluindo disponibilização de informações em formato de vídeo, controles de acesso a dados pessoais, criptografia de dados, controle de acesso e auditorias regulares. No compartilhamento, o Ministério da Saúde envia para outros agentes apenas aqueles dados estritamente necessários, anonimizados ou psuedonimizados quando possível, e delimita em contrato que esses terceiros não podem usar os dados enviados pelo Ministério para nenhuma outra finalidade, estando sujeitos a penalidades e auditorias regulares.

Vale notar que apenas os membros da administração pública podem se valer dessa base legal, a lei impõe uma limitação do sujeito que pode se valer dessa hipótese. Tanto o art. 7º, IV, quanto o art. 11, II, "b", da LGPD, indicam a possibilidade da administração pública tratar dados para a execução de políticas públicas. Dessa forma, por mais que a IPD seja composta de diferentes atores, inclusive agentes privados, o tratamento de dados pessoais só pode ser justificado pela base de execução de políticas públicas se feita pela administração pública.

Cumprimento de obrigações legais ou regulatórias

Ainda, o tratamento de dados pessoais será possível sempre que necessário para atender a uma lei ou regulamento específico. Esta hipótese se aplica tan-

to a agentes do Poder público como para o setor privado. Ela autoriza o agente responsável a tratar informações pessoais sem a necessidade de consentimento do titular, desde que o tratamento seja estritamente necessário para cumprir uma obrigação estabelecida em lei ou por um órgão regulador. Esse agente deve ser capaz de demonstrar qual obrigação legal ou regulatória está sendo cumprida por meio do tratamento de dados, e este deve ser limitado ao necessário para atender a essa obrigação. Esta base legal é particularmente relevante para entidades públicas e privadas que precisam cumprir obrigações legais específicas, como retenção de dados fiscais, transparência pública ativa e passiva, cumprimento de normas trabalhistas ou atendimento a regulamentações setoriais.

Exemplo hipotético

Tratamento de dados para cumprir dever de transparência

O Ministério da Transparência implementou um sistema chamado "Agenda Aberta" para cumprir as obrigações legais previstas nas normas de acesso à informação. O sistema automaticamente coleta e publica online as agendas de todas as autoridades públicas do órgão.

Maria Silva, Secretária Executiva do Ministério, teve sua agenda do dia 16 de janeiro de 2025 publicada no sistema, incluindo:

- 9:00 - Reunião com representantes da empresa XYZ Tecnologia
- 14:00 - Audiência com o Sindicato dos Servidores Públicos
- 16:30 - Despacho com a Ministra

O sistema "Agenda Aberta" trata os seguintes dados pessoais de Maria e dos participantes das reuniões: (i) nome completo; (ii) cargo/função; (iii) órgão/entidade; (iv) data, hora e local dos compromissos; (v) assunto geral das reuniões.

Este tratamento de dados pessoais é realizado sem necessidade de consentimento, com base na obrigação legal de transparência ativa. O objetivo é permitir o controle social e prevenir conflitos de interesse no exercício da função pública. O sistema mantém os registros publicamente acessíveis por dois anos e depois os transfere para um banco de dados em formato aberto, conforme determinado pela comissão de ética.

Ainda, o sistema "Agenda Aberta" não disponibiliza informações pessoais que não estejam no escopo do interesse público e obrigação legal, de forma a divulgar apenas informações necessárias para garantir transparência sobre as atividades de Maria Silva enquanto Secretária Executiva do Ministério.

A partir da definição de uma base legal para cada atividade de tratamento que realiza, ou seja, para cada finalidade que almeja alcançar com o processamento de dados pessoais, o agente responsável passa a ter de cumprir com os requisitos dessa hipótese, bem como a adequação da base com o caso concretos e os outras obrigações de proteção de dados.

4.1.3. Princípios

Para que o uso de dados pessoais em uma IPD seja adequado, deve haver uma mobilização dos **princípios** de proteção de dados para que se preserve a autodeterminação informativa, a proteção de dados contextual e a separação informacional. Isso quer dizer que todo tratamento de dados deve (i) ter como objeto apenas os dados mínimos, necessários e adequados, (ii) observar uma finalidade legítima, específica e informada, (iii) ser realizado apenas pelos agentes que guardam pertinência, (iv) além de garantir os direitos dos titulares, entre outros parâmetros que serão explorados a seguir.

Finalidade e Adequação

Os princípios de finalidade e adequação determinam que o tratamento de dados pessoais deve atender a finalidades com propósitos legítimos, específicos, explícitos e informados ao titular e, se durante o processo do tratamento houver alteração da finalidade, a alteração deve ser compatível com a razão pela qual os dados foram utilizados no primeiro momento. Assim, o tratamento deve ser compatível com as finalidades informadas ao titular.

Esses princípios de finalidade e adequação estão intrinsecamente ligados ao conceito de autodeterminação informativa, que é fundamental para a proteção de dados pessoais. A capacidade de se autodeterminar está associada ao poder de agência das pessoas sobre elas próprias e sobre o desenvolvimento da personalidade delas e ao equivalente dever do controlador de garantir que os dados

não sejam usados em contexto inadequados e para finalidades não compatíveis com o tratamento inicial. Porém, as aplicações de identidade digital podem tensionar fortemente esse fundamento da proteção de dados ao colocar a pessoa como um objeto a ser identificado, em que os dados pessoais provenientes de diferentes fontes e contextos, informados pelo titular ou não, são agregados para formar um perfil que não necessariamente é representativo da sua identidade auto declarada, mas é o que vai ser levado em conta para validar a identidade ou algum aspecto da identidade de uma pessoa.

Esse uso de dados que não estão no controle do titular para formar uma identidade também se relaciona com a teoria da **integridade contextual** (explorada no capítulo anterior). Esta teoria defende a proteção das informações pessoais em acordo com as expectativas estabelecidas a partir de normas contextuais. Essas normas dizem respeito ao contexto do titular, do remetente e do destinatário do dado, além do tipo de informação que transita entre esses três atores, os interesses das partes e a possibilidade de transmitir o dado para um terceiro, fora do campo contextual da primeira coleta do dado.

Como consequência, as informações pessoais podem fluir desde que respeitem as expectativas e circunstâncias do tratamento, destacando a relevância das ferramentas de transparência e prestação de dados. Esses elementos garantem que o titular não será surpreendido por um tratamento estranho ao seu campo de conhecimento e conhecerá as ferramentas necessárias para questionar e responsabilizar os atores da IPD.

A teoria da integridade informacional reconhece a natureza fluida da privacidade e da proteção de dados, que se molda a partir de elementos contextuais definidos em casos concretos, de forma a não indicar para simples restrição no fluxo de informações pessoais, mas compreender os elementos contextuais do tratamento para um trânsito apropriado de dados. Ao considerar o contexto e as expectativas razoáveis de privacidade, a teoria da privacidade contextual[90] fornece uma estrutura flexível e adaptável para proteger a privacidade em um mundo digital em constante evolução, permitindo uma releitura dinâmica e contextualizada do

90 Nota-se que no contexto norte-americano, não há diferença expressa entre privacidade e proteção de dados, como apresentado no início deste capítulo. Nesse sentido, a ideia de privacidade contextual, como apresentado pela professora Nissenbaum, deve ser entendida como em linha com a perspectiva de proteção de dados brasileira, não apenas da privacidade em si.

fluxo de dados, inclusive os que circulam por meio de uma IPD.

Tensões do princípio da finalidade:

CASO
Coleta obrigatória de impressões digitais para fins eleitorais

CONTEXTO
O tribunal eleitoral de um estado implementou um novo sistema de coleta de impressões digitais dos eleitores, alegando que seria usado exclusivamente para fins de identificação no momento da votação.

Seis meses após a coleta, um jornal local revelou que empresa privada contratada para gerenciar o banco de dados biométricos estava utilizando as informações para desenvolver um sistema de reconhecimento biométrico comercial para empresas responsáveis pela administração de condomínios comerciais a fim de garantir que uma pessoa identificada pelo condomínio é a mesma que a cadastrada no sistema biométrico do tribunal.

EXPLICAÇÃO
Este cenário não materializa o princípio da finalidade.

O tribunal eleitoral coletou as impressões digitais dos eleitores com o propósito específico e declarado, no entanto a empresa contratada para tanto estava conduzindo tratamento de dados para outra finalidade.

Essa nova finalidade representa um desvio significativo da finalidade original. Este novo uso não apenas extrapola o escopo inicial da coleta, mas também não foi informado aos titulares dos dados no momento da coleta. Tal prática também pode comprometer a confiança dos cidadãos no sistema eleitoral.

CASO
Cruzamento de dados bancários para fiscalização tributária

CONTEXTO
A Receita Federal de determinado país implementou um sistema próprio e passou a exigir, por meio de norma, que instituições financeiras reportassem mensalmente todas as movimentações financeiras de seus clientes. Isso incluía informações sobre saques, depósitos e transferências, especialmente aquelas que ultrapassavam um certo valor. O objetivo do sistema era identificar indícios de sonegação fiscal e garantir que todos os tributos fossem corretamente recolhidos.

EXPLICAÇÃO
Neste caso, o princípio da finalidade é observado. Por mais que a coleta de dados feita pelas instituições financeiras seja para a realização da transação, a finalidade do cruzamento de dados é explícita e legítima, além de ser informada ao titular.

A Receita Federal estabeleceu um sistema de coleta de dados financeiros com um objetivo claro e legítimo: identificar possíveis casos de sonegação fiscal e garantir a correta arrecadação de tributos. Embora os dados sejam inicialmente coletados pelas instituições financeiras para fins de transações, o uso subsequente pela Receita Federal para fins fiscais é explicitamente informado aos titulares dos dados. Esta transparência, combinada com a legitimidade do propósito e a base legal para tal coleta e uso, alinha-se com o princípio da finalidade na proteção de dados pessoais.

CASO

Uso de dados de saúde para pesquisa epidemiológica

CONTEXTO

Uma universidade iniciou um estudo sobre a prevalência de doenças respiratórias em uma determinada região, coletando dados de saúde de pacientes que buscavam atendimento em unidades de saúde locais. Os pesquisadores solicitaram informações como histórico médico, diagnósticos anteriores e dados demográficos dos pacientes, assegurando que os dados seriam utilizados exclusivamente para fins de pesquisa epidemiológica.

Ao longo do estudo, os pesquisadores da universidade decidiram utilizar esses dados para desenvolver um aplicativo comercial que visava monitorar a saúde respiratória da população e oferecer serviços de telemedicina. Esse uso dos dados não foi previamente informado aos participantes e não estava alinhado com a finalidade original da coleta.

EXPLICAÇÃO

Este cenário representa uma violação do princípio da finalidade.

A universidade inicialmente coletou dados de saúde com o propósito específico e os participantes consentiram com o uso de seus dados exclusivamente para esta finalidade. A decisão posterior dos pesquisadores de utilizar esses mesmos dados para desenvolver um aplicativo comercial de telemedicina constitui um desvio significativo da finalidade original. Este novo uso não apenas não foi informado aos participantes, mas também não está alinhado com o propósito inicial da coleta. Tal prática compromete a ética da pesquisa e viola a confiança dos participantes.

CASO

Uso de dados pessoais para notificações de emergência

CONTEXTO

A Defesa Civil de um estado implementou um sistema de alerta rápido para notificar a população sobre situações de emergência, como enchentes, deslizamentos de terra e outras catástrofes naturais. Para isso, a Defesa Civil utilizou dados pessoais coletados anteriormente durante o cadastro para programas sociais e serviços públicos, como o cadastro único para programas sociais, o cadastro de cidadão que recebem benefício de aposentadoria, além do cadastro de servidores públicos do estado.

A Defesa Civil implementou medidas rigorosas de segurança para proteger as informações pessoais dos cidadãos, garantindo que os dados fossem utilizados apenas para os fins previstos e não compartilhados com terceiros sem autorização. Ainda, o sistema permitiu uma comunicação rápida e eficaz com a população, contribuindo para salvar vidas e minimizar danos durante situações críticas.

EXPLICAÇÃO

Neste caso, o princípio da finalidade é observado.

Embora os dados pessoais tenham sido originalmente coletados para outros fins, seu uso pela Defesa Civil para notificações de emergência pode ser considerado compatível com a finalidade original de prestação de serviços públicos. O uso desses dados para proteger vidas em situações de emergência serve a um interesse público significativo, o que pode justificar esta extensão da finalidade original. Além disso, a implementação de medidas rigorosas de segurança e a limitação do uso dos dados apenas para os fins previstos demonstram um compromisso com a proteção da privacidade dos cidadãos. Este caso ilustra como, em certas circunstâncias, o princípio da finalidade pode ser interpretado de forma flexível, desde que sejam mantidas salvaguardas adequadas.

Ainda imbricada à ideia de proteção de dados contextual, o conceito de **separação informacional dos poderes** (explorado no capítulo anterior) reforça a ideia de que o acesso de dados deve ocorrer apenas quando houver um interesse específico e legítimo para tanto. O pressuposto é de que o Estado não é uma unidade informacional e, por isso, os dados devem fluir em observância à competência do órgão, que determina os limites e interesse do órgão. Assim, se a teoria da privacidade contextual indica para o contexto como baliza do tratamento e fluxo adequado de dados, a teoria da separação informacional tem a definição das funções e autoridades que acessam o dado como marco de definição da legitimidade do fluxo de dados.

No contexto de IPD, uma infraestrutura que reconhece uma separação informacional implica em uma diferenciação entre quais informações podem ser acessadas por quais entidades, em vista de suas funções e competências. Como uma das aplicações bases da IPD, o uso de dados de identidade, além da simples verificação e autenticação de identidade, tem o potencial de se tornar uma medição quase contínua da vida cotidiana das pessoas por meio da coleta, do processamento e do compartilhamento de seus dados pessoais[91], como forma de acompanhamento da evolução da sua própria personalidade.

Exemplo hipotético

Reuso de dados em contextos distintos

Sofia Oliveira era uma mãe solteira de dois filhos e moradora do bairro de baixa renda. Sofia trabalhava como diarista, com renda instável e insuficiente para sustentar sua família.

Em março de 2003, Sofia visitou o Centro de Assistência Social da sua cidade e, para ter acesso aos benefícios do município, ela preencheu um extenso formulário digital, fornecendo informações detalhadas, como seu histórico de empregos dos últimos 5 anos, renda mensal média, dados sobre a ausência do pai das crianças, endereço atual e anteriores e informações sobre sua rede de apoio familiar.

91 BODY AND DATA. Digitization of Identity in Nepal: Efforts, Experiences and Effects. 2023. Disponível em: https://bodyanddata.org/wp-content/uploads/2023/10/BiometricReport_2023_07_31_Final_compressed.pdf. Acesso em: 12 jan. 2025.

Sofia foi informada que esses dados seriam usados exclusivamente para avaliar sua elegibilidade para programas de assistência. Com isso, ela passou a receber auxílio-moradia e cupons de alimentação, que foram cruciais para melhorar a qualidade de vida de sua família.

Em 2025, o Departamento de Segurança Pública da cidade implementou um novo sistema de prevenção preditiva de crimes. Este sistema, desenvolvido por uma empresa de tecnologia sem experiência em políticas sociais, utiliza algoritmos de aprendizado de máquina para identificar "zonas de alto risco" e "indivíduos propensos a atividades criminosas".

Com objetivo de diminuir a criminalidade na cidade, o presidente do Centro de Assistência Social concordou em compartilhar os dados dos beneficiários com o departamento de segurança. Assim, sem o conhecimento ou consentimento dos cidadãos, o banco de dados da Seguridade Social foi integrado ao sistema. O algoritmo atribuía pontuações de risco baseadas em fatores como instabilidade financeira, residência em áreas de alta criminalidade, ausência de figura paterna no lar, e frequência de mudanças de endereço.

Logo após esse compartilhamento, Sofia foi surpreendida por uma batida policial em sua casa. Os oficiais, munidos de um mandado baseado nas análises do sistema de predição, revistaram sua residência, interrogando-a sobre suas "conexões criminosas". As crianças, assustadas, choravam enquanto os policiais vasculhavam seus pertences.

Nos meses seguintes, Sofia enfrentou diversas visitas policiais frequentes, geralmente nas primeiras horas da manhã ou tarde da noite, além de vigilância ostensiva em seu local de trabalho, levando à perda de clientes, bullying das crianças na escola, rotuladas como "filhos de criminosa", e dificuldades em alugar um novo apartamento devido à "ficha criminal" gerada pelo sistema.

O caso de Sofia só foi reavaliado por uma auditoria independente do sistema que revelou seus graves vieses e violações de privacidade. Embora tenha sido oficialmente inocentada, o dano à sua reputação e bem-estar já havia se concretizado.

É fundamental reconhecer e garantir níveis de informação específicos aos agentes que compõem uma IPD. Ou seja, a própria infraestrutura não deve formar uma unidade informacional, colocando todos os agentes em pé de igualdade para acessar e tratar os dados pessoais disponíveis na IPD. Por mais que haja argumentos em defesa de uma suposta eficiência, planos de vincular os dados disponíveis na IPD com outras organizações públicas e privadas devem ser avaliados com precaução por poderem impactar as pessoas em diversas esferas de suas vidas.

Um sistema eficiente não é aquele que possui acesso indiscriminado a dados disponíveis para qualquer finalidade, mas é sim um sistema que possui uma robusta governança desses dados seguindo os preceitos da proteção de dados para tratamento apenas de dados adequados e necessários. Da mesma forma, não há dicotomia entre a concretização do interesse público e a garantia da proteção de dados, como consequência o interesse público não deve ser entendido "como bem jurídico a ser tutelado de forma totalmente distinta e em confronto com o valor constitucional da privacidade e proteção de dados pessoais"[92]. Assim, a execução do interesse público está em linha com a devida proteção de dados, especialmente na definição de finalidades específicas e conhecidas pelo titular.

Necessidade

O princípio da necessidade, ou da minimização dos dados, exige que os dados pessoais objetos do tratamento sejam limitados ao mínimo necessário para o cumprimento das finalidades que justificam os seus usos. Esse princípio restringe o tratamento aos dados pertinentes, proporcionais e não excessivos em relação às finalidades, de forma a permitir que os agentes responsáveis apenas coletem e tratem os dados essenciais e imprescindíveis para a finalidade que se busca alcançar.

Esse princípio pode ser exemplificado por noções já consolidadas no contexto de identidade por meio dos conceitos de "**zero-knowledge**" e **abertura seletiva de dados**[93]. Esses conceitos funcionam como uma maneira de verificar se determi-

92 SUPREMO TRIBUNAL FEDERAL. Ação Direta de Inconstitucionalidade 6.649 Distrito Federal. p. 56. Disponível em: https://portal.stf.jus.br/processos/downloadPeca.asp?id=15358978491&ext=.pdf. Acesso em: 2 dez. 2024.

93 EPICENTER.WORKS. Analysis of Privacy-by-Design EU Legislation on Digital Public Infrastructures. 2024. Disponível em: https://epicenter.works/fileadmin/medienspiegel/user_upload/epicenter.works_-_DPI_Safeguards.pdf. Acesso em: 17 out. 2024. p. 8

nados atributos ou combinações de atributos de uma pessoa são verdadeiros. Um exemplo simples é verificar se uma pessoa é maior de idade sem revelar sua data de nascimento. Isso se tornou um padrão para os modernos sistemas de identidade digital e é uma condição prévia para tornar os sistemas de IPD adequados a padrões modernos de proteção de dados. O "zero-knowledge" também pode impedir a vinculação do usuário em interações com a mesma ou diferente parte confiável em todos os casos em que a identificação completa do usuário não for necessária.

Exemplo hipotético

Acesso a espaços com verificação de idade

Mariana frequenta a mesma boate toda sexta-feira e o agente que checa a maioridade dela não sabe que ela é a mesma pessoa das semanas anteriores. Isso porque ela compartilha com o agente apenas a validação da sua idade e não o seu nome, foto de perfil ou CPF. Por fim, sempre que uma parte confiável, ou seja, o representante da boate, solicita informações da Mariana, ela precisa ser capaz de poder compartilhar todos os dados, nenhum ou "divulgar seletivamente" apenas partes das informações que lhe foram solicitadas.

É nesse sentido que o desenvolvimento de recursos personalizáveis de controle de dados são entendidos como mais uma ferramenta de gerenciamento e configurações de privacidade, permitindo que os usuários ajustem facilmente suas preferências de compartilhamento de dados. Ao mesmo tempo, a integração de diferentes bases de dados por meio de um compartilhamento amplo dessas bases não é a única solução para troca de informações e validações. A integração lógica permite que apenas os dados necessários para uma finalidade específica sejam acessados ou trocados, reduzindo o risco de exposição desnecessária de informações e possibilitando um controle mais preciso sobre quais dados são compartilhados.

Ainda, funcionalidades como exportação de dados e solicitações de exclusão podem garantir às pessoas mecanismos de controle sobre suas informações pessoais. Essas ferramentas de controle individual são apenas uma parte da equa-

ção que indica para garantia do direito à proteção de dados. Cabe ao agente de tratamento adicionar outros elementos nessa equação para gestão dos riscos de forma compartilhada, já que os agentes também controlam os dados e, por conseguinte, os riscos associados ao tratamento.

Primeiras reflexões

Como determinar que o uso de determinados dados é desproporcional para uma atividade de tratamento?

Uma das principais tensões no uso de dados para identificação em uma IPD é a definição de quais dados pessoais são necessários para identificar alguém. Por um lado, alguns argumentam que a maior quantidade e variedade de dados garante maior confiança no processo de identificação, outros indicam que esses elementos em excesso, especialmente fora de contexto, podem colocar em risco o resultado final. Por isso, a definição de quais dados são necessários para identificar alguém é fundamental para garantir a eficácia do próprio processo.

Uma questão similar a essa já foi enfrentada durante a discussão sobre os dados pessoais que podem ou não podem ser utilizados para a definição de um score de crédito. A Lei do Cadastro Positivo, nº 12.414, proíbe que sejam consideradas para composição da pontuação de crédito informações:

- que não estiverem vinculadas à análise de risco de crédito e aquelas relacionadas à origem social e étnica, à saúde, à informação genética, ao sexo e às convicções políticas, religiosas e filosóficas;
- de pessoas que não tenham com o cadastrado relação de parentesco de primeiro grau ou de dependência econômica;
- relacionadas ao exercício regular de direito pelo cadastrado, previsto no inciso II do caput do art. 5º desta Lei.

Ou seja, neste caso, a lei definiu informações que são consideradas excessivas e, por isso, não podem ser utilizadas para definição de score de crédito. A mesma questão é posta no contexto de identidade: quais dados são necessários para avaliar se uma pessoa é possível fraudadora quando identificada para acessar um programa de assistência social, por exemplo? Se na lógica

do big data todo dado pode ser potencialmente útil para identificação de alguém, é necessário definir parâmetros de necessidade que não sejam pautados apenas por elementos técnicos, mas também por elementos de justiça.

É nesse sentido que este Relatório aponta para a necessidade de se observar parâmetros mínimos para um fluxo justo de dados, como a implementação de práticas de separação informacional e proteção contextual para a promoção do valor público e um desenvolvimento autônomo da personalidade dos usuários da IPD.

A separação informacional implica em manter distintos os conjuntos de dados coletados para diferentes finalidades, evitando o cruzamento indiscriminado de informações que pode levar a inferências invasivas ou injustas. Já a proteção contextual visa assegurar que os dados sejam utilizados apenas no contexto para o qual foram originalmente coletados, respeitando as expectativas razoáveis de privacidade dos indivíduos. Essas práticas são fundamentais para equilibrar a necessidade de identificação eficaz com a proteção dos direitos individuais e coletivos. Elas ajudam a prevenir o uso excessivo ou inadequado de dados pessoais, que poderia resultar em discriminação, violação de privacidade ou outros prejuízos aos titulares dos dados.

A título de exemplo, em uma análise contextual para acesso a um programa social, é possível que se perceba não ser razoável o tratamento de dados de pessoas que não tenham relação direta com um beneficiário, como parentes que não sejam dependentes econômicos, ou informações relacionadas ao exercício regular de direitos pelo cidadão, como participação em sindicatos ou associações.

Além dessa análise crítica sobre a necessidade específica de cada dado tratado para atingir uma determinada finalidade, o princípio da necessidade também é um comando normativo para que os agentes utilizem sempre as formas e métodos de tratamento menos intrusivas possíveis para atingir aquela finalidade[94]. Dessa forma, cabe ao agente responsável avaliar se existem outras formas menos onerosas e com menores riscos para os titulares.

94 ANPD. Hipóteses legais de tratamento de dados pessoais Legítimo Interesse. 2024. Disponível em: https://www.gov.br/anpd/pt-br/centrais-de-conteudo/materiais-educativos-e-publicacoes/guia_legitimo_interesse.pdf. Acesso em: 5 fev. 2025.

Transparência e livre acesso

Assim como os princípios da finalidade e da adequação estão intimamente associados aos conceitos de desenvolvimento da personalidade, proteção contextual, e separação informacional, os princípios da transparência e do livre acesso também são impactados por essas noções. O princípio da transparência garante aos titulares o acesso a informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento. Já o princípio do livre acesso garante, aos titulares, possibilidade de uma consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais.

Para que seja possível mensurar as expectativas contextuais dos titulares e, com isso, avaliar se há violação dos seus direitos, é fundamental analisar qual o nível de transparência é concedido a ele pelo agente responsável pelo tratamento. Isso porque se o usuário da IPD recebe as informações pertinentes sobre o tratamento e ele conhece o fluxo de dados é pouco provável que ele seja surpreendido pelo funcionamento da IPD. A privacidade como integridade contextual também é garantida pelo princípio da transparência, já que as expectativas dos titulares são alinhadas e formadas a partir das informações que recebem.

Nesse mesmo sentido, as decisões do STF analisadas neste relatório reforçam o compromisso do Poder Público em dar transparência sobre os compartilhamentos que realiza, cabendo ao órgão dar transparência às atividades de tratamento de dados pessoais que realiza.

Parâmetros para o Poder Público compartilhar dados segundo o STF

O órgão que compartilha deve estar de acordo com a LGPD:

Cumprimento integral dos requisitos, garantias e procedimentos estabelecidos na LGPD, no que for compatível com o setor público. Utilização de sistemas eletrônicos de segurança e de registro de acesso, inclusive para efeito de responsabilização em caso de abuso.

O órgão deve publicizar os tratamentos que realiza:

Obrigação do órgão público dar a devida publicidade às hipóteses em que cada entidade governamental compartilha ou tem acesso a banco de dados pessoais.

O órgão que compartilha deve publicizar o compartilhamento:

Instauração de procedimento administrativo formal, acompanhado de prévia e exaustiva motivação, para permitir o controle de legalidade pelo Poder Judiciário.

O órgão que compartilha deve avaliar os riscos do compartilhamento:

Avaliação da compatibilidade do compartilhamento de dados, verificando se o compartilhamento de dados pessoais a outro órgão público para uma finalidade diversa daquela inicialmente declarada subverte a autorização dos titulares. Adoção de medidas proporcionais e estritamente necessárias ao atendimento do interesse público.

A partir dessas informações, os titulares de dados, usuários da IPD, passam a ter ferramentas adequadas para compreender, decidir e questionar com maior autonomia sobre o tratamento de seus dados pessoais e seus impactos, inclusive no desenvolvimento da sua personalidade.

Exemplo hipotético

Transparência como ferramenta para o usuário da IPD

Em 2030, o governo federal implementou uma IPD chamada "Portal de Transparência de Dados do Cidadão" (PTDC). Este portal permite que qualquer cidadão acesse informações sobre como seus dados pessoais estão sendo utilizados por diferentes órgãos governamentais.

Por meio de um acesso individualizado, cada usuário acessa o portal usando sua identidade digital e passa a ver quais órgãos têm acesso a quais tipos de dados pessoais dele. O portal também permite que o usuário veja um registro de quando e por quem os dados foram acessados, além da finalidade declarada para o uso dos dados. O portal oferece um sistema para que os cidadãos possam questionar o uso de seus dados diretamente aos órgãos responsáveis.

Acessando este portal, Mônica, uma usuária da IPD, acessa o PTDC e descobre que seus dados de saúde foram acessados pela Receita Federal. Intrigada, ela utiliza o mecanismo de questionamento do portal para perguntar o motivo da Receita Federal acessar seus dados de saúde.

A Receita Federal responde dentro de um prazo estabelecido, explicando que o acesso foi feito para verificar se Mônica pode se valer da restituição de imposto de renda por conta do pagamento do plano de saúde. Mônica, não satisfeita com a explicação, por acreditar que o comprovante de matrícula no plano de saúde seria suficiente para essa finalidade, pode então solicitar mais informações, pedir a retificação ou exclusão dos dados, se considerar que estão sendo usados indevidamente, ou registrar uma reclamação formal se acreditar que houve violação de seus direitos.

Por conta desse questionamento, a Receita Federal reavaliará se é necessário que ela acesse dados de saúde dos cidadãos. Esse avanço só foi possível porque, para além de fornecer informações, o princípio da transparência também capacita os cidadãos a serem agentes ativos na proteção de seus dados pessoais.

Ainda, do ponto de vista da LGPD, especificamente para o Poder Público, a lei reforça o dever de publicidade em relação aos tratamentos de dados pessoais realizados pela administração pública, alinhado também aos princípios de impessoalidade e publicidade da administração pública prevista no art. 37, da CF. Segundo o art. 23, I, da LGPD, cabe às pessoas jurídicas de direito público fornecer "informações claras e atualizadas sobre a previsão legal, a finalidade, os procedimentos e as práticas utilizadas para a execução dessas atividades, em veículos de fácil acesso, preferencialmente em seus sítios eletrônicos". Para os casos de compartilhamento de dados, é uma boa prática que os agentes públicos formalizem esse tratamento por meio da celebração de contrato, convênio ou instrumento congênere[95].

Não Discriminação

O princípio da não disciminação impossibilita que o tratamento de dados pessoais seja realizado para fins discriminatórios ilícitos ou abusivos. No contexto de IPD, especialmente de identidade digital, este princípio é crucial para assegurar que o tratamento de dados pessoais seja realizado de forma ética e respeitosa, protegendo os indivíduos contra práticas ilícitas ou abusivas de discriminação que possam surgir do uso indevido de suas informações pessoais, ainda que de forma indireta ou não intencional. O objetivo desse princípio é assegurar que as informações pessoais não sejam utilizadas para perpetuar preconceitos e desigualdades existentes.

Exemplo hipotético

Sistema automatizado com efeitos discriminatórios

Um sistema de avaliação de crédito habitacional foi implementado na Cidade dos Dados, seu objetivo é avaliar, a partir dos dados de identidade das pessoas, a elegibilidade de cidadãos para programas de habitação social. Para tanto, o sistema utiliza dados da identidade digital dos cidadãos, incluindo histórico de emprego, renda, endereço e histórico de crédito. Com base nessas informações, o sistema determina a probabilidade de um candidato cumprir

95 ANPD. Guia Orientativo de Tratamento de dados pessoais pelo Poder Público. 2023. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/documentos-de-publicacoes/guia-poder-publico-anpd-versao-final.pdf. Acesso em: 20 dez. 2024.

com os pagamentos do financiamento habitacional, informação que é usada para aprovar ou rejeitar automaticamente as solicitações de financiamento.

Após um ano de operação, uma auditoria independente revelou que candidatos de certas áreas urbanas, historicamente marginalizadas, tinham uma taxa de rejeição significativamente maior, mesmo quando outros fatores eram semelhantes. Ainda, mulheres, especialmente mães solteiras, eram aprovadas com menos frequência do que homens com perfis financeiros similares.

Logo foi percebido que o sistema foi treinado com dados históricos que refletiam padrões discriminatórios preexistentes no mercado imobiliário. O sistema usava variáveis aparentemente neutras, como código postal, para inferir características protegidas, como raça. Um artigo acadêmico de Ramon Vilarino e Renato Vicente demonstra como o uso de informações de localização introduz preconceito racial em um modelo de pontuação de crédito, mesmo que essa informação não seja diretamente dada ao modelo[96].

Essas questões não foram percebidas durante o desenvolvimento do sistema porque a equipe responsável pelo sistema não era suficientemente diversa para identificar potenciais vieses e esses requisitos não foram considerados. Por conta dessas falhas, o sistema reforçou padrões existentes de segregação habitacional e desigualdade econômica. A revelação desses problemas levou a uma perda significativa de confiança no programa de habitação social e no uso de tecnologia para tomada de decisões governamentais.

Dessa forma, as aplicações de infraestrutura pública digital devem ser testadas proativamente antes de sua implementação para evidenciar que não geram discriminações, podendo inclusive contar com auditorias externas e relatórios públicos, como será debatido na próxima seção. Esses testes permitem a identificação e mitigação de riscos antes que eles se tornem problemas reais, economizando recursos e protegendo os usuários da infraestrutura.

96 VILARINO, Ramon; VICENTE, Renato. An experiment on the mechanisms of racial bias in ML-based credit scoring in Brazil. arXiv preprint arXiv:2011.09865, 2020.

4.1.4. Direitos dos titulares

Os direitos dos titulares de dados representam o aspecto mais robusto e direto da LGPD para o exercício da autodeterminação informativa. Esse conjunto de direitos proporciona aos titulares ferramentas para que eles possam conhecer e interferir no tratamento que suas informações pessoais estão sujeitas, permitindo-lhes, inclusive, tomar decisões informadas sobre o uso de seus dados. A autodeterminação informativa, portanto, não é apenas um conceito abstrato, mas um direito prático e exercitável através dos mecanismos estabelecidos pela LGPD.

Enquanto os princípios e bases legais da LGPD criam um arcabouço geral de obrigações para os agentes responsáveis pelo tratamento, os direitos dos titulares são os instrumentos práticos através dos quais as pessoas podem não apenas exigir o cumprimento dessas obrigações, mas também exercer ativamente sua autodeterminação informativa. Esses direitos capacitam os titulares a questionar, modificar e até mesmo revogar o uso de seus dados pessoais, colocando-os no centro do processo de tratamento de informações.

No campo da proteção de dados, mesmo no contexto de IPD, o titular tem o direito de saber uma série de informações, como quais dados pessoais estão nas aplicações de IPD, quem os acessa e quais são suas responsabilidades, por quanto tempo, para qual finalidade, e com quem compartilham, conforme artigo 9º da LGPD. Ainda, as pessoas usuárias da IPD devem receber informações sobre seus direitos enquanto titulares de dados e a forma do tratamento a que seus dados estão submetidos.

Especificamente, os titulares podem: (i) solicitar a confirmação de que seus dados pessoais estão sendo tratados por determinada aplicação de IPD, (ii) acessar os dados pessoais que são tratados, (iii) solicitar a correção dos dados incompletos, incorretos ou desatualizados, (iv) solicitar a anonimização, bloqueio e eliminação de dados desnecessários, excessivos e/ou tratados em desconformidade com a LGPD, (v) solicitar informações sobre as entidades públicas e privadas com as quais a empresa realiza uso compartilhado de dados, (vi) solicitar a portabilidade dos seus dados para outro fornecedor de serviço ou produto, observados os segredos comercial e industrial, e (vii) opor-se ao tratamento realizado com fundamento em uma das hipóteses de dispensa de consentimento, em caso de descumprimento à LGPD.

Ainda, quando a base legal que justifica o tratamento for o consentimento, o titular pode (viii) não fornecer o consentimento, (ix) revogar o consentimento a qualquer momento por meio de procedimento gratuito e simplificado, e (x) solicitar a eliminação de dados tratados com base no consentimento, exceto quando necessário para cumprimento de obrigação legal ou regulatória pelo controlador; estudo por órgão de pesquisa, garantida a anonimização dos dados; transferência a terceiro; ou uso exclusivo do controlador, vedado o acesso por terceiro, e desde que anonimizados os dados.

Quando forem utilizadas decisões automatizadas, o titular tem o direito de (xi) solicitar revisão das decisões que afetem os seus interesses e (xii) obter informações claras e adequadas sobre os critérios e procedimentos utilizados para as decisões automatizadas.

Primeiras reflexões

Decisões automatizadas na formação de uma identidade

Os processos de identidade cada vez mais abarcam práticas de profiling e de decisões automatizadas para a definição da probabilidade de uma pessoa ser quem diz ser ou possuir um atributo ou característica, seja por meio de uma identidade em camadas, seja pelo uso massivo de dados.

Como argumentado anteriormente, as aplicações na IPD podem tensionar a capacidade de autodeterminação informativa das pessoas, o livre desenvolvimento da personalidade e a autonomia. Processos como o de profiling têm como objetivo justamente inferir preferências, atitudes, comportamentos ou eventos futuros apenas com base na correlação de dados capturados e inferidos, sem levar em conta relatos pessoais e reivindicações narrativas, o que pode limitar sobremaneira as oportunidades garantidas às pessoas e a forma delas agirem. Isso porque esses sistemas visam prever e inferir possíveis comportamentos no futuro e direcionar as pessoas justamente para essas possibilidades, definindo um padrão de comportamentos adequados e esperados. Essa fixação de um padrão pode levar à sistematização de discriminações e injustiças, ameaçando direitos fundamentais de pessoas que não chegaram a praticar nenhuma ação contrária ao esperado, mas que foram identificadas por um sistema automatizado como possuindo uma alta probabilidade para tanto.

Nesse mesmo contexto de decisões automatizadas para identificação, também estão sendo aplicadas lógicas probabilísticas, o que significa que os sistemas não buscam mais uma identificação absoluta e inequívoca dos indivíduos, mas trabalham com graus de probabilidade e margens de erro aceitáveis. Essa abordagem implica que as decisões são tomadas com base em inferências estatísticas e correlações de dados, em vez de certezas sobre a identidade ou características de uma pessoa. Assim, as pessoas perdem a visibilidade como seus dados estão sendo utilizados para identificação. Isso significa que elas deixam de exercer papel ativo para serem identificadas e passam a ser objeto de identificação, sem saber quais informações foram usadas e formam sua identidade.

Em face dessas novas práticas de identificação, os direitos dos titulares surgem como ferramentas para sopesar essas práticas com a capacidade de autodeterminação das pessoas. Esses direitos permitem que a identidade não seja criada apenas por um monólogo da parte identificadora, mas um diálogo entre a parte identificadora e a parte identificada. De forma específica, o direito de obter informações sobre os critérios e procedimentos utilizados é um instrumento para se compreender o processo de tomada de decisão automatizada e, com isso, garantir os outros direitos do titular, como contestar e solicitar revisão da decisão com base nas informações dadas.

Os dois direitos visam "equilibrar a distribuição de poderes na tomada de decisão, a fim de garantir que o titular participe, proporcionalmente, do processo de decisão que afete seus interesses"[97]. Por isso, no contexto de identidade como IPD, o titular pode utilizar esses direitos para ferramentas para que ele conheça os elementos que formam a sua identidade e, com essas informações, possa se opor e pedir revisão desses elementos.

Vale notar que dois direitos são aplicáveis inclusive no caso de decisões intermediárias. Em regra, um processo de decisão automática é dividido em diversas etapas, que podem conter ou não a participação de uma pessoa para tomar a decisão final e alguns poderiam argumentar que esse direito só existe quando a decisão final não é humana. Porém, a LGPD dá abertura a uma "maior capilaridade para tratamentos automatizados serem considerados como processos de tomada de decisão, ainda que não sejam o último ponto de uma árvore de decisão"[98]. Logo, as pessoas podem requerer esses direitos em uma IPD, mesmo que a decisão automatizada não seja final, mas que afetem seus interesses e direitos fundamentais.

---

97 ALMEIDA, Eduarda Costa. Diga-me os seus dados, que eu lhe direi quem você vai ser: o Direito à explicação como garantia da autodeterminação informativa na Lei Geral de Proteção de Dados Pessoais. 2023. 168 f., il. Trabalho de Conclusão de Curso (Bacharelado em Direito) – Universidade de Brasília, Brasília, 2023.

98 MARTINS, Pedro Bastos Lobo. A regulação do profiling na lei geral de proteção de dados: o livre desenvolvimento da personalidade em face da governamentalidade algorítmica. Dissertação (mestrado) - Universidade Federal de Minas Gerais, Faculdade de Direito, 2021, p. 77. Disponível em: https://repositorio.ufmg.br/bitstream/1843/43900/4/Pedro%20Martins%20-%20Disserta%C3%A7%C3%A3o%20-%20A%20REGULA%C3%87%C3%83O%20DO%20PROFILING%20NA%20LEI%20GERAL%20DE%20PROTE%C3%87%C3%83O%20DE%20DADOS%20o%20livre%20desenvolvimento%20da%20personalidade%20em%20face%20da%20governamentalidade%20algor%C3%ADtmica.pdf. Acesso em: 28 jun. 2024.

A divulgação dessas informações deve ocorrer por meio de materiais claros, simples e acessíveis. Essa obrigação dialoga com o dever de transparência e informação sobre os tratamentos de dados pessoais na infraestrutura. Nesse sentido, a implementação de **canais acessíveis de atendimento dos direitos dos titulares, suporte e denúncia** é fundamental para garantir que os cidadãos possam registrar reclamações e problemas enfrentados na utilização da IPD. Esses canais facilitam e agilizam a identificação de falhas ou vulnerabilidades no sistema, o que aumenta a responsividade da infraestrutura e, consequentemente, aumenta a confiança dos usuários na IPD.

Esses canais devem ser inclusivos e acessíveis a qualquer pessoa, seja de forma digital ou física, inclusive aquelas com restrições de acesso à IPD. Diante da complexidade de atores que compõem a IPD, os agentes responsáveis pelo tratamento de dados devem acordar entre si quem terá a competência de atender os direitos dos titulares, garantindo de todos os requerimentos sejam devidamente tratados e respondidos. É igualmente importante estabelecer prazos claros para resposta e resolução de problemas, garantindo que as pessoas sintam que suas preocupações estão sendo tratadas com seriedade.

O encarregado é o agente responsável por responder os requerimentos dos titulares, além de receber comunicações da autoridade nacional, entre outros. Esse encarregado é nomeado pelo agente responsável pelo tratamento, ou seja, todo agente que decide sobre os aspectos de um tratamento de dados deve ter um encarregado. No Poder Público, isso significa que as obrigações de agente responsável "são exercidas pelos órgãos públicos que desempenham funções em nome da pessoa jurídica da qual fazem parte, fenômeno que caracteriza a distribuição interna das competências"[99]. Logo, cabe ao órgão público que trata dados cumprir a LGPD, inclusive nomeando um encarregado.

99 ANPD. Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado. 2021. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/2021.05.27GuiaAgentesdeTratamento_Final.pdf. Acesso em: 20 jan. 2025.

Exemplo hipotético

Atualizando dados em uma IPD

Marília, uma usuária de uma aplicação de IPD de saúde, recentemente realizou novos exames médicos que apresentaram resultados diferentes dos registrados no sistema. Esses exames mais recentes não estão registrados na infraestrutura porque foram feitos em uma clínica não vinculada a essa aplicação, porém ela deveria atualizar os dados da aplicação para poder agendar uma consulta médica de análise do resultado dos exames. Para atualizar suas informações, ela decide exercer seu direito de alteração de dados pessoais, especificamente médicos.

Inicialmente, Marília tenta atualizar suas informações através do aplicativo de saúde em seu smartphone. No entanto, ela percebe que não há opção para atualizar manualmente os resultados de exames. Ainda, a aplicação da IPD é composta por vários agentes, como o Ministério da Saúde, responsável pela gestão geral do sistema, hospitais públicos e privados, que fornecem dados de atendimento, laboratórios, que compartilham resultados de exames, além da plataforma de identificação da IPD, que fornece autenticação digital dos usuários.

Diante de tantos agentes, Marília busca o contato do encarregado desses agentes para poder requerer seu direito. Porém, apenas encontra o contato da plataforma de identificação da IPD. Frustrada, Marília não encontra orientações claras sobre como proceder. Ela tenta entrar em contato com seu médico, mas é informada que ele não tem permissão para alterar os dados na IPD.

Marília então decide entrar em contato com o encarregado da plataforma de identificação da aplicação da IPD. Após várias transferências, ela é informada que precisa entrar em contato com a instituição de saúde que realizou os exames originais. Contudo, quando Marília explica que os novos exames foram feitos em um laboratório diferente, o atendente não sabe como proceder e Marília acaba sem saber a quem recorrer.

Este cenário destaca a necessidade de um ponto de contato claro e acessível para usuários que precisam atualizar seus dados na IPD, além de procedimen-

tos bem definidos para a atualização de informações e maior transparência e educação dos usuários sobre seus direitos e os processos relacionados à gestão de seus dados de saúde na IPD. A situação de Marília ilustra como o exercício de direitos dos titulares é benéfico para todos os agentes que compõem a IPD e para o próprio funcionamento da infraestrutura.

A experiência do usuário é um fator crucial. Os agentes participantes podem fornecer insights valiosos sobre a usabilidade e acessibilidade dos sistemas, garantindo que a IPD atenda às necessidades reais das pessoas. A construção de uma IPD justa e cidadã depende da inclusão digital, permitindo que todos os segmentos da sociedade tenham acesso à infraestrutura. O envolvimento da comunidade no desenvolvimento da IPD aumenta a transparência e, consequentemente, a **confiança** nas instituições públicas e na própria infraestrutura digital.

A coleta sistemática de feedback e o acompanhamento das mudanças na capacidade das pessoas em navegar na IPD são essenciais para avaliar a eficácia do sistema. Realizar pesquisas regulares de satisfação do usuário, além de implementar métricas para avaliar a facilidade de uso e navegação permite a identificação de áreas que necessitam de melhorias. Mesmo após o desenvolvimento da solução, o **monitoramento participativo** é essencial para o adequado funcionamento da IPD.

O exemplo a seguir ilustra como uma aplicação de identidade em IPD pode tensionar os elementos de proteção de dados:

Elementos da identidade	Tensões à proteção de dados
João possui uma carteira de identidade em seu nome, identificando-o com sua biometria, foto, nome completo, CPF, sexo, data de nascimento, filiação, naturalidade e nacionalidade, além do órgão expedidor e o local de expedição da carteira de identidade.	A emissão de um documento de identidade é um dos requisitos mais frequentes para acessar serviços e produtos essenciais ou não, como contas bancárias, benefícios sociais, espaços de lazer e outros. Em regra, esse documento é emitido pelo Poder Público e utilizado por outros agentes, públicos ou privados, em diversos contextos. Em regra, o compartilhamento de dados de identidade ocorre de forma ilimitada e não rastreável, ou seja, o documento e todos seus dados são enviados para terceiros, mesmo sua cópia, sem que seja possível registrar com quais agentes as informações foram compartilhadas e o contexto associado.
João, ao completar 18 anos, passa a declarar imposto de renda. Para a declaração do imposto de renda, João se cadastra no portal do governo do seu país e autoriza o órgão responsável pelos tributos a usar os seus dados para a emissão da declaração de imposto de renda pré-preenchida.	A separação informacional indica para um cenário em que o órgão responsável pelos tributos não possui as mesmas informações do órgão responsável pela emissão da identidade, já que a finalidade do tratamento é diversa. Ao mesmo tempo, sabendo da diferença de competência dos órgãos, cabe ao titular autorizar esse fluxo.
Ao perder seu emprego de motorista de caminhão, João se registra no cadastro para programas sociais do governo como requisito para receber uma assistência social do governo. Esse registro é feito por meio da sua conta do portal do governo.	A identidade, sendo uma das ferramentas para acessar benefícios sociais, é utilizada pelo órgão de assistência social. Para tanto, é possível que o cidadão tenha de acessar o portal do governo enquanto faceta digital de seus serviços. O cadastro feito pelo cidadão é feito em determinado contexto, que delimita a forma e as balizas do tratamento de dados para garantia de sua autonomia enquanto sujeito de direitos.

João, ao abrir conta em um banco visando a busca de crédito para abrir um empreendimento, faz seu registro nesse banco a partir do portal do Estado, que transmite apenas as informações essenciais para que o banco consiga identificar João e validar sua identidade bem como seus dados cadastrais. Ao solicitar o empréstimo, João tem o crédito negado. Alguns dos motivos da negativa é o fato de João estar no cadastro para programas sociais, o que indicaria uma situação de vulnerabilidade financeira, e a informação de que João se declarou isento de imposto de renda há 4 anos. Essa informação foi acessada pelo banco por meio do portal. João não foi capaz de contestar a decisão por não existir mecanismo de transparência que informasse os motivos da negativa do crédito e um sistema de revisão da decisão. João não está mais inserido no cadastro de assistência social que anteriormente recebia e não declara imposto de renda, pois toda sua renda vem de atuação profissional informal, e busca a formalização de seu empreendimento a partir deste empréstimo solicitado.	Para validar sua identidade, pode não ser necessário o compartilhamento de todos os dados relacionados à identidade de uma pessoa. Nesse caso, o compartilhamento dos dados ou de sua validação podem ser feitos como forma de minimizar o tratamento realizado por outros agentes, como uma instituição bancária. No entanto, o compartilhamento ou a simples comunicação de dados entre agentes que possuem finalidades e competências diferentes pode indicar violação de princípios como a separação informacional e a proteção contextual, afetando a autonomia e desenvolvimento da personalidade de uma pessoa. No caso, a instituição bancária acessa informações conhecidas pelo órgão responsável pela emissão da identidade e pelo órgão responsável pelos tributos. Os dados tratados por cada agente ocorre em determinado contexto e versa sobre uma situação específica, não necessariamente sendo pertinente, útil ou eficaz uma comunicação entre agentes, como na definição de acesso ao crédito. Apesar disso, havendo comunicação de dados, mecanismos de informação, contestação e revisão sobre essa troca de dados são essenciais para a garantia da autonomia da pessoa. Isso porque o acesso a determinados produtos e serviços passa a ser balizado pela troca de dados. Esses mecanismos de oposição à comunicação ou aos seus efeitos é ferramenta básica para a minimização dos efeitos negativos desse tratamento, garantindo um fluxo justo de dados.

João se cadastra em uma plataforma privada de busca de emprego, e faz o seu login por meio do portal do governo, que inicialmente informa apenas o nome e CPF de João, garantindo a sua identificação para a plataforma, que solicita dados cadastrais complementares como email e histórico educacional e profissional. Ao se candidatar em uma vaga de motorista de caminhão dentro dessa plataforma, o processo de candidatura solicita validação da identidade por meio do portal, e solicita autorização para acessar outros dados do portal, dentre eles dados relativos a transações financeiras de João, uma vez que o empregador arcará com o seguro do caminhão que seria dirigido por João. João tem sua candidatura declinada. As informações relativas a seu registro no cadastro para programas sociais e sua pontuação de crédito foram fatores determinantes para essa decisão.	As informações de identidade vinculadas ao cidadão podem passar a fluir para finalidades de acesso ao trabalho, para além da simples validação de sua identidade. Novamente, a falta de mecanismos de oposição pode prejudicar o cidadão. O contexto do tratamento pode não estar sendo levado em conta, ao não observar a esfera social do tratamento do titular, enquanto cidadão e não futuro empregado, o destinatário da informação, bem como o tipo de dado compartilhado e as expectativas definidas pelo contexto de identificação. No caso, a violação dos parâmetros de proteção de dados na relação de identidade e acesso a benefício social ganha nova camada ao se adicionar nova relação, a trabalhista. Vale destacar a possibilidade do titular autorizar a plataforma de busca de emprego acessar dados tratados pela autoridade responsável pela identidade. Por mais que o cidadão possa não autorizar, reconhece-se sua posição de vulnerabilidade diante do impacto da não autorização, qual seja, a negativa de oferta de emprego. Por mais que haja espaço para não autorização, é possível questionar o quão livre seria esse consentimento.

João volta a uma situação de vulnerabilidade financeira e solicita novamente a sua inclusão no programa de assistência social. Ao fazer esse requerimento, é solicitado que João envie uma foto de alta qualidade de seu rosto e de sua carteira de identidade. Isso ocorreu pois o sistema de detecção de fraudes indicou um indício de fraude na solicitação de João. Esse sistema antifraude é operado pela mesma empresa que presta serviços de pontuação de crédito para o banco que negou empréstimo a João. O celular de João está com a câmera quebrada e não há postos de atendimento presencial no distrito rural em que vive.	Em um contexto de IPD, a falta de concretização do direito de proteção de dados pessoais por ferramentas de proteção contextual e separação informacional afetam a capacidade de desenvolvimento da personalidade do cidadão. O efeito dessa violação ganha complexidade ao criar camadas de aplicações que se comunicam e, com isso, comunicam suas vulnerabilidades. Em um contexto de digitalização sem IPD, as falhas e vulnerabilidades do sistema poderiam ter impactos locais, ou pouco transversais. Porém, o desenvolvimento de uma infraestrutura digital possibilita justamente que aplicações diferentes possam ter implicações entre si, o que possibilita a transmissão dessas falhas. Nesse cenário, a necessidade de ferramentas efetivas de proteção são ainda mais imprescindíveis para seu devido funcionamento em acordo com o direito das pessoas.

Diante das tensões entre a proteção de dados e o desenvolvimento de soluções de identidade, a elaboração de **avaliações de impacto** se mostram ferramentas fundamentais na estruturação dessa arquitetura informacional. O objetivo da avaliação é, a partir do mapeamento e da antecipação dos possíveis riscos de uma aplicação, auxiliar no processo de tomada de decisões informadas e proteger interesses sociais[100]. Isso porque, antes mesmo de eventos negativos acontecerem, inclusive com a violação de direitos, as organizações que conduzem essas avaliações já procuram ativamente minimizar a probabilidade deles ocorrerem e adotar salvaguardas mais protetivas.

Ainda, avaliações de impacto também funcionam como ferramentas de prestação de contas dos agentes envolvidos no desenvolvimento dos sistemas. Antes mesmo deles serem disponibilizados para uso geral, já é possível entender quais práticas serão adotadas para endereçar e minimizar os riscos identificados. A elaboração e revisão deste relatório fortalece a ideia de **justiça procedimental[101],** uma vez que elas não se resumem apenas à obtenção de um resultado justo, mas de um caminho percorrido até esse resultado que também o seja[102].

No contexto de sistemas de identidade, avaliações de impacto podem funcionar como ferramenta estratégica para garantir-se que a aplicação de identidade esteja adequada à proteção de dados, diante do **alto risco no tratamento de dados[103].** Os sistemas de identidade, especialmente em contexto de IPD, visam ser acessíveis a grande número de pessoas, dando causa a um tratamento de dados pessoais em larga escala, além de afetar significativamente os interesses e direitos dessas pessoas. É por meio da identidade que as pessoas acessam uma série de direitos e benefícios.

Diante dos riscos envolvidos em um sistema de identidade em IPD, o desenvol-

---

100 KLOZA, Dariusz et al. Avaliações de impacto sobre a proteção de dados na União Europeia: complementando o novo regime jurídico em direção a uma proteção mais robusta dos indivíduos. d.pia.lab Policy Brief, 1/2017, 2020.

101 KLOZA, Dariusz. Privacy Impact Assessments as a Means to Achieve the Objectives of Procedural Justice. Jusletter IT. Die Zeitschrift für IT und Recht, 2014. Disponível em: https://researchportal.vub.be/en/publications/priva-cy-impact-assessments-as-a-means-to-achieve-the-objectives-o. Acesso em: 11 mai. de 2024.

102 KLOZA, Dariusz. Privacy Impact Assessments as a Means to Achieve the Objectives of Procedural Justice. Jusletter IT. Die Zeitschrift für IT und Recht, 2014. Disponível em: https://researchportal.vub.be/en/publications/priva-cy-impact-assessments-as-a-means-to-achieve-the-objectives-o. Acesso em: 11 mai. de 2024.

103 BIONI, Bruno; GARROTE, Marina; MEIRA, Marina; PASCHOALINI, Nathan. Entre a visibilidade e a exclusão: um mapeamento dos riscos da Identificação Civil Nacional e do uso de sua base de dados para a plataforma gov.br. Associação Data Privacy Brasil de Pesquisa, 2022.

vimento de um sistema em conjunto com um relatório de impacto que abranja possíveis impactos sobre os direitos e as liberdades fundamentais de indivíduos e grupos é útil para um mapeamento e uma mensuração desses riscos. Essa avaliação pode ser tornada pública antes de qualquer processamento de dados[104], a fim de que haja espaço para análise e discussão dos riscos a serem enfrentados. Essa avaliação pode incluir um levantamento das salvaguardas adequadas para limitar e mitigar os riscos identificados.

Vale notar que o desenvolvimento de um relatório de impacto deixa evidente como as diretrizes de proteção de dados pessoais surgem como ferramentas úteis no desenvolvimento e implementação dos sistemas de identidade em uma IPD, evitando a retenção de dados desnecessários e garantindo um compartilhamento seguro e não abusivo de dados. Isso reforça a noção de parâmetros de proteção de dados funcionarem como ferramentas relevantes na concretização do bem comum, requisito essencial para perceber uma aplicação digital como parte de uma IPD.

4.2. Prestação de contas e participação na IPD

4.2.2. Prestação de contas para prevenção e precaução

O racional regulatório da Lei Geral de Proteção de Dados segue uma lógica de prevenção, ou seja, a busca da proteção dos titulares antes da concretização do dano e a adoção de medidas para evitar que eles aconteçam, por isso ela é chamada de *ex ante*. A ideia é de que regular e criar sanções aplicáveis apenas depois que o problema acontecer pode ser extremamente custoso do ponto de vista social. Ainda, os supostos custos elevados da incerteza sobre os efeitos da regulação podem ser atenuados, mesmo com um grau relativamente pequeno de conhecimento antecipado que os reguladores podem alcançar[105].

Ao invés do regulador prescrever uma série de comandos regulatórios e aplicar controles seguindo uma lógica repressiva por meio da responsabilização, seja civil ou penal, quando dano for causado, a LGPD estabelece uma obrigação dos

104 COUNCIL OF EUROPE. Guidelines on National Digital Identity. Consultative Committee of the Convention for the protection of individuals with regard to automatic processing of personal data. Council of Europe, February 2023. p. 12.

105 GALLE, Brian, In Praise of Ex Ante Regulation, Georgetown Law Faculty Publications and Other Works, 2015, p. 1759.

agentes prestarem contas acerca das medidas implementadas para endereçar possíveis danos e "da eficiência das medidas adotadas não só para a contenção dos riscos das suas atividades, mas, também, a respeito do cumprimento das normas de proteção de dados em geral"[106].

A prestação de contas, como um princípio da LGPD, orientou uma mudança lógica da lei, em que para além de garantir o direito de reparação de danos, quando eles ocorrerem, o agente responsável pelo tratamento também deve atuar antes mesmo desses danos se concretizarem. Essa nova lógica de regular o tratamento de dados e incentivar práticas responsáveis é uma resposta a uma maior discricionariedade e liberdade que os agentes de tratamento possuem para processar dados, já que a lei não é prescritiva sobre o que deve ou não ser feito.

Em normas como o Marco Civil da Internet (art. 7º, VII e IX), o legislador apontava para um contexto em que o titular era responsável por decidir se seu dado pessoal poderia ou não ser tratado. Porém, a LGPD compartilhou progressivamente o poder decisório sobre a possibilidade e a forma do tratamento de dados com os agentes de tratamento, cabendo a eles escolher os métodos para cumprir efetivamente a legislação. Essa evolução permite que os agentes de tratamento adaptem suas práticas de proteção de dados de acordo com suas necessidades específicas, desde que cumpram os objetivos da lei.

A falta de prescrição do agir dos agentes responsáveis garante maior liberdade a suas atividades de tratamento, inclusive na construção de soluções digitais em uma IPD, e, como contraprestação, esses agentes passam a ter mais responsabilidades para garantir que o tratamento seja adequado, ou seja, não viola direitos dos titulares de dados. Para atingir esse objetivo, o agente deve adotar medidas de mitigação que previnam a ocorrência de danos para as pessoas e essas medidas devem ser eficazes, isso quer dizer que o agente tem o ônus argumentativo de demonstrar que os instrumentos implementados por ele são suficientes para minimizar os riscos mapeados.

Essas medidas são identificadas por Bruno Bioni como um maquinário precaucionário, que foi lapidado pela LGPD para descrever-se instrumentos básicos para

106 BIONI, Bruno Ricardo. Accountability no desenho (design) da regulação de dados pessoais: virtudes e vicissitudes. 2021. Tese (Doutorado em Direito Comercial) - Faculdade de Direito, Universidade de São Paulo, São Paulo, 2021. doi:10.11606/T.2.2021.tde-25102022-123810. Acesso em: 2025-01-26. Resumo.

esse sistema de prestação de contas, que é composto dos seguintes elementos[107]:

- ☐ Obrigação de os agentes responsáveis pelo tratamento de dados manterem um registro das atividades de tratamento de dados pessoais que realiza (art. 37);

- ☐ Obrigação de os agentes responsáveis pelo tratamento de dados nomearem um encarregado pelo tratamento de dados pessoais (art. 41);

- ☐ Obrigação de os agentes responsáveis pelo tratamento de dados elaborarem relatório de impacto à proteção de dados pessoais como a documentação do processo de gerenciamento de risco (art. 38);

- ☐ Obrigação de os agentes responsáveis pelo tratamento de dados implementarem, desde a fase de concepção do produto ou do serviço até a sua execução, medidas aptas a proteger os dados pessoais de qualquer forma de tratamento inadequado ou ilícito (art. 46, §2º);

- ☐ Obrigação de os agentes responsáveis pelo tratamento de dados adotarem boas práticas a fim de que a organização atenda de forma ampla e procedimentalmente o previsto na LGPD (art. 50).

Em um contexto de IPD, essa lógica da prestação de contas tem como efeito a obrigação do agente de tratamento agir antes do dano ocorrer a partir do mapeamento do impacto da infraestrutura na garantia de direitos das pessoas e no delineamento de práticas que façam face a esse impacto. Esse agir é uma forma também dos atores envolvidos na construção de uma IPD assumirem para si suas responsabilidades enquanto a desenvolvedores e operadores da IPD, mesmo que seja uma infraestrutura formada por uma complexa rede de agentes, sejam eles de natureza pública ou privada.

Assim como indicado na seção anterior, a prestação de contas reforça o dever dos agentes atuarem em observância aos princípios de proteção de dados, além da indicação de uma hipótese legal que sustente e fundamente o tratamento e

107 BIONI, Bruno Ricardo. Accountability no desenho (design) da regulação de dados pessoais: virtudes e vicissitudes. 2021. Tese (Doutorado em Direito Comercial) - Faculdade de Direito, Universidade de São Paulo, São Paulo, 2021. doi:10.11606/T.2.2021.tde-25102022-123810. Acesso em: 2025-01-26. p. 66.

das ferramentas de concretização dos direitos dos titulares. Por meio do cumprimento dessas obrigações e por uma perspectiva de proteção de dados, o valor público da IPD é desbloqueado e passa a ser atendido na medida em que os procedimentos de proteção de dados são implementados.

Assim como a adoção de medidas de prestação de dados, o desenvolvimento da IPD é um processo contínuo e dinâmico, não é uma tarefa finita ou estática no tempo. As IPDs operam em um ambiente tecnológico e social em constante evolução. As necessidades das pessoas, as ameaças à segurança, as inovações tecnológicas e as expectativas em termos de serviços essenciais disponíveis no meio digital estão em constante mudança. Portanto, é crucial que o desenvolvimento e a manutenção das IPDs sejam vistos como um processo iterativo e adaptativo.

Por sua vez, a lógica de prestação de contas deve acompanhar essa natureza dinâmica das IPDs. As medidas de *accountability* não podem ser simplesmente implementadas uma vez e depois esquecidas. Elas precisam ser continuamente avaliadas, atualizadas e aprimoradas para garantir que permaneçam eficazes e relevantes diante das mudanças nas tecnologias, nas políticas públicas e nas expectativas sociais.

Além disso, a própria compreensão do que constitui uma prestação de contas eficaz ou uma aplicação de IPD pode evoluir com o tempo. Por isso, são exigidas atualizações constantes nas práticas de *accountability*. Tanto o desenvolvimento das IPDs quanto às medidas de prestação de contas associadas devem ser vistas como processos contínuos de aprendizagem, adaptação e melhoria. Isso requer uma abordagem flexível e responsiva, capaz de incorporar feedback, lições aprendidas e novas perspectivas ao longo do tempo, garantindo assim que as IPDs continuem a servir efetivamente ao interesse público.

Uma das consequências desse movimento de prestação de contas e garantia da sua eficácia é o estabelecimento de um fórum público para escrutínio e debate sobre mapeamento de riscos e possíveis medidas de mitigação. O dever de prestação de contas tem como efeito obrigar o responsável pelo tratamento a "gerar conhecimento sobre quais são os possíveis efeitos adversos de uma atividade e, com isso, debater quais serão as medidas a serem adotadas não apenas antes,

mas, também, durante e depois de uma atividade de tratamento de dados"[108].

Vale notar as duas faces da prestação de contas, uma (i) preventiva, que busca "evitar um dano ou coibir um risco que afigura-se certo ou confirmado"[109], mensurável, e outra (ii) precaucionária, que tem como objeto os riscos abstratos, não conhecidos ou percebidos antes da sua ocorrência[110]. Cabe ao agente de tratamento observar essas duas faces, que se complementam, para implementar uma visão ampla de prestação de contas, não apenas limitada ao cumprimento formal e mecânico de ações de compliance já mapeadas. Uma prestação de contas precaucionária deve desencadear "qualitativamente um processo de contestação e co-deliberação concernente ao desenho final da sua atividade de tratamento de dados"[111].

Exemplo hipotético

Pesos e contrapesos da prevenção e precaução na IPD

O Estado A implementou um sistema de identidade digital chamado "ID-Seguro". Essa solução de identidade permitia que a pessoa solicitasse sua identidade digital através de um aplicativo do Estado e, após a coleta de dados biográficos e biométricos, a pessoa poderia acessar serviços públicos estaduais e privados online, de forma que o ID-Seguro funcionasse como uma chave de acesso digital.

Antes do lançamento, a equipe desenvolveu políticas de segurança robustas, implementou criptografia de ponta a ponta, contratou auditorias de segurança externas, treinou extensivamente a equipe em práticas de proteção de dados, ainda realizou uma avaliação de impacto à proteção de dados (RIPD) detalhada.

Todos esses processos e documentações foram mantidos internos, compartilhados apenas com autoridades reguladoras quando solicitados. O público

108 BIONI, Bruno Ricardo. Accountability no desenho (design) da regulação de dados pessoais: virtudes e vicissitudes. 2021. Tese (Doutorado em Direito Comercial) - Faculdade de Direito, Universidade de São Paulo, São Paulo, 2021. doi:10.11606/T.2.2021.tde-25102022-123810. Acesso em: 2025-01-26. p. 225.

109 HARTMANN, O princípio da precaução e a sua aplicação no direito do consumidor. Direito & Justiça v. 38, n. 2, p. 156-182, jul./dez. 2012. p.157

110 HARTMANN, O princípio da precaução e a sua aplicação no direito do consumidor. Direito & Justiça v. 38, n. 2, p. 156-182, jul./dez. 2012. p.157

111 BIONI, Bruno Ricardo. Accountability no desenho (design) da regulação de dados pessoais: virtudes e vicissitudes. 2021. Tese (Doutorado em Direito Comercial) - Faculdade de Direito, Universidade de São Paulo, São Paulo, 2021. doi:10.11606/T.2.2021.tde-25102022-123810. Acesso em: 2025-01-26. p. 229.

em geral não teve acesso a essas informações ou oportunidade de contribuir para o desenvolvimento do sistema.

O Estado B, vizinho ao A, vendo o desenvolvimento do ID-Seguro, decidiu desenvolver o sistema similar. Durante o processo o Estado B publicou versões preliminares do RIPD para consulta pública, realizou audiências públicas para discutir o design do sistema, criou um comitê consultivo com representantes da sociedade civil, implementou um mecanismo de opt-out para certas funcionalidades após feedback público, e estabeleceu um portal de transparência onde os cidadãos podem acompanhar o desenvolvimento e uso do sistema.

Embora o Estado B tenha realizado menos ações quantitativas de prevenção, sua abordagem qualitativa voltada à precaução permitiu maior escrutínio público e ajustes baseados no feedback dos cidadãos.

Como consequência, quando uma vulnerabilidade de segurança foi descoberta em ambos os sistemas, o Estado A, apesar de suas medidas preventivas, enfrentou maior resistência pública devido à falta de transparência. O Estado B, por outro lado, conseguiu responder mais rapidamente e com maior apoio público, pois já havia estabelecido canais de comunicação e confiança com a população.

A ideia principal é de que uma abordagem de accountability baseada na precaução, que envolve transparência e participação pública, pode ser mais eficaz em construir confiança e resiliência em IPD, mesmo que quantitativamente menos ações possam ser tomadas em comparação com uma abordagem puramente preventiva[112].

112 BIONI, Bruno Ricardo. Accountability no desenho (design) da regulação de dados pessoais: virtudes e vicissitudes. 2021. Tese (Doutorado em Direito Comercial) - Faculdade de Direito, Universidade de São Paulo, São Paulo, 2021. doi:10.11606/T.2.2021.tde-25102022-123810. Acesso em: 2025-01-26. p. 228.

É nesse sentido que os deveres de prestação de contas, para além das obrigações de transparência e acesso a dados, fortalecem também as medidas eficazes de prevenção de danos e de escrutínio público como forma de balancear a liberdade e a discricionariedade dos agentes responsáveis por tratar dados pessoais. Os deveres de prestação de contas não se restringem à elaboração meramente artificial, burocrática e formal de documentos que indicam o vínculo das aplicações de IPD com as obrigações de proteção de dados, mas abarcam ações eficazes para minimizar os riscos que surgem com o tratamento de dados pessoais na IPD.

Dessa forma, em conjunto com os mecanismos de prestação de contas preventivo, as ferramentas de participação também podem auxiliar na promoção de um **fluxo justo de dados**. No contexto de IPD como identidade, as diretrizes de proteção de dados pessoais surgem como ferramentas úteis no desenvolvimento e implementação dos sistemas de identidade, evitando a retenção de dados desnecessários e garantindo um compartilhamento seguro e não abusivo de dados.

A elaboração de um relatório ou avaliação de impacto é um processo fundamental para mapear riscos e endereçá-los por meio de medidas de salvaguardas, como defendido anteriormente. Com isso, a construção desse documento está vinculada ao nível de contingenciamento do poder decisório para destravar o fluxo informacional concluído a partir da definição do risco residual no tratamento[113]. É justamente por conta da liberdade do agente em tratar dados que o RIPD surge como estratégia regulatória para deixar evidente de que forma os interesses no tratamento de dados objeto do relatório estão sendo balanceados com os interesses dos titulares de dados.

O relatório de impacto é tanto um mecanismo de prevenir danos mapeáveis quanto como um espaço de precaução por meio da participação e escrutínio público[114]. Assim, uma vez que os agente de tratamento tem mais liberdade para tratar dados, os

113 BIONI, Bruno Ricardo. Accountability no desenho (design) da regulação de dados pessoais: virtudes e vicissitudes. 2021. Tese (Doutorado em Direito Comercial) - Faculdade de Direito, Universidade de São Paulo, São Paulo, 2021. doi:10.11606/T.2.2021.tde-25102022-123810. Acesso em: 2025-01-26. p. 110.

114 GOMES, Maria Cecília O. Para além de uma "obrigação legal": o que a metodologia de benefícios e riscos nos ensina sobre o relatório de impacto à proteção de dados. In Direito Digital: Debates Contemporâneos, orgs. LIMA, Ana Paula. HISSA, Carmina. SALDANHA, Paloma Mendes. São Paulo: Revista dos Tribunais, 2019, pp 141-153.

seguintes elementos devem ser considerados numa avaliação de impacto[115]:

- O RIPD deve ser elaborado antes da implementação do tratamento, a fim de que seja possível avaliar, de antemão, os possíveis riscos associados a esse tratamento e, com isso, iniciar o processamento com o menor risco possível.

- Para cada nova atividade ou processo que surgir, é necessário avaliar os riscos e mapear os dados pessoais envolvidos para verificar a necessidade ou não da elaboração de um RIPD, bem como para atualização do registro de operações de tratamento.

- O RIPD deve contar uma descrição dos (i) tipos de dados pessoais tratados, (ii) operações de tratamento, (iii) finalidades (incluindo interesses legítimos) e (iv) hipóteses legais, além de uma (v) avaliação da necessidade e da proporcionalidade das operações de tratamento, os riscos para os direitos e liberdades dos titulares de dados e (vi) as medidas a serem adotadas para minimizar esses riscos.

- Quando houver divergências no processo decisório sobre os riscos e medidas de mitigação, a ANPD recomenda, como uma boa prática, o registro de diferentes opiniões identificadas no processo de elaboração do RIPD, incluindo as justificativas para a opção adotada.

- O RIPD é um documento em constante evolução, inclusive porque os riscos de determinado procedimento podem ser mitigados a partir da adoção de medidas adicionais.

Diante das peculiaridades e da centralidade de dados pessoais em sistemas de identidade, a elaboração e atualização do RIPD relacionado ao tratamento de dados é uma das ferramentas para se garantir uma justiça procedimental no uso desses dados. Nesse sentido, o Alan Turing Institute elaborou um modelo de relatório de impacto específico para o contexto de identidade, em que há constante análise de proporcionalidade e necessidade no tratamento, além do intenso fluxo de da-

115 ANPD. Relatório de Impacto à Proteção de Dados Pessoais (RIPD). 2023. Disponível em: https://www.gov.br/anpd/pt-br/canais_atendimento/agente-de-tratamento/relatorio-de-impacto-a-protecao-de-dados-pessoais-ripd. Acesso em: 17 jan. 2025.

dos[116]. Especificamente, o modelo do instituto cita os seguintes tópicos de atenção:

- Os limites do relatório devem ser claramente delineados, especificando quais componentes, processos e fluxos de dados estão incluídos no escopo do relatório. Ao definir o escopo, é importante considerar todo o ciclo de vida da aplicação de identidade digital, desde o registro e a autenticação iniciais até o gerenciamento contínuo e a eventual desativação. Isso pode incluir elementos como mecanismos de comprovação de identidade, processos de emissão de credenciais, protocolos de autenticação, sistemas de controle de acesso e acordos de compartilhamento de dados com terceiros. As organizações também devem levar em conta qualquer infraestrutura de suporte, como bancos de dados, APIs ou serviços em nuvem que desempenhem um papel no ecossistema de identidade digital.

- Todos os tipos de dados pessoais coletados, processados ou armazenados pelo sistema devem ser mapeados. Para cada categoria de tratamento, uma descrição detalhada dos elementos de dados específicos coletados e sua finalidade no sistema deve ser descrita. Esse inventário é essencial para entender o escopo e a sensibilidade das informações tratadas pelo sistema. Ao dividir os dados em categorias específicas, como informações pessoais básicas, detalhes de contato, identificação emitida pelo governo e dados biométricos, é possível avaliar melhor as possíveis implicações de proteção de dados associadas a cada tipo de informação.

- Deve haver uma descrição detalhada de todos os métodos usados para coletar dados pessoais. Para cada método, deve-se descrever o processo e os tipos de dados coletados, além das fontes diretas e indiretas. Isso ajuda a identificar possíveis riscos e garante transparência nas práticas de tratamento de dados.

- Deve ser apresentada uma justificativa clara do motivo pelo qual seu sistema é necessário, considerando alternativas e possíveis impactos. Essa justificativa deve estar alinhada com seus objetivos declarados e demonstrar considerações cuidadosas sobre as implicações de privacidade para

116 THE ALAN TURING INSTITUTE. Privacy impact assessment. Disponível em: https://view.officeapps.live.com/op/view.aspx?src=https%3A%2F%2Fwww.turing.ac.uk%2Fsites%2Fdefault%2Ffiles%2F2024-09%2Ftdi_privacy_impact_assessment_template.docx&wdOrigin=BROWSELINK. Acesso em: 17 out. 2024.

responder, por exemplo, quais outras soluções foram exploradas? Por que essas alternativas não foram escolhidas? Como os usuários finais se beneficiarão diretamente desse sistema? Que melhorias na experiência do usuário eles podem esperar?

- Os mecanismos de justiça e transparência em vigor para garantir o processamento seguro de dados pessoais devem ser explicados, inclusive detalhes sobre avisos de privacidade e quaisquer medidas para evitar práticas enganosas ou discriminatórias. É importante detalhar como garantir-se que os titulares dos dados sejam totalmente informados sobre as atividades de processamento de dados. Considere todos os pontos de contato em que a transparência é crucial, desde a coleta de dados até o exercício dos direitos dos titulares.

- Deve ser fornecido uma visão geral abrangente de todas as interações de terceiros envolvendo dados pessoais dentro de um sistema de identidade digital. É importante detalhar sobre a complexa rede de parcerias e provedores de serviços (em sistemas de identidade), por exemplo, serviços de verificação de identidade, provedores de armazenamento em nuvem, plataformas de análise ou órgãos governamentais. O objetivo é criar um mapa claro de onde os dados fluem, por que são compartilhados e como são protegidos ao longo de sua jornada.

Esse modelo é bastante similar ao RIPD, o que o torna uma referência relevante entre a intersecção de proteção de dados e identidade digital. Essas ferramentas são fundamentais para prestar contas do tratamento de dados pessoais, enquanto peças chave para o funcionamento de soluções de identidade em uma IPD. É por meio da elaboração de um relatório de impacto que é possível mapear os riscos a serem enfrentados pelos usuários da IPD, como indicado na tabela a seguir:

Risco	Medida de mitigação
Não observância à separação informacional e à competência dos agentes	Todo tratamento de dados deve objetivar o atendimento de uma finalidade específica por um agente competente. Nesse sentido, é a finalidade que direciona quem deve processar determinado dado pessoal, não sendo possível afirmar que um agente é competente para tratar os dados que conhece para qualquer propósito, nem que todas as entidades que formam esse agente podem tratar os dados que uma de suas partes têm acesso, como se fosse uma unidade informacional. Os dados pessoais devem ser segregados em função do propósito do seu tratamento, evitando uma concentração de informação, que levaria a uma concentração de poder. Uma forma de evitar possíveis abusos no compartilhamento de dados é pautar o fluxo de dados pela divisão de competências dos agentes que enviam e recebem dados pessoais.
Execução de tratamento de dados de forma intrusiva	O tratamento de dados deve versar apenas sobre os dados necessários para atingir uma determinada finalidade e, se houver outra forma de tratamento menos intrusiva, ela deve ser implementada. Por esse motivo, o agente responsável deve manter um registro da descrição do problema específico que a aplicação de IPD pretende resolver, bem como das oportunidades que ele busca capitalizar, das outras alternativas consideradas e do motivo pelo qual essas opções não foram escolhidas. Também é importante indicar como os usuários finais se beneficiarão diretamente desse sistema, quais melhorias na experiência do usuário eles podem esperar e como o sistema aumenta a eficiência ou a eficácia operacional da atividade que já era cumprida antes fora da IPD.
Para quem envia dados: compartilhamento inadequado.	Todo o processo de compartilhamento deve ser documentado, seja para enviar ou receber dados pessoais. Isso inclui uma descrição do nome da instituição terceira que envia ou recebe dado, o motivo do compartilhamento, os dados compartilhados e a base legal para o compartilhamento.

Para quem recebe dados: irregularidade no reuso.	Ainda, os dados só podem ser tratados para uma finalidade secundária se os seguintes critérios forem preenchidos: ☐ indicação de base jurídica apropriada para sustentar o novo tratamento; ☐ compatibilidade da finalidade secundária com a finalidade do tratamento de dados no momento da coleta dos dados, a finalidade primária; ☐ previsão de finalidade suficientemente especificada, que permita a avaliação do interesse público a ser atingido; ☐ observância dos princípios de proteção de dados e direitos dos titulares, em especial o princípio da transparência, necessidade, adequação e prestação de contas e o direito de informação e acesso.
Pessoa como objeto de identificação e não sujeito a ser identificado	Em uma lógica probabilística de identificação, vários dados são valorados como elementos com algum grau de relevância para identificar alguém, mesmo que essas informações não tenham sido informadas pela pessoa a ser identificada. A pessoa passa a exercer função passiva, ser objeto de identificação, sem saber quais informações foram usadas e formam sua identidade. Com base nessa probabilidade de ser quem diz ser ou participar de um grupo específico, a pessoa passa a ser perfilada a partir de inferências estatísticas e correlações de dados, em vez de certezas sobre a identidade ou características de uma pessoa. Essa versão digital da pessoa é suficiente para que ela possa acessar determinados bens ou serviços essenciais, mesmo que de forma limitada, colocando em risco às pessoas objeto de identificação. Dessa forma, devem ser implementados modelos de profiling seguros, trilhas de auditoria para garantir que as decisões sejam razoáveis e adequadas, além de uma contínua revisão regular de algoritmos de criação de perfil para evitar viés, e supervisão e revisão humana.
Desequilíbrio de poder na falta de informação sobre o tratamento de dados que a pessoa está submetida e na falta de mecanismos de atendimento dos direitos dos titulares	A falta de conhecimento sobre o tratamento de dados e a IPD, no geral, impede que o usuário possa se opor, questionar e saber como seu dado está sendo tratado, o que aumenta um desequilíbrio de poder entre os usuários e os agentes responsáveis pela IPD. Na falta de instrumentos para que o usuário reporte problemas com a IPD e requeira a concretização de seus direitos como titular de dados, um módulo que permita o endereçamento e responsabilização de falhas deve ser adicionado na IPD, sob pena, inclusive, de se criar um contexto de desaprovação e desconfiança no seu funcionamento.

A identificação de riscos para o usuário vai além dos riscos de segurança da informação ou acesso a informações íntimas numa lógica de sigilo[117]. Esses riscos não são objeto de um RIPD, já que este visa compreender risco aos direitos e liberdades dos titulares. É necessário maior contextualização e aprofundamento para a indicação de riscos pertinentes a um RIPD, como indicado na tabela acima.

O procedimento de elaboração do relatório de impacto é fundamental, na medida em que não apenas o resultado do processo é relevante para definir-se se o tratamento deve prosperar ou não e se as medidas são suficientes para minimizar os riscos percebidos. A forma com que esses resultados são articulados impacta na própria validade e legitimidade do relatório, que passa a observar o tratamento por meio de diversas perspectivas diferentes e complementares. Para garantir essa legitimidade, dois modelos são interessantes do ponto de vista regulatório[118]:

117 Dessa forma, o modelo de RIPD desenvolvido pela SGD apresenta uma estrutura de descrição da atividade de tratamento relevante para contextualização do tema, mas, quando exemplificando os riscos ao tratamento de dados, o modelo indica o tratamento de dados sem o consentimento do titular como um risco, bem como o compartilhamento de dados com terceiros sem o consentimento do titular e a perda ou roubo dos dados. SGD. Framework, Guias e Modelos do Programa de Privacidade e Segurança da Informação (PPSI). https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/ppsi/guia_template_ripd.docx. Acesso em: 06 fev. 2025

118 BIONI, Bruno Ricardo. Accountability no desenho (design) da regulação de dados pessoais: virtudes e vicissitudes. 2021. Tese (Doutorado em Direito Comercial) - Faculdade de Direito, Universidade de São Paulo, São Paulo, 2021. doi:10.11606/T.2.2021.tde-25102022-123810. Acesso em: 2025-01-26. p. 112.

RIPD como ferramenta de prestação de contas[119]		
Medida	Publicação do RIPD em espaço acessível aos interessados	Envolvimento das partes interessadas na elaboração do RIPD
Finalidade	Escrutínio público do juízo de valor do porquê uma atividade de tratamento de dados é considerada como sendo baixo, médio ou alto risco	Participação na definição da metodologia pela qual o gerenciamento de risco será implementado. Oportunidade dos interessados e impactados terem espaço de fala desde o ponto de partida e não apenas de chegada.
Efeito da não implementação da medida	RIPD seria instrumento de reforço de assimetria de informação entre o agente que realiza a atividade de tratamento e as pessoas sujeitas a ele.	RIPD seria um documento burocrático e tido como neutro, sem espaço para sua revisão e questionamento por parte dos interessados.
Desvantagem da implementação da medida	Os interessados poderiam apenas acessar os resultados do RIPD, sem espaço para diálogo efetivo.	Organização de espaços formais e fixos para o envolvimento de todos os interessados.

Como consequência, o processo do agente responsável pelo tratamento demonstrar que adota medidas eficazes e capazes de comprovar a observância das normas de proteção de dados não é um monólogo que em apenas esse agente tem espaço de fala. Garantir a participação significativa de pessoas e grupos afetados deve ser o pré-requisito de um processo que busca avaliar os impactos sobre os direitos humanos. A partir de mecanismos de participação, os titulares de direitos passam a ter acesso a informações e compreender melhor o projeto e os impactos resultantes, mas também que aprendam sobre seus direitos e as respectivas responsabilidades dos agentes de tratamento. Se feita com cuidado,

119 GOMES, Maria Cecília O. Para além de uma "obrigação legal": o que a metodologia de benefícios e riscos nos ensina sobre o relatório de impacto à proteção de dados. In Direito Digital: Debates Contemporâneos, orgs. LIMA, Ana Paula. HISSA, Carmina. SALDANHA, Paloma Mendes. São Paulo: Revista dos Tribunais, 2019, pp 141-153.

a participação pode ser uma forma de capacitar os titulares.[120]

O RIPD, como um instrumento de prestação de contas, deve ser construído em diálogo com os agentes impactados pela atividade de tratamento, especialmente em soluções de IPD, que, por definição, atingirão grande parte da sociedade que a utiliza, causando um tratamento de dados em larga escala.

Para a ANPD, a publicação do RIPD não é obrigatória, mas reconhece que "permitir o acesso ao público em geral pode ser uma medida que demonstra a preocupação do controlador com a segurança dos dados pessoais que estão sob sua responsabilidade e seu compromisso com a privacidade dos titulares, além de atender aos princípios do livre acesso, da transparência e da responsabilização e prestação de contas"[121]. A publicação do RIPD é uma forma de atendimento dos fundamentos da LGPD por tornar evidente os agentes responsáveis pelo tratamento, sejam eles pessoas de direito público ou privado, bem como os riscos identificados e as medidas de mitigação implementadas para endereçar esses riscos, abrindo espaço para que as pessoas afetadas conheçam de antemão os parâmetros mapeados pelo responsável.

Ao mesmo tempo, em relação às entidades públicas, a autoridade prevê que "RIPD deverá ser publicado: (i) por determinação da ANPD, nos termos do art. 32 da LGPD; ou (ii) pelo próprio controlador, quando não identificada hipótese de sigilo aplicável ao caso, em conformidade com a Lei nº 12.527, de 18 de novembro de 2011"[122], a Lei de Acesso à Informação (LAI). A LAI visa garantir a publicidade das informações tratadas pelo Poder Público, incidindo também sobre as entidades privadas sem fins lucrativos que recebam, para realização de ações de interesse público, recursos públicos diretamente do orçamento ou mediante subvenções sociais, contrato de gestão, termo de parceria, convênios, acordo, ajustes ou outros instrumentos congêneres. Com consequência, quando não houver hipótese

120 THE DANISH INSTITUTE FOR HUMAN RIGHTS. Crosscutting: Stakeholder engagement human rights impact assessment guidance and toolbox. 2020. Disponível em: https://www.humanrights.dk/files/media/document/HRIA%20Toolbox_Stakeholder%20Engagement_ENG_2020.pdf. Acesso em: 17 jan. 2025.

121 ANPD. Relatório de Impacto à Proteção de Dados Pessoais (RIPD). 2023. Disponível em: https://www.gov.br/anpd/pt-br/canais_atendimento/agente-de-tratamento/relatorio-de-impacto-a-protecao-de-dados-pessoais-ripd. Acesso em: 17 jan. 2025.

122 ANPD. Relatório de Impacto à Proteção de Dados Pessoais (RIPD). 2023. Disponível em: https://www.gov.br/anpd/pt-br/canais_atendimento/agente-de-tratamento/relatorio-de-impacto-a-protecao-de-dados-pessoais-ripd. Acesso em: 17 jan. 2025.

de sigilo que se aplique à publicação do RIPD, a entidade privada que se submete à LAI também deverá publicar o relatório.

A prestação de contas serve como um mecanismo de controle e aprimoramento contínuo da IPD. Ao exigir que os agentes de tratamento comprovem a conformidade com os princípios de proteção de dados e os direitos dos titulares, garante-se que o interesse público seja efetivamente atendido. Ainda, a noção de prestação de contas assegura também que o uso de dados pessoais em IPD seja transparente e justificável perante a sociedade. Isso é crucial para manter a confiança pública nas instituições e nos serviços digitais oferecidos.

4.2.2. Prestação de contas por meio para procedimentos de participação

A definição e a promoção do valor público em uma IPD pressupõe um processo inclusivo e participativo. Como argumentado neste relatório, a IPD deve estar orientada para o atendimento do interesse não apenas de agentes privados, mas para o bem comum da sociedade que a utiliza. Esse bem comum, esse valor público, não deve ser percebido como um conceito abstrato definido por especialistas ou gestores públicos, mas como uma **construção coletiva que emerge da interação** entre diferentes setores e grupos sociais. Compreender o valor público significa reconhecer a diversidade de perspectivas, necessidades e aspirações dos grupos que compõem uma comunidade.

Promover o valor público é pressuposto para qualquer IPD, quando apresentado nas seções anteriores. Nesse sentido, a participação efetiva da sociedade no desenvolvimento de infraestruturas digitais é fundamental para garantir que as soluções tecnológicas respondam genuinamente aos anseios coletivos. Ao possibilitar espaços de co-criação, as comunidades podem influenciar ativamente no desenho, implementação e monitoramento dessas infraestruturas. Como consequência, essa abordagem colaborativa permite criar ferramentas que não apenas resolvem problemas imediatos, mas promovem transformação social, inovação e crescimento inclusivo.

Sabendo que uma IPD e suas aplicações devem atender o interesse público, as práticas de participação social passam a ser **ferramentas** para garantir que os interesses e demandas da sociedade estão sendo endereçados, seja antes, du-

rante ou após a implementação de uma IPD.

O bem comum emerge justamente dessa construção coletiva, onde diferentes setores dialogam para definir prioridades e estratégias para a IPD. As infraestruturas públicas digitais passam então a ser compreendidas não como instrumentos neutros, mas como espaços vivos de transformação social, cujo valor se materializa na capacidade de responder às necessidades específicas de cada comunidade. Assim, o valor público se constitui como um **processo dinâmico** de aprendizado e colaboração permanente.

A participação cívica assegura que essa infraestrutura seja desenvolvida de acordo com as expectativas da população. Por meio do envolvimento da comunidade, é possível priorizar serviços digitais que são mais urgentes ou relevantes para o cotidiano das pessoas. Além disso, diferentes regiões ou grupos sociais podem ter necessidades específicas que precisam ser consideradas na implementação da IPD, promovendo uma abordagem mais inclusiva e adaptada ao contexto local.

A participação cidadã não é apenas um requisito democrático, mas também um requisito fundamental para a **eficiência** das políticas digitais[123]. Quando adotada em todo o ciclo de vida dessas políticas, uma governança participativa pode reduzir os riscos criados pelo sistema, acelerar a inovação com soluções criativas para demandas concretas e aumentar a aceitação e uso contínuo das aplicações de IPD.

A participação é uma das ferramentas chave para identificar lacunas e potenciais riscos antes que eles se tornem problemas reais. Cidadãos de diferentes origens e experiências, além de representantes de outros setores e interesses, podem oferecer perspectivas diversas, apontando desafios que os desenvolvedores e gestores públicos podem não ter previsto.

Essa interação com outros agentes para mapear lacunas da IPD pode resultar em benefícios inclusive econômicos, diante da **minimização de casos de retraba-**

123 LUCIANO, Maria. Digital Public Services for Whom? Participation and Care as Prerequisites for Efficiency. 2024. Disponível em: https://www.techpolicy.press/digital-public-services-for-whom-participation-and-care-as-prerequisites-for-efficiency/. Acesso em: 25 jan. 2025.

lho[124]. Em um cenário sem participação de diversos agentes na IPD, após o desenvolvimento da aplicação, é provável que ela tivesse de ser revista por conta de uma falha ou coluna facilmente percebida por outros atores em momento anterior.

Dessa forma, para que haja participação na construção do valor público, é fundamental a consolidação de **mecanismos formais** que permitam essa participação plural. Não basta criar canais de consulta eventuais e simbólicos, é necessário instituir processos de deliberação, nos quais diferentes grupos possam compartilhar suas perspectivas, contribuir com conhecimentos e participar das decisões. A formalização desses momentos de participação são essenciais para garantir paridade e previsibilidade na interação dos setores, garantindo que todos possam efetivamente influir no processo de tomada de decisão da IPD.

Um dos mecanismos formais de participação utilizados pelo Poder Público são as **consultas públicas** em que os grupos interessados se inscrevem para debater uma versão preliminar da norma. Com a alteração da Lei de Introdução das Normas do Direito brasileiro pela Lei 13.655[125], a consulta pública ganhou destaque como uma das etapas a serem implementadas pelos órgãos públicos durante a edição de atos normativos. O art. 29 dessa Lei dispõe que "em qualquer órgão ou Poder, a edição de atos normativos por autoridade administrativa, salvo os de mera organização interna, poderá ser precedida de consulta pública para manifestação de interessados, preferencialmente por meio eletrônico, a qual será considerada na decisão".

O objetivo é garantir oportunidade para que os interessados se manifestem e que seus apontamentos sejam considerados na decisão final do órgão. Para tanto, é fundamental a disponibilização de informações e relatórios que embasaram a consulta, de forma que a participação seja informada, e que hajam respostas às "contribuições enviadas, motivando a incorporação ou não das sugestões na versão final do ato [...] e publicizando suas razões referentes ao conteúdo final"[126].

---

124 TENNISON, Jeni. Mechanisms for Governance Cooperation Why We Need Inclusive Data Governance in the Age of AI. 2024. Disponível em: https://www.cigionline.org/articles/why-we-need-inclusive-data-governance-in-the-age-of-ai/. Acesso em: 2 dez. 2024.

125 BRASIL. Lei nº 13.655, de 25 de abril de 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13655.htm

126 LIMA, Gabriel; GASPAR, Luciana. As Consultas Públicas Enquanto Mecanismo de Legitimação dos Atos Administrativos. Revista Opinião Jurídica, v. 20, n. 34, p. 1-29, 2022. Disponível em: https://www.redalyc.org/journal/6338/633875004001/html/. Acesso em: 2 dez. 2024.

Essa audiência pode ser conduzida em qualquer momento da construção da norma, seja antes ou até mesmo após a publicação, tendo em vista os desafios e particularidades que surgem na implantação da norma.

A participação da sociedade também tem o potencial de garantir maior legitimidade para a IPD a partir da audiência das pessoas interessadas. Enquanto uma medida necessária para a condução de processos relacionados à IPD, a consulta não seria apenas uma ferramenta retórica, ela permitiria que as pessoas passassem a efetivamente influenciar no processo de tomada de decisão. Essa dinâmica colaborativa permite que as tecnologias sejam verdadeiramente centradas nas pessoas, refletindo a diversidade e a complexidade social.

Em atenção ao elemento de participação na IPD, o art. 16, do Decreto nº 12.069/2024, determina que a Secretaria de Governo Digital deve promover o desenvolvimento, a implementação e o uso da IPD, em articulação com outros agentes, inclusive externos ao Poder Público, como representantes da sociedade, do setor acadêmico e do setor privado. O próprio governo federal reconhece que a IPD e suas aplicações devem ser construídas em **diálogo** com diversos agentes para além do Poder Público.

Além das consultas públicas, esse diálogo pode ser construído pela formação de comitês multissetoriais instituídos com o objetivo de fixar normas e diretrizes para a IPD. A previsão de comitês como espaço deliberativo sobre as atividades desenvolvidas pelo Poder Público que afetam a sociedade é comum e uma das formas de se garantir abertura e participação nas atividades públicas. Como exemplo, a Lei 13.444/2017, que dispõe sobre a Identificação Civil Nacional (ICN), instituiu o Comitê Gestor do programa, o Decreto 10.046/2019 criou o Comitê Central de Governança de Dados (CCGD), já a LGPD previu o Conselho Nacional de Proteção de Dados Pessoais e da Privacidade (CNPD), composto por representantes de diversos setores como esse espaço de oxigenação de outras áreas no debate público.

Vale notar que não é qualquer tipo de conselho que atende aos princípios e valores democráticos de participação. O STF, no julgamento da **ADI 6649**, processo já discutido neste relatório, declarou inconstitucional a composição do CCGD prevista no artigo 22 do Decreto 10.046/2019. O tribunal considerou que os critérios para escolha dos membros do comitê eram contrários à constituição, pois

incluíam apenas representantes da administração pública federal, sem **abertura democrática** adequada.

No contexto do art. 21 do Decreto, o CCGD era responsável por deliberar sobre regras para o compartilhamento de dados, orientações e diretrizes para integração dos órgãos, além da instituição de outros cadastros base de referência do setor público. Na estrutura original, esse Comitê seria composto apenas por representantes do Poder Público, sem qualquer participação de outros setores.

Diante das competências e da composição do Comitê, o relator da ADI argumentou que o Comitê "não apenas oferece proteção deficiente para valores centrais da ordem constitucional, como também constitui fator de desestabilização das garantias previstas na Lei 13.709/2018". Isso porque há "certo consenso acerca da necessidade de criação de autoridades administrativas independentes, destacadas especificamente para fiscalização e controle de atividades potencialmente lesivas ao direito de privacidade"[127].

Na contramão desse consenso, o Comitê seria "instituição com **perfil insular, hostil a qualquer proposta de abertura democrática e de pluralização do debate** e, nessa medida, fechada à participação de representantes oriundos de outras instituições republicanas e de entidades da sociedade civil"[128]. Por isso, o Comitê foi declarado inconstitucional.

Dessa forma, é fundamental prever espaços de debate e participação em temas relacionados à afetação do direito fundamental de proteção de dados, esses espaços devem ser independentes, abertos e plurais. O tribunal é explícito em reconhecer que a "tutela efetiva do direito à privacidade depende da correta calibragem do perfil institucional dos órgãos responsáveis pela regulamentação, controle e monitoramento de atividades de tratamento de dados pessoais"[129].

Nesse sentido, vale destacar que, para a garantia de um direito fundamental à

---

127 SUPREMO TRIBUNAL FEDERAL. Ação Direta de Inconstitucionalidade 6.649 Distrito Federal. p. 57. Disponível em: https://portal.stf.jus.br/processos/downloadPeca.asp?id=15358978491&ext=.pdf. Acesso em: 2 dez. 2024

128 SUPREMO TRIBUNAL FEDERAL. Ação Direta de Inconstitucionalidade 6.649 Distrito Federal. p. 61. Disponível em: https://portal.stf.jus.br/processos/downloadPeca.asp?id=15358978491&ext=.pdf. Acesso em: 2 dez. 2024.

129 SUPREMO TRIBUNAL FEDERAL. Ação Direta de Inconstitucionalidade 6.649 Distrito Federal. p. 60. Disponível em: https://portal.stf.jus.br/processos/downloadPeca.asp?id=15358978491&ext=.pdf. Acesso em: 2 dez. 2024.

proteção de dados pessoais, há de se "considerar a íntima vinculação entre direitos fundamentais, organização e procedimento, no sentido de que os direitos fundamentais são, ao mesmo tempo e de certa forma, dependentes da organização e do procedimento [...], mas simultaneamente também atuam sobre o direito procedimental e as estruturas organizacionais"[130]. A previsão de conselhos deliberativos sobre atividades de tratamento de dados é fundamental para a **preservação do direito fundamental à proteção de dados**, além disso esses espaços devem ser independentes, participativos e plurais.

Tendo em vista a decisão do STF na ADI 6649, atualmente o CCGD é composto por diversos órgãos dos três poderes, como a Casa Civil, CGU, MJ, Bacen, CNJ, Senado e Câmara dos Deputados, além de dois membros da sociedade civil[131]. Em 2020, o CCGD instituiu o Subcomitê Técnico de Governança de Dados com competência para propor orientações para estruturação da Governança de Dados dos órgãos e entidades da administração pública federal direta, autárquica e fundacional e os demais Poderes da União[132]. Essa atribuição impacta diretamente como possíveis arquiteturas de IPD podem ser estruturadas no sentido de promover ou restringir o fluxo de dados, inclusive pessoais.

As atribuições do CCGD são próximas às questões de governança e fluxo de dados, inclusive pessoais. Porém, é possível argumentar que a sua composição não é representativa o suficiente para endereçar os interesses dos grupos afetados por uma IPD, já que é majoritariamente composto por órgãos do Poder Executivo, com oito membros, além de dois membros da sociedade civil e quatro membros convidados dos outros poderes. Sabendo que o valor público emerge da interação dos grupos interessados, para além de gestores públicos, devem fazer parte desses conselhos os operadores da infraestrutura, destinatários das suas funcionalidades, e instituições e grupos afetados pela IPD.

---

130 INGO SARLET. Proteção de dados pessoais e deveres de proteção estatais. Consultor Jurídico. Disponível em: https://www.conjur.com.br/2021-ago-27/direitos-fundamentais-protecao-dados-pessoais-deveres-protecao-estatais/. Acesso em: 2 dez. 2024.

131 MGI. Comitê Central de Governança de Dados (CCGD). 2020. Disponível em: https://www.gov.br/governodigital/pt-br/infraestrutura-nacional-de-dados/governancadedados/comite-central-de-governanca-de-dados. Acesso em: 2 dez. 2024.

132 MGI. Cartilha de Governança de Dados. Disponível em: https://www.gov.br/governodigital/pt-br/infraestrutura-nacional-de-dados/governancadedados/arquivos/CartilhadeGovernancadeDadosEcossistemadeDados.pdf. Acesso em: 2 dez. 2024

No contexto da infraestrutura pública, seja pela reforma do CCGD ou não, esse conselho poderia ser composto por agentes de diversos setores, no mínimo do setor público, das três esferas de poder, setor privado, terceiro setor, e da comunidade acadêmica, e poderia atuar inclusive na avaliação e resolução de problemas relacionados à IPD[133], promovendo transparência e responsabilidade entre os agentes, e protegendo os direitos e interesses dos usuários.

Para ser efetivo, o conselho deve ter autoridade para analisar reclamações e fazer recomendações, operando com independência em relação ao governo e aos provedores de tecnologia. É importante que haja independência na forma de decisão do órgão, a fim de que ele não seja subordinado a outras estruturas que podem ter interesses próprios não vinculados ao objeto da IPD. Assim, o conselho seria competente para:

- Propor diretrizes estratégicas e fornecer subsídios para o desenvolvimento de uma IPD;
- Elaborar estudos e realizar debates e audiências públicas sobre a IPD;
- Supervisionar as mudanças e o atendimento de feedbacks dos usuários da IPD; e
- Sugerir ações a serem adotadas pelos agentes que compõem a IPD.

Nota-se que essas competências são mais amplas que a do CCGD, a qual se limita a deliberar sobre o compartilhamento de dados entre órgãos da administração pública federal no contexto do Cadastro Base do Cidadão[134]. Ainda, a implementação de medidas de transparência ativa em suas ações e decisões também poderia fortalecer a confiança pública no conselho.

A participação confere maior **legitimidade** à IPD, pois ela é vista como um produto do esforço coletivo e não apenas uma imposição governamental. A diversidade de perspectivas trazida pelos participantes pode levar a soluções inovadoras

133 Essa é a composição mínima de conselhos como o CGI.br e o CNPD. Disponível em: https://cgi.br/membros/ e https://www.gov.br/anpd/pt-br/cnpd-2/composicao-cnpd/estrutura-cnpd-1.

134 PRESIDÊNCIA DA REPÚBLICA. Decreto n 10.046, de 9 de outubro de 2019. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/decreto/d10046.htm. Acesso em: 2 dez. 2024.

e criativas para desafios complexos enfrentados pela sociedade. Ademais, uma IPD desenvolvida com ampla participação tem mais chances de ser sustentável a longo prazo, pois conta com o apoio e a compreensão da população.

Os benefícios da participação estão ancorados em melhorias tangíveis na IPD que as percebem em suas vidas diárias. Seja por meio de serviços aprimorados, do desenvolvimento de infraestrutura específicas ou da simplificação de processos, o engajamento participativo e os esforços de colaboração são chave para o êxito de uma IPD[135]. Assim, para além das práticas de prevenção de dados, os procedimentos de participação também funcionariam como uma das formas de prestação de contas da IPD para a sociedade, garantindo a promoção do bem comum.

Entender a prestação de contas como uma ferramenta de concretização do interesse público também implica em estabelecer um espaço institucional para proposição e deliberação pública. Seja por meio de consultas públicas ou pela instituição de conselhos específicos, ferramentas de participação devem ser implementadas para assegurar um **processo normativo e regulatório colaborativo**[136].

Assim, a partir de uma perspectiva formal, plural e robusta, é possível estabelecer diretrizes para que a IPD aponte para o bem comum. Uma estrutura de governança adequada incentiva o uso de tecnologia que permita a colaboração entre os agentes interessados, ou mesmo a co-criação. Isso inclui a promoção da inovação em conformidade com as diretrizes estabelecidas, a adoção da interoperabilidade e a estruturação de ferramentas que facilitem a governança participativa com base em um entendimento plural e voltado para o interesse público.

---

135 ODI RESEARCH. What makes participatory data initiatives successful? [s.l.: s.n.], 2024. p. 9. Disponível em: https://theodi.cdn.ngo/media/documents/What_makes_participatory_data_initiatives_successful_.pdf. Acesso em: 2 dez. 2024.

136 BIONI, Bruno Ricardo. Accountability no desenho (design) da regulação de dados pessoais: virtudes e vicissitudes. 2021. Tese (Doutorado em Direito Comercial) - Faculdade de Direito, Universidade de São Paulo, São Paulo, 2021. doi:10.11606/T.2.2021.tde-25102022-123810. Acesso em: 2025-01-26. p. 129

05.
CONSIDERAÇÕES FINAIS

5 Considerações finais

Os desafios e riscos de implementar sistemas de identidade digital enquanto uma ferramenta na IPD estão sendo mapeados e compreendidos com o próprio desenvolvimento das soluções na IPD. É nesse sentido que este relatório se debruça sobre a **intersecção entre identidade, IPD e proteção de dados**, justamente para identificar possíveis tensões e espaços de aprimoramento. Com base nas conexões entre identidade digital, IPD, e a gramática constitucional brasileira de proteção de dados, o relatório propõe medidas de governança para garantir um fluxo justo de informações.

Para tanto, a pesquisa utiliza entrevistas com especialistas, análise bibliográfica e de jurisprudência e discussão em eventos para compreender os temas de tensão e, com isso, traçar recomendações, que incluem a promoção da participação cidadã, transparência, e a adoção de estruturas robustas para a gestão de IPD e soluções de identidade. O relatório enfatiza a necessidade de conciliar inovação tecnológica com a proteção dos direitos fundamentais diante de obrigações de **governança para promoção do valor público e prestação de contas** no tratamento desses dados.

Inicialmente, o relatório explora os conceitos chave dos temas de IPD e identidade digital com objetivo de mapear as variáveis presentes nesse contexto, já que a IPD fornece a base para o funcionamento dos sistemas de identidade digital. A IPD é a infraestrutura necessária para o funcionamento de sistemas e serviços essenciais no meio digital, visando promover o bem comum e atender a um valor público. Por isso, ela deve ter elementos de **participação, interoperabilidade e proteção de dados para permitir a construção de novas aplicações a partir de um alicerce comum que vise o atendimento do interesse público**. A identidade, como uma das aplicações dessa IPD, deve observar esses elementos fundantes.

Diante da extensividade da identidade como IPD, os riscos à direitos fundamentais devem ser percebidos. No que tange ao direito à proteção de dados, o relatório aborda a assimetria de poder entre Estado e cidadão, intensificada pela digitalização, e a resposta da LGPD na busca por um novo equilíbrio. O julgamento da ADI nº 6387 pelo STF, que reconheceu a **proteção de dados como direito autônomo**, afirma justamente a tutela jurídica de todos os dados pessoais, independentemente de sua natureza. Nesse sentido, o desenvolvimento de IPD e

soluções de identidade se enquadra nesse novo paradigma, devendo observar o direito constitucional à proteção de dados.

Os conceitos de autodeterminação informativa e o livre desenvolvimento da personalidade ganham relevância neste novo contexto de tutela dos dados pessoais. A autodeterminação vai além do consentimento, devendo garantir a autonomia do indivíduo na definição de seus interesses e necessidades em relação aos seus dados. Com base nesses conceitos, a identidade digital, construída a partir de dados que fluem na infraestrutura digital, pode ser um instrumento de **distribuição de poder** na medida em que o seu desenvolvimento assegura a autodeterminação informativa.

Teorias como a da privacidade como integridade contextual são relevantes justamente para traçar barreiras e diretrizes para que o tratamento de dados esteja de acordo com as expectativas do titular. De acordo com essa teoria, a privacidade estaria preservada na medida em que o **fluxo de dados respeitasse normas contextuais**. Segundo Nissenbaum, cinco elementos definem essas normas: esferas sociais do titular, remetente e destinatário, tipo de informação e restrições à transmissão. Ainda, para identificar se o fluxo de dados está adequado ou não, deve-se considerar os interesses das partes, valores políticos e éticos, além dos propósitos e valores contextuais. Assim, no contexto de IPD, o compartilhamento de dados, incluindo dados de identidade, poderia ocorrer se observar o contexto da relação entre os agentes envolvidos.

Além disso, do ponto de vista da **separação informacional de poderes**, no contexto do constitucionalismo digital, o Estado não deve ser uma unidade informacional. Isso significa que o compartilhamento de dados entre órgãos e entidades públicas deve respeitar suas competências para tratar dados específicos de titulares específicos. Nesse sentido, as decisões da ADI nº 6529/DF, ADPF nº 692/DF e MS nº 36.150/DF consolidaram o entendimento de que o **compartilhamento de dados deve ser motivado, atender ao interesse público, respeitar a reserva de jurisdição e observar os princípios da LGPD**.

A gramática constitucional brasileira de proteção de dados desempenha um papel fundamental no desenvolvimento de aplicações de identidade na IPD. Portanto, é imprescindível que estes parâmetros, já consolidados na jurisprudência brasileira, sejam levados em consideração para nortear o desenvolvi-

mento dessa infraestrutura.

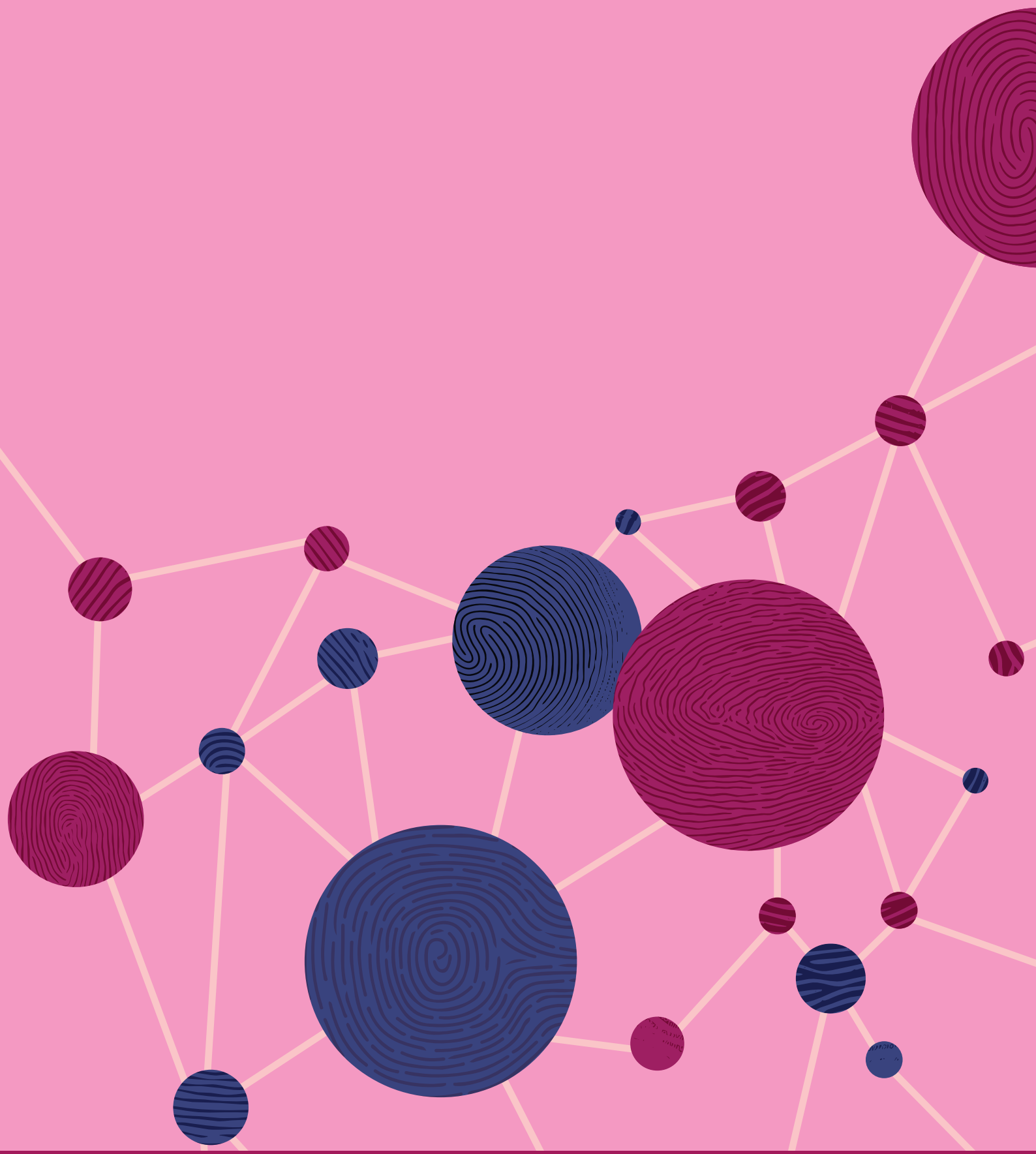
A preservação do bem comum na IPD está intrinsecamente ligada à garantia do direito fundamental à proteção de dados pessoais. O valor público não se resume à geração de valor econômico a partir dos dados, mas exige uma distribuição justa e equitativa dos benefícios, com respeito aos direitos individuais. Como consequência, o foco objeto de proteção não é apenas o sigilo, mas a circulação segura e adequada dos dados pessoais. Essa proteção de dados, conforme estabelecido pelo STF, também promove o interesse público, e as obrigações legais da LGPD instrumentalizam essa promoção com segurança jurídica.

Para a garantia dessas proteção, é essencial definir núcleos de responsabilidade e mecanismos de prestação de contas. Os usuários devem ter mecanismos de reparação por danos sofridos, com clareza sobre as responsabilidades de cada agente. A confiança na infraestrutura depende da definição robusta dos níveis de responsabilidade. Por isso, o fluxo informacional deve ser mapeado e alinhado com os parâmetros de proteção de dados para garantir o interesse público e observância aos demais parâmetros de proteção de dados.

A lógica regulatória da proteção de dados também implica na implementação de obrigações de prestação de contas por um racional preventivo, com o objetivo de proteger os titulares de dados antes que danos ocorram, em vez de apenas aplicar sanções a posteriori. Os agentes envolvidos na IPD devem demonstrar responsabilidade, prestando contas sobre as medidas implementadas para mitigar danos potenciais e assegurar o cumprimento das normas de proteção de dados. Essa responsabilidade é impulsionada pela maior liberdade que esses agentes possuem ao construir soluções digitais dentro da IPD. Assim, a elaboração do RIPD, bem como a implementação de práticas de participação e o escrutínio público são incentivados como forma de equilibrar a liberdade e a discricionariedade dos agentes responsáveis pelo tratamento de dados pessoais.

Para que sistemas de identidade sejam considerados aplicações na IPD, é imprescindível que eles maximizem o bem público e sejam sistemas governáveis, participativos e que permitam o aprimoramento a partir da responsabilidade dos agentes envolvidos. Em um contexto de identidade em camadas, processos transparentes, responsáveis, coletivos são fundamentais para que uma identidade seja ferramenta de acesso à infraestrutura e suas aplicações.

Em conclusão, destaca-se a importância de uma abordagem proativa à proteção de dados no desenvolvimento da IPD e da identidade digital, utilizando a gramática constitucional brasileira como base. Em acordo inclusive com os julgados do STF, tem-se que **os conceitos de proteção de dados e interesse público não são antagônicos, pelo contrário, eles devem ser balanceados, tendo em vista que o interesse público se concretiza na efetiva garantia à proteção de dados pessoais.** Nesse sentido, a identificação do interesse comum, as ferramentas de prestação de contas e participação social de diversos agentes são cruciais para garantir um fluxo informacional justo, proteger os direitos fundamentais e promover o valor público.



REALIZAÇÃO:

DataPrivacyBR Research

APOIO:

ripple