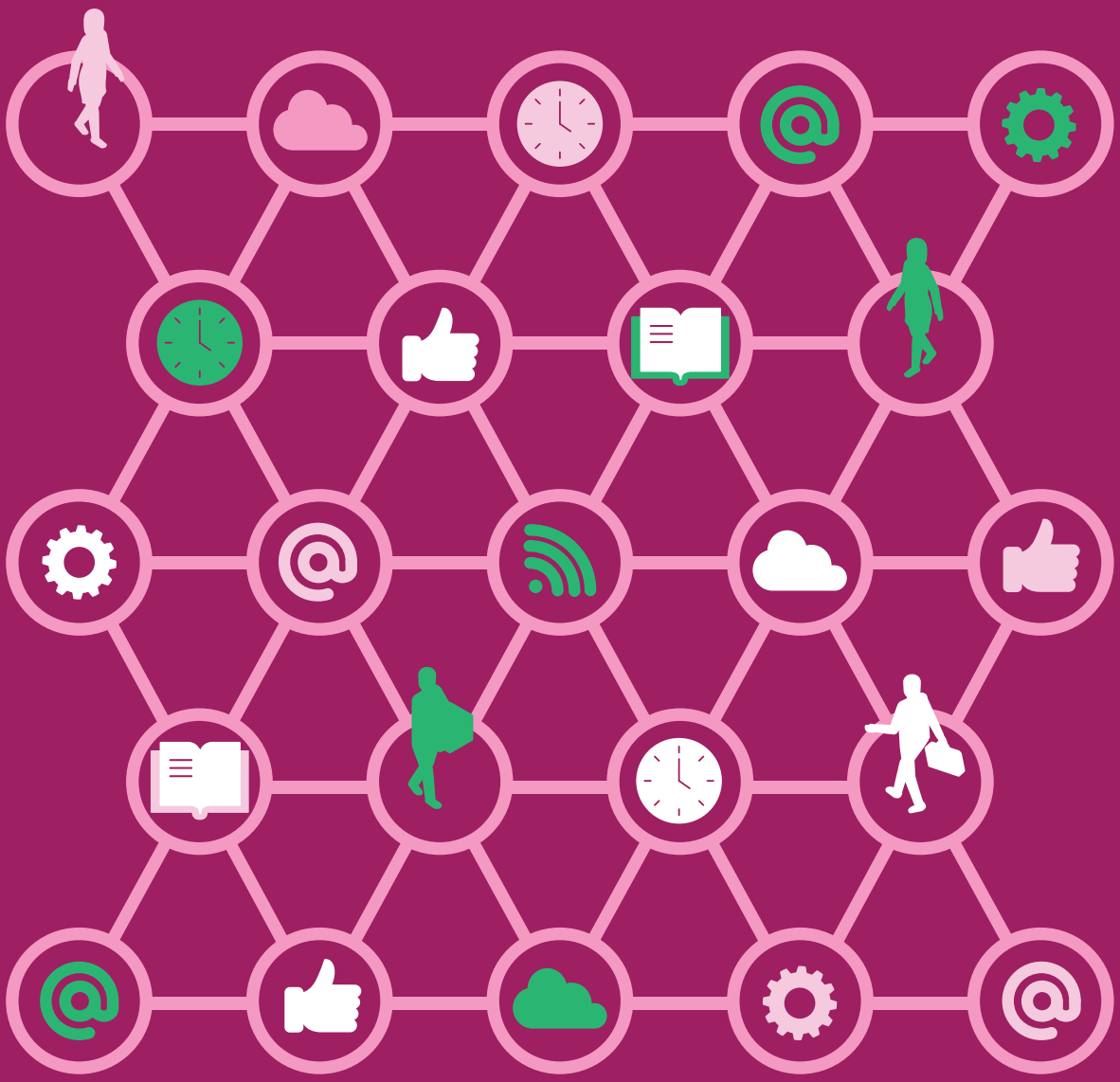


A INFRAESTRUTURA DA IDENTIDADE: OS INFLUXOS DE UMA IDENTIDADE DIGITAL COMO APLICAÇÃO DA IPD

Eduarda Costa Almeida
Pedro Bastos Lobo Martins

DataPrivacyBR Research

APOIO
ripple

Ficha técnica

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.

DIREÇÃO

Bruno Bioni, Mariana Rielli e Rafael Zanatta

COORDENAÇÃO

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

EQUIPE

Alicia Lobato, Eduarda Costa, Eduardo Mendonça, Gabriela Vergili, Horrara Moreira, Isabela Gomes, Isabelle Santos, Johanna Monagreda, João Paulo Vicente, Júlia Mendonça, Louise Karczeski, Matheus Arcanjo, Mekebib Assefa, Nathan Paschoalini, Otávio Almeida, Pedro Henrique, Rafael Guimarães, Rafael Regatieri, Roberto Junior, 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. A Infraestrutura da identidade: os influxos de uma identidade digital como aplicação da IPD. São Paulo: Associação Data Privacy Brasil de Pesquisa, 2024.

Sumário Executivo

Existe uma necessidade crescente do desenvolvimento de uma infraestrutura pública digital (IPD) para promover acesso a direitos e serviços essenciais para as pessoas, à semelhança da infraestrutura física. Há um esforço relevante dos debates internacionais para se delinear contornos a uma IPD, bem como seu conceito e suas aplicações. Para além disso, é fundamental perceber que os elementos de tecnologia aberta e interoperável, com governança robusta e participação multissetorial, são essenciais para garantir a confiança, transparência e responsabilidade da infraestrutura, bem como promover a inclusão e a inovação.

Embora a definição de IPD ainda esteja em evolução, é importante reconhecer que as aplicações dessa infraestrutura devem **servir ao bem comum e maximizar o valor público**. O elemento do valor público se soma a outros essenciais para caracterizar uma aplicação como IPD. As aplicações de IPD se constituem como tais em um processo de constante atualização, e não apenas a partir de uma classificação estanque a qual entende a aplicação como parte ou não de um ecossistema de IPD.

Um desses outros elementos estruturais da IPD é a **participação ativa de diferentes setores da sociedade na construção e governança da IPD**. Essa participação é fundamental para impulsionar a inovação e criar soluções centradas nas pessoas, especialmente em aplicações como a de identidade. No entanto, essa participação multissetorial, para ser efetiva, exige a fixação de critérios formais e materiais em que a sociedade passa a influenciar no desenvolvimento das aplicações de IPD, sua implementação e acompanhamento.

Uma das principais materializações de IPD são as aplicações de identidade. Isso porque uma infraestrutura digital só funciona e ganha relevância prática quando, por meio dela, passa a ser possível identificar o beneficiário das aplicações de maneira segura e conveniente. Com a digitalização da infraestrutura, processos de validação de identidade se tornam essenciais para que as pessoas possam **acessar** direitos, bens e serviços públicos ou privados.

Nesse sentido, a identidade digital funciona como um conjunto de atributos eletrônicos únicos que exercem algumas funções, como a de garantir a confiabilidade da credencial de uma pessoa, com o potencial de simplificar esse processo de identificação. Em geral, esses sistemas devem cumprir funções básicas de identificação, autenticação e autorização, formando um ciclo essencial para garantir sua utilidade.

Para além das funções tradicionais, esses sistemas podem envolver **poucos ou diversos atores** com funções específicas, como provedores de identidade, operadores de sistemas e entidades de confiança. Esses agentes podem organizar os sistemas de identidade em estruturas **centralizadas**, **federadas** e **descentralizadas**, o que influencia a gestão desses sistemas. Ainda, os sistemas de identidade podem ter finalidades **fundacionais**, buscando prover uma **identidade universal reconhecida legalmente**, ou funcionais, emitindo credenciais para autorizar **acessos específicos, ou mesmo outras finalidades a depender do contexto** em que a identidade é validada.

Com a complexificação dos sistemas de identidade e a combinação dessas molduras, modelos de identidade baseados em **camadas** ganham espaço como aplicações de IPD. Esses modelos são resultados da integração de múltiplos sistemas digitais formados por diferentes fontes e contextos, que tensionam a **finalidade** da coleta dos dados com a compatibilidade dos usos posteriores.

Sistemas de identidade em uma IPD apresentam **riscos** específicos para a autonomia e o desenvolvimento da personalidade das pessoas que vão além da soma dos riscos de um sistema de identidade e da sua digitalização isoladamente considerados. O monitoramento constante e não informado do comportamento e dos atributos das pessoas pode restringir a autonomia e livre desenvolvimento dos identificados.

Assim, o compartilhamento de informações de identificação de contextos diferentes pode levar a graves afetações de direitos à privacidade e proteção de dados, diante da falta de **separação informacional** entre os agentes envolvidos. Além disso, é possível que os riscos gerados em um contexto de identificação (por exemplo, na detecção de fraudes) passem a se manifestar em outros contextos (por exemplo, na candidatura para um emprego), diante do fluxo de dados.

Em vista desses riscos, os sistemas de identidade devem:

- Implementar a proteção de dados como princípio fundamental, exigindo a adoção de abordagens de transparência, especificação de propósito e finalidade e regras de compartilhamento de dados, buscando sempre a minimização desse compartilhamento;
- Buscar abordagens que priorizem o poder de agência das pessoas, garantindo sempre o direito à explicação e revisão de decisões tomadas a seu respeito;

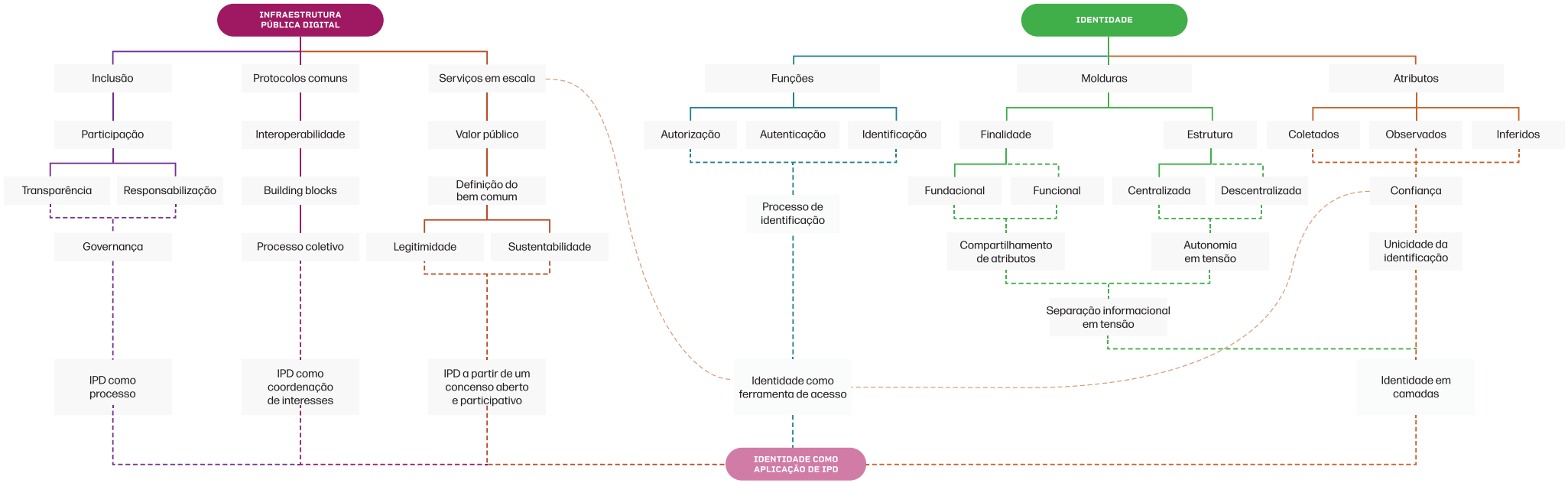
- Prevenir a agregação de dados em uma única base centralizada ou a retenção de dados desnecessários, limitando a coleta e o uso de dados pessoais para proteger as pessoas contra o uso indevido de dados;
- Introduzir arranjos robustos para garantir que o compartilhamento de atributos e credenciais ocorra de maneira segura e rastreável, além de que os dados sejam precisos, completos, mantidos atualizados e relevantes;
- Garantir ferramentas de prestação de contas dos agentes envolvidos no desenvolvimento dos sistemas, para que eles se responsabilizem pelas práticas, especialmente as que impactam grupos vulnerabilizados;
- Possuir sistemas de governança participativa desde a concepção, garantindo a participação efetiva dos diversos atores interessados, especialmente a sociedade civil e grupos vulnerabilizados que podem ser afetados por sistemas de identidade digital.

A integração de camadas de identidade visa aumentar a **confiança** nos sistemas, mas a falta de governança pode resultar em violações de direitos. Por isso, sua implementação requer abordagens cuidadosas para garantir segurança, confiabilidade e inclusão. 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.

Portanto, para que sistemas de identidade sejam considerados aplicações de IPD, é imprescindível que eles 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 e de maximização do, valor público são fundamentais para que uma identidade seja ferramenta de acesso à infraestrutura e suas aplicações.

O seguinte mapa mental consolida os pressupostos, vínculos e nuances desse ecossistema de identidade na IPD:

MAPA MENTAL


INFRAESTRUTURA PÚBLICA DIGITAL
Inclusão
Protocolos comuns
Serviços em escala
Participação
Interoperabilidade
Valor público
Transparência
Responsabilização
Building blocks
Definição do bem comum
Governança
Processo coletivo
Legitimidade
Sustentabilidade
IPD como processo
IPD como coordenação de interesses
IPD a partir de um concenso aberto e participativo
IDENTIDADE
Funções
Molduras
Atributos
Autorização
Autenticação
Identificação
Finalidade
Estrutura
Coletados
Observados
Inferidos
Fundacional
Funcional
Centralizada
Descentralizada
Confiança
Processo de identificação
Compartilhamento de atributos
Autonomia em tensão
Unicidade da identificação
Separação informacional em tensão
Identidade como ferramenta de acesso
Identidade em camadas
IDENTIDADE COMO APLICAÇÃO DE IPD

Sumário

Sobre a cartilha

Qual a finalidade dessa cartilha?

Essa cartilha foi desenhada como um recurso para os agentes que atuam no ecossistema de identidade reconhecerem os fundamentos, as aplicações e as funcionalidades de uma identidade digital no contexto de Infraestrutura Pública Digital (IPD). A cartilha organiza um mosaico difuso sobre o papel da identidade em uma IPD a partir de exemplos para, assim, lançar luz aos principais pontos-chave para que essa aplicação da infraestrutura promova direitos fundamentais.

Qual o público alvo da cartilha?

Instituições, órgãos públicos, empresas e pesquisadores que planejam, desenvolvem e implementam funcionalidades ou produtos de identidade digital.

Como navegar pela cartilha?

EXEMPLOS: CASOS CONCRETOS

! **Caixa de explicação:** conceitos chave

1 EM BUSCA DOS CONSENSOS EM UMA INFRAESTRUTURA PÚBLICA DIGITAL

Assim como há investimento público para construção de infraestrutura física, como a construção de ruas, rodovias e ferrovias, cada vez mais é necessária a implementação de uma infraestrutura pública digital (*digital public infrastructure* ou IPD).

Mesmo sem perceber, as pessoas usam a infraestrutura física para se locomoverem e acessarem espaços no cotidiano. Para as pessoas visitarem repartições públicas, agências bancárias, clínicas de saúde, lojas e amigos, elas dependem de infraestruturas como rodovias, avenidas, ônibus, carros, postos de gasolina, paradas de ônibus, faixas de pedestres e calçadas. No entanto, cada vez mais as pessoas usam espaços digitais para realizar essas atividades. É possível e conveniente acessar conta bancária, conversar com família e amigos, pagar impostos, realizar consultas médicas, receber benefícios do governo, entre outros, sem sair de casa.

Assim, da mesma forma que a infraestrutura física é fundamental para que as atividades do cotidiano sejam realizadas, o debate sobre a construção de uma infraestrutura digital ganha destaque. Essa estrutura é entendida como uma solução para simplificar o fluxo de pessoas e dados, e, com isso, ampliar o bem-estar social.

Por ter como objetivo a reconstrução e o aprimoramento das estruturas fundantes das mais diversas organizações, o desenvolvimento de uma IPD pode criar resultados exponenciais para diferentes setores, como o financeiro, a saúde, o comércio, e para a sociedade como um todo.

No entanto, ainda não há um **conceito** único do que seria uma IPD. Diversas entidades debatem o tema justamente para definir quais elementos essenciais compõem uma aplicação de IPD. A partir dessa definição, seria possível fomentar e direcionar os incentivos para aplicações de IPD homogêneas e que respeitasse esses parâmetros.

Em vista da potencialidade dessa infraestrutura, o G20, especialmente durante a presidência da Índia, encampou o tema como ferramenta fundamental para a prestação de serviços públicos em escala. A partir daí, foram sendo delineados sentidos para uma IPD. O próprio G20[1] formulou uma definição do que seria uma IPD.

---

1 G20. Compilation of documents annexed to the G20 New Delhi Leaders' Declaration and other official documents adopted during India's G20 Presidency. **G20 Digital Economy Ministers' Meeting Outcome Document and Chair's Summary**. Bengaluru, 19 ago. 2023, p. 333. Disponível em: https://www.g20.in/content/dam/gtwen-

Com o avanço dos debates internacionais sobre o conceito e as aplicações de uma IPD, outros agentes se somam a esse contexto para moldar o que se entende como aplicação dessa infraestrutura. A título de exemplo, para o Banco Mundial[2], a IPD seria como os "trilhos" que sustentam as transações e as conexões digitais inclusivas entre pessoas, empresas e governos, incluindo a prestação de serviços e operações nos setores público e privado.

A delimitação desses conceitos serve para os rumos de uma IPD ganharem sentido e direção. Por meio do uso de qualificadores como "inclusivo", "interoperável" e "com envolvimento de diversos setores", começa-se a delinear quais tipos e critérios para que uma aplicação seja reconhecida globalmente como uma IPD.

Uma aplicação de IPD inclusiva significa que ela pode ser utilizada por todas as pessoas que se interessarem, eliminando qualquer barreira discriminatória.

As aplicações de IPD devem ser capazes de se comunicar entre si. Aplicações interoperáveis surgem a partir da definição de padrões que permitirão a troca de dados mesmo entre sistemas diferentes.

Em regra, soluções de infraestrutura são planejadas e implementadas por vários atores, já que elas impactam não só um setor, mas toda a sociedade. Aplicações de IPD devem ser resultado de um esforço conjunto de diversos grupos sociais.

ty/gtwenty_new/document/nov-23/Compilation_of_documents_annexed_to_the_G20_NDLD.pdf. Acesso em: 22 abril 2024.

2 WORLD BANK. ID4D. **A Digital Stack for Transforming Service Delivery: ID, Payments, and Data Sharing**. 22 fev. 2022. Disponível em: https://documents1.worldbank.org/curated/en/099755004072288910/pdf/P1715920edb5990d60b83e037f756213782.pdf. Acesso em: 27 mar. 2024.

Em 2024, o debate internacional ganha molduras brasileiras. O Brasil assumiu a presidência do G20, aproximando as discussões sobre o desenvolvimento e as premissas de uma infraestrutura pública digital no Brasil. Um dos fatores que evidenciam essa mistura é a aprovação de uma Estratégia Nacional de Governo Digital por meio do Decreto nº 12.069, de 21 de junho de 2024[3].

O Decreto visa articular e direcionar as estratégias de transformação digital da administração pública brasileira, no âmbito federal, estadual e municipal. A Estratégia está prevista na Lei de Governo Digital, a Lei 14.129, de 29 de março de 2021, e seu texto, que esteve em consulta pública, é resultado de uma construção feita pelo Ministério da Gestão e da Inovação em Serviços Públicos[4].

Para o Decreto, IPD são soluções de escala universal resultantes da orquestração de diversos atores, seja do setor público ou privado.

Cada entidade tem apresentado descrições e enfoques diversos e específicos para delimitar uma IPD. Apesar da difusão de sentidos, a definição de um conceito de IPD permitiria traçar diretrizes globais ou mesmo locais para o desenvolvimento dessa infraestrutura.

---

3 BRASIL. Presidência da República. **Decreto nº 12.069, de 21 de junho de 2024**. 2024. Disponível em: https://www.planalto.gov.br/ccivil_03/_Ato2023-2026/2024/Decreto/D12069.htm. Acesso em: 24 jun. 2024.

4 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.

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

Com a assimilação dos parâmetros do G20 por diversas entidades, é possível dizer que está se formando um nível de consenso a respeito das características desse sistema. A infraestrutura deve ser composta por tecnologia aberta e interoperável com interfaces de governança transparentes, responsáveis e participativas para permitir a inovação e o desenvolvimento de um valor social[5]. Enquanto infraestrutura, as aplicações de IPD são resultados de um ecossistema robusto de partes interessadas, sejam elas representantes do setor público, privado e da sociedade civil. Assim, para além desses atores impulsionarem a inovação, eles também garantem o desenvolvimento contínuo, a confiança e a responsabilização da infraestrutura.

O que "**infraestrutura**" quer dizer? Algumas categorias são reconhecidas como parte da infraestrutura física, a exemplo da malha de transporte, da geração e distribuição de energia, das estruturas de telecomunicações, da distribuição de água e do saneamento. Mesmo assim, para além desses exemplos, ainda é vago definir o que é uma infraestrutura. Em uma linguagem cotidiana, infraestrutura pode ser entendida como "coisas que usamos para construir outras coisas" ou "a tecnologia e os sistemas necessários ao funcionamento da sociedade[6]".

Apesar da vagueza do que seria considerado infraestrutura, esse é o conceito chave para se evitar que o conceito de IPD seja amplo demais[7]. Ou seja, que ele abarque aplicações diferentes e divergentes e, com isso, faça o termo perder sentido. Para definir infraestrutura, o professor Porteous utiliza os princípios para infraestrutura do mercado financeiro (Principles for Financial Market Infrastructures ou PFMI), publicado pelo Banco de Compensações Internacionais. Nessa abordagem, dois elementos merecem destaque:

- caráter multilateral da infraestrutura;
- existência de um operador responsável por fazer a infraestrutura funcionar orquestradamente.

Segundo essa abordagem proposta, soluções que não permitem uma interação

---

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

6 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.

7 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.

com várias entidades, pessoas e organizações são serviços ou aplicações que não podem ser percebidas como infraestrutura. Ainda, para fins de supervisão e regulação, é fundamental que haja uma entidade que opere a infraestrutura. Esse elemento é tensionado em casos de aplicações descentralizadas, como a internet, em que não há uma única autoridade central responsável pelos sistemas. Porém, apesar da tensão sobre esse aspecto, ele não deixa de ser útil para se caracterizar uma infraestrutura.

Caso M-Pesa

O Kenia possui uma solução de pagamento móvel chamada M-Pesa. Essa solução é amplamente utilizada e pode ser considerada essencial para as pequenas empresas. No entanto, a solução não é verdadeiramente multilateral, apesar de envolver outras partes, como os bancos e prestadores de serviços[8]. Isso porque a solução é gerida de forma centralizada pela empresa Safaricom[9] e ela permite apenas a participação de algumas entidades, sobretudo bancos, as quais possuem acordos bilaterais com a Safaricom, em vez de fazer parte de um sistema aberto e interoperável onde múltiplas instituições financeiras podem interagir livremente.

Assim, de forma geral, aplicações de infraestrutura seriam aquelas utilizadas pelo coletivo, com utilidade ampla, para além de necessidades de grupos específicos e, por isso, acessada pelos mais diversos atores. Ainda, a infraestrutura seria um conjunto de sistemas que permitiria pessoas, governos, e empresas se relacionarem para finalidades não limitadas pela própria infraestrutura. Ou seja, ela funcionaria como intermediária para aplicações desenvolvidas nela, atendendo necessidades e propósitos diversos.

I + P + D Outro elemento da IPD é o sentido de "**público**", já que qualquer infraestrutura digital deve ser pública para ser considerada uma IPD. Em uma primeira vista, é importante notar o que uma IPD não é.

Ser uma infraestrutura pública não significa ser de responsabilidade de um governo,

---

8 PORTEOUS, David. **Is DPI a useful category or a shiny new distraction?** 2023, p. 11. Disponível em: https://www.integralsolutionists.com/is-dpi-a-useful-category-or-a-shiny-new-distraction. Acesso em: 27 abril 2024.

9 DONOVAN, Kevin. Chapter 4. **Mobile Money for Financial Inclusion**. 2012. Disponível em: https://documents1.worldbank.org/curated/en/727791468337814878/585559324_20140619104205l/additional/722360PUB0EPI00367926B9780821389911.pdf. Acesso em: 25 jun. 2024.

ou mesmo ser possuída ou licenciada pelas entidades do Poder Público. Para além disso, definir os parâmetros para uma aplicação ser considerada pública é tarefa árdua e controversa entre pessoas que pesquisam e implementam essas abordagens.

David Eaves e Mariana Mazzucato, Beatriz Vasconcellos, da Universidade de Londres (UCL)[10], entendem que o sentido de uma infraestrutura pública é refletido pela maximização do valor público daquela aplicação. O primeiro passo seria tornar explícito o significado de valor público. Este conceito está intimamente ligado ao que uma sociedade entende por bem comum, ou *'common good' framework*.

O bem comum, pela perspectiva de Mazzucato[11], possui cinco pilares:

- **Objetivo e direção:** Definir uma direção ambiciosa para a qual as políticas podem ser concebidas, as parcerias público-privadas formadas e os cidadãos envolvidos;
- **Co-criação e participação:** Definir as regras e os mecanismos de co-investimento, colaboração e coordenação que envolvam um grupo diversificado de entidades;
- **Aprendizagem coletiva e compartilhamento de conhecimentos:** Repensar práticas institucionais que apoiem a aprendizagem coletiva e desenvolvam capacidades e competências a longo prazo;
- **Acesso para todos e compartilhamento de benefícios:** Garantir que o valor público é distribuído de forma equitativa (crescimento inclusivo); e
- **Transparência e responsabilização:** Ganhar e manter a confiança dos cidadãos no acompanhamento do progresso através de práticas que demonstrem um compromisso com a transparência e a responsabilidade.

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[12]. É a partir da definição do bem comum que o valor público ganha sentido e direcionamento. Assim, as tecnologias e aplicações

---

10 EAVES, David; MAZZUCATO, Mariana; 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/sites/bartlett_public_purpose/files/iipp_wp_2024-05.pdf. Acesso em: 25 abril 2024.

11 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.

12 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.

de IPD passam a atender finalidades e objetivos específicos da comunidade em que estão inseridas.

Além da ideia de bem comum, os aspectos de governança e o papel do estado devem ser levados em consideração para identificação de uma IPD. Isso porque o processo para se entender o que é considerado valor público é tão importante quanto o seu próprio resultado e deve ser conduzido de forma coletiva e coordenada. Com isso, é fundamental criar estruturas de governança para que os diferentes interessados possam avançar coletivamente no sentido do bem comum[13].

Entender o que é considerado valor público através de um processo é essencial para assegurar que as iniciativas de IPD realmente atendam às necessidades e aspirações da comunidade. Esse entendimento não só direciona os esforços de maneira eficaz, mas também garante a legitimidade e a sustentabilidade dos resultados alcançados. Com isso, a coordenação de interesses no processo é essencial para assegurar que as diversas perspectivas e interesses sejam considerados, promovendo um consenso aberto e participativo sobre o que constitui valor público. Portanto, investir em estruturas de governança que promovam a participação ativa e a coordenação entre todos os stakeholders é fundamental para maximizar o valor público.

Sistema de pagamento desenvolvido por uma empresa de bandeira de cartões de pagamento:

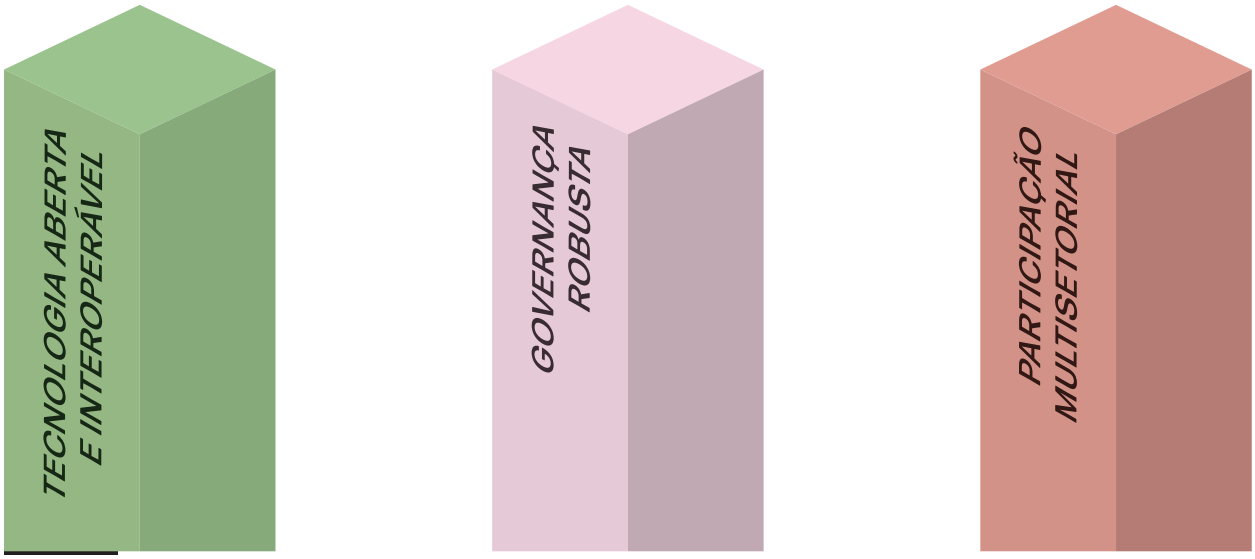
É possível argumentar que a evolução dos meios de pagamentos contribuíram para a inclusão financeira e para a participação das pessoas na economia digital global. Porém, de acordo com Eaves, Mazzucato e Vasconcellos, a criação de valor público significa que os objetivos sociais amplamente aceitos podem ser alcançados em processos de inovação colaborativa entre diferentes atores que co-criam mercados. Para gerar efetivamente tais resultados, é essencial disponibilizar conhecimentos no planejamento, implementação, gestão e coordenação entre vários grupos de interesse. Não necessariamente esse foi o processo encampado pelo sistema de pagamento em questão, por isso é questionável a interpretação de que esses sistemas configuram como IPD.

13 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.

I + P + D Em regra, o termo **"digital"** da IPD não restringe o conceito de infraestrutura pública digital a depender do nível de intensidade de sua digitalização. Parece haver poucos benefícios em restringir a IPD a alguns tipos de aplicações digitais, mas é relevante notar as gradações de digitalização existentes[14]. Como exemplo, a OCDE propôs uma classificação de digitalização em três níveis: uma camada nuclear, nos casos em que apenas há o uso de dispositivos eletrônicos, como computador e celular; uma camada estreita, que inclui a realização de atividades no digital; e uma camada ampla, em que as atividades foram significativamente melhoradas pelas tecnologias e dados digitais[15]. Mesmo com essa gradação, diferentes tipos de aplicações podem ser consideradas digitais pelo uso desse novo meio.

Diante da dificuldade de se traçar parâmetros objetivos do que seriam aplicações de IPD, algumas definições limitam-se a enumerar os três setores reconhecidamente chamados de IPD. Esses setores são o de pagamentos, o de identidade e o de compartilhamento de dados. Essa forma de definir IPD não restringe o conceito a apenas estes setores, mas cria a inferência de que, para que outros setores sejam acrescentados, teriam de demonstrar fortes semelhanças com estes três setores principais[16].

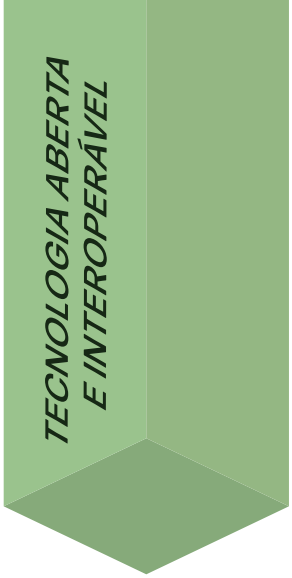
Por outro lado, alguns buscam entender a IPD a partir de seus elementos fundamentais. No sentido apresentado pelo G20, a IPD se fundamenta em **três pilares**:



14 PORTEOUS, David. **Is DPI a useful category or a shiny new distraction?** 2023, p. 11. Disponível em: https://www.integralsolutionists.com/is-dpi-a-useful-category-or-a-shiny-new-distraction. Acesso em: 27 abril 2024.

15 OECD. **Handbook on Measuring Digital Platform Employment and Work**. 3. Conceptual framework, concepts and definitions. 2023. Disponível em: https://www.oecd-ilibrary.org/sites/2d333ec3-en/index.html?itemId=/content/component/2d333ec3-en. Acesso em: 25 abril 2024.

16 PORTEOUS, David. **Is DPI a useful category or a shiny new distraction?** 2023, p. 11. Disponível em: https://www.integralsolutionists.com/is-dpi-a-useful-category-or-a-shiny-new-distraction. Acesso em: 27 abril 2024.

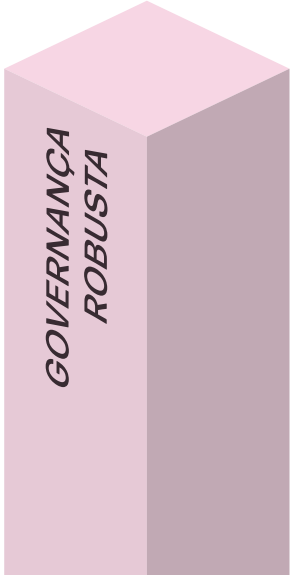


(i) tecnologia aberta e interoperável, (ii) governança robusta, e (iii) participação multissetorial[17]. Sem esses elementos, é provável que os objetivos da IPD sejam bastante prejudicados e limitados a um grupo específico, sem produzir o impacto geral que se pretende.

O primeiro conceito indica que a infraestrutura deve ser desenhada em **protocolos comuns** para que outras funcionalidades possam ser adicionadas a ela e essas possam interagir entre si. O ecossistema deve ser construído com base em princípios de abertura, interoperabilidade e escalabilidade, de forma que módulos independentes possam ser adicionados e aprimorados conforme desenvolvimento da infraestrutura. É imprescindível que seja possível a comunicação e a troca de informações entre sistemas de forma a gerar confiança e facilitar o fluxo de dados.

No contexto de IPD, os conceitos de interoperabilidade e escalabilidade são fundamentais para garantir que o sistema seja eficiente, flexível e capaz de evoluir conforme as demandas crescem. A escalabilidade é justamente a capacidade de um sistema aumentar sua capacidade e funcionalidade de forma eficiente à medida que a demanda cresce, sem comprometer o desempenho ou a qualidade dos serviços oferecidos. Como será visto nesta seção, a interoperabilidade refere-se à capacidade de diferentes sistemas, dispositivos, aplicativos ou serviços de se comunicarem, trocarem dados e utilizarem essas informações de maneira coordenada e eficiente, independentemente das suas origens ou plataformas.

A partir da troca de informações entre sistemas, outras características da tecnologia surgem como base para a IPD, como a extensividade e a escalabilidade[18]. Esses elementos indicam para uma abordagem de "*building blocks*", ou seja, blocos de construção, em que é possível acomodar mudanças e aumentar funcionalidades da infraestrutura sem perder suas funcionalidades anteriores, permitindo atualizações e aprimoramentos sempre que necessário. Com isso, a tecnologia utilizada na construção de uma IPD permite que módulos independentes possam ser adicionados e aprimorados conforme desenvolvimento da infraestrutura.



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

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

O segundo elemento determina que o ecossistema de IPD esteja de acordo com parâmetros de **governança**, isto é, a infraestrutura deve ser confiável, transparente e responsável. Uma das utilidades da governança é permitir que obrigações legais sejam incorporadas diretamente na arquitetura da infraestrutura, garantindo que os agentes cumpram a lei através do simples ato de participação. Por padrão, as regulamentações setoriais seriam cumpridas, já que o sistema estaria adequado, inclusive a normas de proteção de dados pessoais, que é um dos direitos com maior tensão no âmbito de uma IPD.

Um sistema com governança robusta significa que ele é projetado de forma que as conformidades legais sejam integradas e automáticas. Esse é um desafio para os desenvolvedores de aplicações de IPD, porém, para que seja considerada IPD, a aplicação de forma que as conformidades legais sejam integradas e automáticas.

Na prática, isso se traduz no design de sistemas com regras incorporadas, como mecanismos de proteção de dados que garantam a privacidade dos usuários conforme regulamentos. Isso pode incluir criptografia, controle de acesso e anonimização de dados. Além disso, protocolos de segurança cibernética e autenticação devem ser integrados para proteger contra acesso não autorizado e garantir a integridade dos dados. Essas ferramentas reforçam o entendimento do desenvolvimento de aplicações de IPD ser um processo de constante avaliação e aprimoramento, apenas assim elas poderão concretizar os pilares de uma IPD.

A implementação de parâmetros de governança implica em maximizar o benefício aos cidadãos, a confiança e a transparência que garantem que a IPD seja segura, protegida, confiável e responsável[19]. A governança também promove a inclusão, já que durante a condução de processos necessários para se ter uma governança sobre a IPD, invariavelmente os parâmetros de inclusão devem ser enfrentados[20].

Já o elemento de **participação ativa** de diferentes setores da sociedade na construção da IPD destaca a relevância da inovação no mercado e da prestação de serviços para potencializar as experiências das pessoas. É apenas por meio da participação de grupos de empresas,

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

20 EAVES, David; MAZZUCATO, Mariana; 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/sites/bartlett_public_purpose/files/iipp_wp_2024-05.pdf. Acesso em: 25 abril 2024.

entidades da sociedade civil, associações, consumidores, pesquisadores, acadêmicos e qualquer agente impactado que será possível desenvolver soluções centradas no cidadão, usuário daquela aplicação. A cooperação entre atores permite o desenvolvimento de soluções inovadoras e a sustentabilidade do sistema[21]. Ao permitir que outros grupos contribuam ativamente, é possível que os governos possam criar um ecossistema digital mais dinâmico, sustentável e inclusivo.

Para que uma aplicação seja considerada parte de uma IPD, é imprescindível que exista um aspecto formal de participação que transcenda a mera consulta orientativa e se estabeleça como elemento fundamental e vinculante. A participação efetiva da sociedade com poder de decisão e direcionamento das diretrizes é pressuposto sem a qual não há desenvolvimento de IPD. Assim, a procedimentalização dessa participação deve abranger a cadeia de desenvolvimento e implementação da aplicação durante todo seu curso, definindo regras mínimas e mecanismos que garantam a inclusão efetiva de grupos vulnerabilizados.

Isso pode incluir, por exemplo, a destinação de parte dos recursos da IPD para financiar pesquisas sobre o impacto da aplicação, bem como ofertas de auxílio para representantes da sociedade civil participarem ativamente dos fóruns de discussão multissetorial. Além disso, essa participação deve ter um caráter vinculante, permitindo que o escrutínio público tenha o poder de barrar propostas ou alterar sua direção, assegurando um processo verdadeiramente deliberativo e não apenas consultivo.

O pilar de participação, somado a uma governança robusta, garante que os objetivos da infraestrutura sejam atingidos de maneira ampla e inclusiva. Nesse sentido, um sistema robusto deve permitir à sociedade espaços de aprimoramento das aplicações a partir da identificação de desafios e pontos de melhoria a partir da experiência dos cidadãos, já que estão em contato com as funcionalidades da aplicação e com os responsáveis pelo seu desenvolvimento.

Nesse sentido, apesar de uma IPD ser complexa e composta de diversos elementos e atores, é por meio da implementação de um ecossistema digital que países buscam impulsionar o crescimento inclusivo, a inovação e a capacitação. A infraestrutura digital é uma ferramenta já implementada em algum nível por diversos países. Nesses casos, ela é percebida como uma ponte para facilitar a inclusão,

---

21 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-dpi-approach-pub-89721. Acesso em: 27 jan. 2024.

eficiência e empoderamento da população em face das atividades comuns de uma sociedade[22].

O Brasil é um dos países que está caminhando para a consolidação de uma infraestrutura pública digital incidente em diversos setores, de forma a impactar não apenas como serviços públicos são prestados, mas também qualquer outra atividade ou serviço utilizado pelos cidadãos. O Brasil já lidera discussões globais de infraestrutura tecnológica no setor financeiro, com o desenvolvimento do Pix, e no acesso a serviços públicos, com o Gov.br.

A construção de uma IPD sólida e efetiva depende intrinsecamente de seus pilares em uma tecnologia aberta e interoperável, uma governança robusta e um engajamento multissetorial. A adoção de tecnologias abertas e interoperáveis assegura que os sistemas sejam flexíveis, acessíveis e capazes de se comunicar entre si, promovendo a inovação e o aprimoramento dos sistemas. A governança robusta garante que as decisões sejam tomadas de maneira transparente e responsável, enquanto a participação social ativa, especialmente com mecanismos que permitam a inclusão de grupos vulnerabilizados, assegura que as diversas vozes da sociedade sejam ouvidas e consideradas. Juntas, essas bases não apenas potencializam o impacto da IPD, mas também promovem um desenvolvimento equitativo e sustentável.

---

22 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-dpi-approach-pub-89721. Acesso em: 27 jan. 2024.

2 IDENTIDADE DIGITAL: UMA DAS APLICAÇÕES CHAVE DA IPD E SUAS FUNÇÕES TÍPICAS

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 esses sistemas só podem funcionar se for possível identificar o beneficiário das aplicações 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.

É por meio de validações de identidade, seja online ou offline, que as pessoas acessam serviços essenciais, públicos ou privados, nacionais ou internacionais. 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.

Por exemplo, para que um banco conceda um empréstimo para um cliente, ele deve saber com quem está contratando e quais as características dessa pessoa, a mesma situação é replicada para acessar um benefício social e para uma consulta médica, entre outros. Essas informações de identidade podem estar dispersas em molduras ou camadas diferentes e complementares, coletadas em diversos contexto, como será descrito na próxima seção desta cartilha.

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-se a identidade dos sujeitos envolvidos no processo.

Como tornar esse processo digital sem que ele deixe de ser confiável? Uma identidade digital é apontada como mais uma maneira de facilitar o processo de autenticação de identidade, tornando o acesso a bens e serviços mais seguro e menos burocrático.

De acordo com a OCDE, uma **identidade digital** é um conjunto de atributos coletados e armazenados eletronicamente que podem ser utilizados para provar uma

caraterística, qualidade, ou afirmação sobre um cidadão e, quando necessário, apoiar a identificação única desse usuário[23]. Com essa ferramenta, é possível simplificar o acesso a diversos serviços, adicionando uma alternativa opcional à verificação de credenciais físicas e, assim, fortalecer uma abordagem de IPD.

Credenciais: Um objeto ou estrutura de dados que vincula com autoridade uma identidade (e opcionalmente, atributos adicionais) a um *token* possuído e controlado por uma entidade confiada pela entidade provedora da credencial[24].

Informação pessoalmente identificável (*Personal Identifiable Information*, PII): informações utilizadas para identificar, contactar ou localizar uma pessoa de forma única.

Nessa infraestrutura, novas ferramentas são desenvolvidas para conduzir processos confiáveis e protetivos de identificação, já que eles criam valor para organizações e governos a partir da identidade dos usuários. Nota-se que uma das características da identificação, diante do conceito da OCDE, é seu caráter único, ou seja, só é possível identificar um ente se apenas ele possui aquela identidade.

Esse caráter de **unicidade** da identidade cria uma tensão que é ainda mais agravada no contexto digital. É comum que uma pessoa possua diferentes atributos e utilize parte deles sempre que necessário. A depender do contexto, uma pessoa pode se identificar como uma professora, irmã, filha, paciente de um hospital, cliente de uma loja ou associada a uma academia de esportes, sem que tenha que ser todos esses atributos de uma vez[25]. Essa fragmentação da identidade é bastante comum, mas controversa em contextos digitais, em que é possível agrupar e disponibilizar uma série de atributos de uma pessoa, mesmo que eles só sejam úteis em contextos diferentes.

---

23 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.

24 NIST. **Withdrawn NIST Technical Series Publication**. 3 jul. 2019, p. 51. Disponível em: https://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf. Acesso em: 2 maio 2024.

25 CARIBOU DIGITAL. **Identities: New practices in a connected age**. Farnham, Surrey, United Kingdom: Caribou Digital Publishing, 2017. Disponível em: https://www.identitiesproject.com/wp-content/uploads/2017/11/Identities-Report.pdf. Acesso em: 2 jun. 2024.

Soluções de identidade são complexas justamente pela multidisciplinaridade que ela afeta, desde efeitos jurídicos, para políticas públicas, para consumo, além da própria personalidade e impactos culturais. Diante da diversidade de âmbitos afetados, as tecnologias que se valem de *big data*, a garantia de interoperabilidade desse sistema, a centralização ou descentralização de bancos de dados, os registros em *blockchains*, e a coleta de biometria como informação para comprovar a unicidade, trazem nova camada de complexidade para esse cenário. O estabelecimento de identificadores únicos ou a dispersão desses atributos indicam para novos desafios no tema.

Ao mesmo tempo que a verificação de identidade é um processo útil, ainda há pouca nitidez sobre quais requisitos uma solução de identidade digital deve ter para ser reconhecida como suficiente para identificar e ser digital. Isso porque não há uma definição de quais funcionalidades são necessárias para que o sistema seja considerado de identidade e, com isso, possa ser um sistema de identidade digital. Os elementos comuns desses sistemas e, por isso, as suas possíveis molduras, serão analisadas no próximo capítulo.

O Banco Mundial entende por sistemas de identificação digital aqueles que utilizam tecnologia durante todo o ciclo de vida da identidade, inclusive para captura, validação, armazenamento e transferência de dados, gerenciamento de credenciais, verificação e autenticação de identidade[26]. Essa definição reconhece que a identidade pode ser fornecida diretamente pelo governo, em parceria ou em terceirização com o setor privado. Porém, apesar de ter essa flexibilidade na emissão, em regra, a identidade digital está vinculada à identidade legal de uma pessoa, que é reconhecida pelo governo para uso com fins oficiais.

É importante destacar que uma identidade digital, mesmo que inserida em um contexto de IPD, não se confunde com uma identidade legal, que é o reconhecimento de uma pessoa como sujeito de direitos e deveres por parte de um Estado[27]. A identidade legal é um direito humano, de acordo com o art. 6 da Declaração Universal dos Direitos Humanos[28], e o acesso a uma identidade legal é o objetivo 16.9 dos Objeti-

---

26 WORLD BANK. **Technology Landscape for Digital Identification**. Washington: World Bank License, 2018. Disponível em: https://documents1.worldbank.org/curated/en/199411519691370495/Technology-Landscape-for-Digital-Identification.pdf. Acesso em: 27 jan. 2024.

27 FUNDACIÓN KARISMA. **Conceptos básicos de los sistemas de identidad**. 7 dez. 2021. Disponível em: https://digitalid.karisma.org.co/2021/12/07/conceptos-basicos-id/. Acesso em: 27 jan. 2024.

28 ONU. **Declaração Universal dos Direitos Humanos**. Adotada e proclamada pela Assembleia Geral das Nações Unidas (resolução 217 A III) em 10 de dezembro 1948. Disponível em: https://www.unicef.org/brazil/declaracao-universal-dos-direitos-humanos. Acesso em: 28 jan. 2024.

vos de Desenvolvimento Sustentável (ODS) definidos pelas Nações Unidas (ONU)[29]. Ao mesmo tempo, sistemas de identidade, online ou offline, possuem semelhanças, como a sua função.

Apesar da diferença de conceitos, existe uma intersecção entre os temas. Atualmente, existe uma lacuna de identidade expressiva no mundo, estima-se que aproximadamente 1 bilhão de pessoas não tenham documento oficial de identidade. A falta de documento de identidade exclui essas pessoas do acesso a serviços essenciais, sejam públicos ou privados. A ONU tem entendido que, por meio da disseminação de soluções digitais, seria possível garantir que mais pessoas possuíssem uma identidade legal[30].

CIN (Brasil):

A emissão da nova identidade legal brasileira se dá no papel e no digital. A CIN está no aplicativo Gov.br. A partir de uma identidade legal, em papel, a pessoa também passa a ter acesso a outros serviços públicos digitais fornecidos pelo acesso ao Gov.br.

Apesar de variar de acordo com seus elementos e molduras, qualquer sistema de identidade tem três **funções** basilares[31]:

- Identificar,
- Autenticar, e
- Autorizar.

A função de **identificação** determina o registro de uma pessoa por meio da coleta de informações pessoais biográficas e da emissão de credenciais para que seja possível provar uma identidade. A coleta dessas informações, em regra, acontece por meio da apresentação de documentos de registro civil, como certidão de nascimento ou certidão de casamento.

---

29 ONU. **Objetivo de Desenvolvimento Sustentável 16**. Paz, Justiça e Instituições Eficazes. Disponível em: https://brasil.un.org/pt-br/sdgs/16. Acesso em: 28 jan. 2024.

30 UNDP. **How digital can close the 'identity gap'**. 19 maio 2022. Disponível em: https://www.undp.org/blog/how-digital-can-close-identity-gap.

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

Dados biográficos: dados pessoais mínimos registrados sobre uma pessoa. Esses dados podem variar a depender da autoridade que expede a credencial. Na União Europeia, os dados mínimos são: (1) nome(s) de família atual(is), (2) nome(s) atual(is), (3) data de nascimento e (4) um identificador único. Atributos adicionais incluem: (5) sobrenome de nascimento, (6) primeiro nome de nascimento, (7) local de nascimento, (8) endereço atual e (9) sexo[32].

Em regra, essa função do sistema de identidade é alcançada a partir de ações conduzidas pelas autoridades públicas do lugar no qual os documentos de registro civil foram emitidos. A partir da coleta das informações, elas podem ser verificadas, momento em que se estabelece uma ligação entre uma identidade reivindicada e a pessoa que apresenta as provas. No entanto, algumas pessoas não possuem nenhum documento de registro. Nestas situações, os sistemas de identificação podem verificar a identidade e o endereço da pessoa de outra forma[33].

Uma vez concluída a verificação, é possível que se identifique alguma duplicidade na emissão do documento, se colete algum registo biométrico e se emita o documento de identificação. Esse documento é a credencial que será utilizada nas interações subsequentes. Essa credencial pode ser física ou digital, mas é fundamental que ela seja interoperável para autenticação, de forma que outras pessoas possam verificar sua validade.

---

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

33 WORLD BANK. **Technology Landscape for Digital Identification**. Washington: World Bank License, 2018, p. 5. Disponível em: https://documents1.worldbank.org/curated/en/199411519691370495/Technology-Landscape-for-Digital-Identification.pdf. Acesso em: 5 maio 2024.

eID (União Europeia)[34]

A identificação eletrônica (eID), resultado do Regulamento eIDAS (910/2014), é um conjunto de serviços prestados pela Comissão Europeia para permitir o reconhecimento mútuo dos sistemas nacionais de eID além-fronteiras de cada país da UE. A eID permite que os cidadãos europeus utilizem os seus eID nacionais quando acessarem serviços online de outros países europeus. O sistema garante uma interoperabilidade jurídica, organizacional, semântica e técnica, de forma a validar identidades emitidas por outras entidades e, com isso, facilitar as operações digitais que requerem reconhecimento de identidade transfronteiriço.

Já a **autenticação** é a possibilidade 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 responsável por uma determinada identidade diz ter, conhecer ou ser. Em regra, esses fatores são as senhas que uma pessoa conhece, as informações biométricas que apresenta, um acesso a um serviço que ela já possui, um token, ou uma combinação desses elementos.

Coisas que uma pessoa...

TEM	SABE	TEM (E SÓ ELA TEM)
▪ cartão ▪ certificado ▪ token de segurança ▪ aplicativo ▪ cartão de acesso	▪ senhas ▪ frase de acesso ▪ PIN ▪ *challenge response* ▪ segredos	▪ impressão digital ▪ iris ▪ rosto ▪ comportamento ▪ dados biométricos

Inspirado em *ID4D Practitioner's Guide*[35]

---

34 UNIÃO EUROPEIA. European Commission. **How does it work?** 2024. Disponível em: https://ec.europa.eu/digital-building-blocks/sites/pages/viewpage.action?pageId=467109866. Acesso em: 2 maio 2024.

35 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.

Sistemas de autenticação tendem a ser mais seguros se eles combinam mais de um desses fatores, de forma a, por exemplo, a pessoa demonstrar que sabe a senha de um aplicativo e possui um dispositivo de confiança, como um celular ou uma senha. Essa combinação de fatores é conhecida como duplo grau de autenticação.

Nesse momento, alguns desafios já são conhecidos: reduzir o tempo de processamento, melhorar a precisão da autenticação, garantir uma experiência com poucas barreiras para as pessoas, mitigar desafios com conectividade de rede, combater comportamentos fraudulentos e encontrar soluções de hardware e software acessíveis. Assim, não basta que uma pessoa se identifique, diga quem ela é, ela deve ser capaz de provar que ela é quem diz ser. A sua identidade tem de ser identificável.

Background check em entrevista de emprego

Quando uma pessoa aplica para uma vaga de emprego, é possível que os recrutadores solicitem documentos que comprovem suas experiências prévias, bem como suas credenciais acadêmicas. É possível que esses recrutadores verifiquem a validade de um diploma de bacharelado a partir das informações disponibilizadas no próprio diploma, bem como no sistema de autenticação de documentos da própria universidade emissora da credencial.

Já a função de **autorização** determina a possibilidade de uma pessoa com identidade autenticada acessar serviços ou informações específicas, adequadas e limitadas para o seu nível de acesso. A partir da autenticação de uma identidade, são definidos os direitos de acesso que uma entidade associou à determinada identidade. Nos regimes de autorização mais complexos, as regras de acesso podem ser contextuais e dinâmicas.

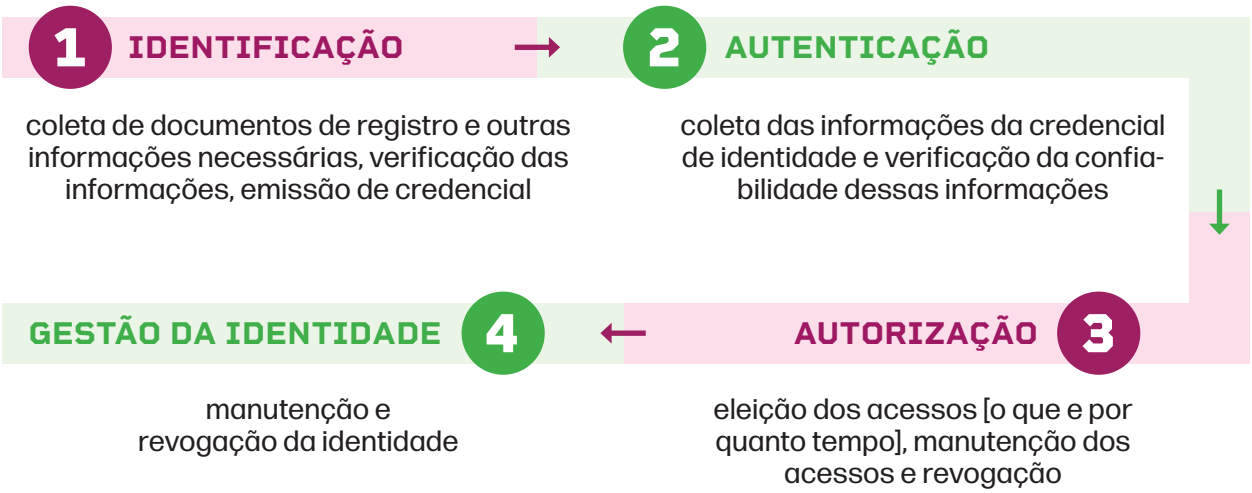
Blitz de trânsito

é comum que forças policiais realizem processos de verificação de identidade das pessoas que conduzem veículos. Nesses processos, as autoridades verificam a autenticidade da identidade, bem como as autorizações que a credencial da carteira de identidade garante. É o caso da autoridade que fiscaliza uma pessoa condutora de caminhão. Se a pessoa que dirige esse veículo, apesar de ter carteira de habilitação autentica, não tem autorização para conduzir caminhão, a sua identidade limita os acessos que a pessoa possui.

Sistemas de identidade são fundamentais para a prestação de serviços e o cumprimento de direitos e obrigações. Esses sistemas devem atender às funções de identidade, já que comuns a qualquer sistema de identidade, não havendo diferença se o sistema está inserido ou não no contexto de uma IPD.

Em algumas situações, tanto as instituições do setor público como o privado precisam saber quem são as pessoas com quem estão se relacionando. Ainda, para transações econômicas, sociais, políticas e digitais básicas, essas entidades devem ser capazes de confiar que as pessoas são quem dizem ser, ou seja, que ninguém roubou ou hackeou suas credenciais de identidade. Além disso, é possível que essas entidades precisem confirmar, seja durante a integração inicial de um novo beneficiário ou cliente, ou de forma contínua, que a pessoa é elegível para acessar um determinado direito, serviço, informação ou funcionalidade do sistema[36]. Dessa forma, é evidente que as funções de sistemas de identidade são exercidas em diferentes momentos para garantir confiança na aplicação utilizada.

Essas funções não são independentes entre si, mas são entrelaçadas e convergentes no contexto concreto de aplicação. De acordo com o Banco Mundial, elas formam um ciclo em que, a partir da identificação, é possível autenticar e autorizar acessos até que a identidade seja revogada. Isso ocorre, por exemplo, quando a pessoa identificada falece.



36 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.

O desenvolvimento de sistemas de identidade digitais, enquanto uma das aplicações chave da IPD, está sendo endossado por entidades internacionais, principalmente em vista do objetivo 16.9 dos ODS[37]. Ao mesmo tempo, para que seja reconhecido enquanto parte de uma IPD, é fundamental que seja possível destacar de que forma as aplicações de ID compõem uma infraestrutura digital de forma a gerar valor público de acordo com as funções que esses sistemas possuem. Por meio de processos de verificação de identidade digital, é possível garantir o acesso a benefícios, direitos e serviços para aquelas pessoas que fazem jus.

No mundo digital, diante das demandas, principalmente, de prevenção à fraude e da garantia de confiança na relação firmada pelo digital, os elementos que formam um sistema de identidade se tornaram complexos. Para além de não haver uma definição dos requisitos de uma identidade digital, sistemas de identificação podem ser compostos de diversos elementos e pressupostos que formam molduras próprias.

Por sua vez, essas molduras delimitam a estrutura que esses sistemas podem ter, inclusive suas funcionalidades. Por isso, é necessário sedimentar os consensos e avançar no tema para que seja possível desenvolver uma identidade digital cidadã, ou seja, com bases fortes nos valores de uma IPD.

---

37 EAVES, David; MAZZUCATO, Mariana; 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). p. 17. Disponível em: https://www.ucl.ac.uk/bartlett/public-purpose/sites/bartlett_public_purpose/files/iipp_wp_2024-05.pdf. Acesso em: 25 abril 2024.

3 POSSÍVEIS MOLDURAS PARA OS SISTEMAS DE IDENTIDADE

Com o avanço tecnológico, diversos sistemas de identidade foram desenvolvidos por várias entidades, públicas ou privadas, para finalidades diferentes. Todas essas aplicações têm em comum o objetivo de criar e confirmar credenciais em momentos e contextos específicos, garantindo que aquela pessoa tem algo em comum ou é a mesma que fez um primeiro cadastro. É por conta desse elemento que várias soluções podem ser percebidas como sistemas de identidade. Com base nas similaridades desses sistemas, serão apresentadas três possíveis molduras que remontam elementos peculiares desse ecossistema de identidade.

Vale notar que essas molduras não levam em consideração os requisitos de uma infraestrutura pública digital, já que refletem as demandas de sistemas de identificação sem pretenderem ser validados pelos parâmetros de uma IPD - cruzamento que será feito na próxima seção. Mesmo assim, essas molduras importam na construção de uma identidade digital enquanto aplicação da IPD, a fim de se perceber as variações concretas desses sistemas.

3.1 Entidades envolvidas no sistema

Um sistema de identidade pode se organizar de forma simples ou complexa, a depender do número de entidades envolvidas na sua implementação.

Em regra, um sistema mais tradicional, principalmente aquele vinculado à função de identificar, envolve poucas entidades para sua implementação. Por isso, esse sistema é percebido como **simples**.

O sistema simples é formado por dois atores: uma pessoa identificável e uma entidade responsável por identificar. Essa entidade, que assume diversas funções para permitir a identificação, emite uma identidade e, com base nas credenciais emitidas por ela própria, reconhece a pessoa identificada. Nos sistemas simples, é possível que a pessoa e a entidade reconheçam uma à outra ou elas dividam suas funções entre usuário e provedor de serviço de identidade.

Assim, com menos intervenientes envolvidos, o modelo de confiança na identidade de sistema simples é pouco complexo, uma vez que existem menos pontos potenciais de falha ou de quebra de confiança. Ao mesmo tempo, esta simplicidade pode dificultar a escalabilidade e interoperabilidade do sistema.

Nesse sistema, apenas a entidade que identifica pode validar aquela identidade, o que pode tornar o sistema não adequado para a interação de vários usuários que frequentemente precisam confirmar sua identidade. Ainda, em sistema simples, o processo de verificação de identidade não depende da colaboração de outras entidades e pode não ser compatível com outros sistemas - tanto em termos de arranjo tecnológico, quanto de requisitos para reconhecer essa verificação. Esta falta de interoperabilidade pode dificultar ou impossibilitar a integração com serviços, organizações ou ecossistemas externos.

Já os sistemas de identidade **complexos** são formados por diversos atores, que coexistem para, exercendo funções diferentes e complementares, compor o ecossistema daquela identidade. Esses sistemas podem ser formados por vários atores que, em regra, possuem as seguintes funções[38]:

- **Pessoa:** aquela que necessita ser identificada, que precisa de uma identidade para acessar espaços e sistemas;

> ! Para além de sistemas de identificação de pessoas, existem sistemas de identificação de dispositivos eletrônicos, objetos, outros seres vivos, que não serão explorados nesta cartilha, apesar de serem úteis em determinados contextos e possuírem suas próprias complexidades.

- **Representante legal:** a quem a pessoa, o sujeito da identidade, dá poderes para atuar em seu nome, a exemplo dos responsáveis de uma criança, que atuam em nome dela;
- **Provedor de identidade:** entidade responsável por expedir a identidade e controlar os dados dela, que normalmente são coletados e armazenados pelo provedor;
- **Operador do sistema de identidade:** entidade contratada pelo provedor da identidade para exercer algumas funções delegadas por ela, como fornecer serviços tecnológicos para o funcionamento do sistema;

---

38 WORLD ECONOMIC FORUM. **Identity in a Digital World: A new chapter in the social contract**. Geneve: set. 2018, p. 14. Disponível em: https://www3.weforum.org/docs/WEF_INSIGHT_REPORT_Digital%20Identity.pdf. Acesso em: 25 maio 2024.

- **Dispositivos, grupos de dispositivos, ativos físicos e virtuais:** o meio que as pessoas possuem ou utilizam para acessar sua identidade e que podem possuir seus próprios identificadores, como o IMEI de um celular;
- **Entidades de confiança:** entidades autorizadas pelo provedor para confirmar sua expedição;
- **Partes confiantes:** organizações que confiam nas identidades emitidas pelo provedor ou nas confirmadas pelas entidades de confiança para permitir ou negar o acesso a bens, serviços, direitos ou informações;
- **Reguladores:** aqueles que orientam a forma de gerir e utilizar as identidades.

É importante notar que a função de verificar e autenticar a identidade pode ser um serviço compartilhado fornecido pelo provedor a entidades do setor público e privado. Isso ocorre nos casos em que o sistema de identidade permite que usuários aproveitem as credenciais e a autenticação realizada pelo próprio sistema, tornando desnecessária a construção de sistemas de autenticação paralelos e independentes do provedor[39]. Assim, não necessariamente a entidade que deve conduzir o processo de identificação precisa criar um sistema próprio de autenticação dessa identidade ou de emissão de uma nova identidade, ela pode se valer de um sistema já criado, se tornando parte confiante do sistema.

Outra possibilidade é que essas entidades que conduzem processos de identificação o façam enquanto parte confiante de entidades de confiança. Isso significa que a organização que identifica não necessariamente conhece as credenciais e os dados das pessoas identificadas, mas confia na autenticação feita pela entidade de confiança.

Em comparação com sistema simples, vários agentes podem atribuir e validar identidades, além de ser possível que outros agentes componham o ecossistema para apoiar o seu desenvolvimento em outras frentes. Tendo em vista a multiplicidade de atores, esses sistemas também são caracterizados pela multiplicidade de responsáveis, uma vez que cada um exerce funções específicas.

---

39 WORLD BANK. ID4D **Practitioner's Guide: Version 1.0.** Washington: World Bank License, out. 2019, p. 15. Disponível em: https://documents1.worldbank.org/curated/en/248371559325561562/pdf/ID4D-Practitioner-s-Guide.pdf. Acesso em: 28 jan. 2024.

Os sistemas complexos são resultados das demandas de identificação, tanto no mundo analógico quanto no digital. Em um cenário de *Big Data*, os sistemas de identidade passam a ser formados por diversas entidades, seja para acesso a políticas públicas, cadastro em um e-commerce ou streaming, cumprimento de obrigações fiscais, realização de transferência bancária, intimação em um processo judicial, ou precificação de algum serviço de seguro, por exemplo.

É comum que as pessoas se identifiquem de diferentes maneiras e finalidades, em contextos específicos. Ainda, pode ocorrer de as pessoas não serem identificadas a partir do que são, sabem ou possuem, mas sim de informações pessoais compartilhadas por outras entidades. Nesse cenário, a noção de identidade possui impacto direto com atividades de compartilhamento de dados pessoais entre entidades, inferências de informações, integração de sistemas e cruzamento de dados, inclusive pessoais. Todos esses elementos são amplificados em um sistema de identidade complexo composto por diversos atores.

Agentes do ecossistema

Maria é uma profissional que recentemente solicitou um empréstimo para comprar um carro. Para isso, ela forneceu suas informações pessoais ao banco, como nome, CPF, endereço, histórico de emprego, entre outros dados relevantes. O banco, por sua vez, utiliza esses dados para avaliar a credibilidade de Maria.

Entidades participantes:

Banco: O banco envia os dados de Maria para um birô de crédito para obter um relatório de crédito. O relatório inclui informações sobre o histórico de pagamentos de Maria, eventuais dívidas pendentes, e outros fatores que influenciam sua pontuação de crédito.

Birô de Crédito: O birô de crédito agrega os dados recebidos do banco com outras informações já existentes em seu sistema, coletadas de várias fontes, como lojas de varejo, operadoras de cartão de crédito, e concessionárias de serviços públicos.

Outras Entidades: Além das fontes mencionadas, o birô de crédito pode receber informações de outras entidades, como tribunais (sobre processos judiciais que envolvem Maria), redes sociais (que podem fornecer inferências sobre o comportamento e a estabilidade financeira de Maria) e instituições financeiras com as quais Maria já teve relacionamentos.

Com base nos dados recebidos de diversas fontes, o birô de crédito pode inferir informações adicionais sobre Maria. Essas inferências não são baseadas apenas nas informações que ela forneceu diretamente ao banco, mas também em dados agregados de várias outras fontes, muitos dos quais ela pode nem estar ciente. Em um sistema complexo, Maria pode não ser identificada apenas pelo que ela é, sabe ou possui, mas também por informações inferidas e compartilhadas por outras entidades.

Assim, soluções de identidade se tornam cada vez mais imbricadas, inclusive com a adição de novas funcionalidades a partir do papel de cada agente. Esses sistemas passam a ser compreendidos por molduras e camadas, implicando em novos desafios, inclusive em relação aos propósitos e às finalidades específicas do sistema de identidade construído.

3.2 Entidades envolvidas no sistema

A estrutura de um sistema de identidade refere-se à forma de gestão e interação entre os componentes e os atores do sistema. Essa estrutura pode variar a depender do contexto e das demandas que o sistema de identidade visa atender, impactando, inclusive, a forma de registro e de organização dos dados e das entidades envolvidas, e o nível de controle sobre a identidade.

Em uma estrutura **centralizada**, há apenas um único provedor para um sistema de identificação[40]. Essa entidade é responsável por toda a cadeia do sistema, inclusive pelas funções de checagem de identidade, emissão de credenciais, autenticação e armazenamento de dados.

Nesse caso, o próprio provedor é o único agente que oferece serviços com base na identidade que emite. Cada provedor de serviços fornece o identificador (por exemplo, nome de usuário) e a credencial correspondente (por exemplo, senha) aos clientes que desejam receber seus serviços[41]. Essa estrutura é comumente utiliza-

40 WANGHAM, Michelle et al. Capítulo 1. **Gerenciamento de Identidades Federadas**. 2010, p. 8. Disponível em: https://www.researchgate.net/publication/228401861_Gerenciamento_de_Identidades_Federadas. Acesso em: 28 jun. 2024.

41 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.

da em serviços de *login* em geral, como em uma rede social, um *e-commerce*, ou um banco, que em cada serviço a pessoa tem credenciais próprias.

> Um dos avanços de sistemas de identificação é a implementação de serviço de autenticação única, o *Single Sign-on* (SSO). Por meio desse serviço, o provedor da identidade permite às pessoas identificadas interagirem com outras entidades sem que necessitem realizar o processo de autenticação manual em cada uma dessas. Elas podem se valer das credenciais emitidas por uma entidade e reconhecidas por todas as outras, que as percebem enquanto forma de autenticação válida[42].

O elemento característico de uma estrutura centralizada é o fato de a autoridade central ter total controle sobre o sistema. Ela pode inclusive compartilhar as informações de identidade, bem como validá-las com terceiros, sem que as pessoas identificadas conhecessem esse compartilhamento[43]. Essa autoridade, enquanto entidade que conhece e expede a identidade, teria ferramentas suficientes para utilizar esses dados de forma autônoma.

Atualmente, a maior parte das identidades e dos dados relacionados está sob gerência dos provedores de identidade e não é controlada pela própria pessoa. Esse modelo centralizado, além de ser vulnerável a hackers e ao compartilhamento indevido de informações, impede que os usuários tenham total gerência sobre seus dados pessoais[44]. Foi nesse contexto que outras estruturas foram pensadas.

Uma estrutura **federada** envolve único provedor de identidade e um ou mais provedores de serviços, as partes confiantes. O provedor de identidade emite identificadores e as respectivas credenciais para a pessoa e os provedores de serviços dependem do provedor de identidade para autenticar o usuário e fornecer os atributos do usuário e seus valores aos provedores de serviços[45].

---

43 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, p. 38.

44 LEITE, Raquel Pereira; HENRIQUES, Marco Aurélio Amaral. **Análise de viabilidade de implantação de sistema de autenticação baseado em Identidades Digitais Federadas e Identidades Digitais Descentralizadas**. Campinas, p. 2. Disponível em: https://sol.sbc.org.br/index.php/sbseg_estendido/article/view/21714/21538. Acesso em: 28 jun. 2024.

45 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.

Para acessar qualquer serviço, as pessoas se autenticam no provedor de identidade e, uma vez autenticados, são redirecionados ao provedor de serviços para acessar o serviço. Depois que um usuário é autenticado no provedor de identidade, ele pode acessar serviços de todos os provedores de serviços que compartilham o mesmo provedor de identidade. O domínio de identidade compartilhada é conhecido como domínio de identidade federada e é criado quando uma noção de confiança é estabelecida entre o provedor de identidade e os provedores de serviços correspondentes.

Em regra, essa noção de confiança é resultado do estabelecimento de um contrato entre as entidades correspondentes. A descentralização também é resultado da robustez dos sistemas de identidade, com novos atores e funcionalidades, que interagem entre si.

Experiência de compra com base em identidade federada

Lucas decidiu comprar um novo laptop. Ele abriu seu navegador e acessou sua plataforma de compras online favorita, onde a experiência de compra é facilitada pelo modelo de identidade federada. Nessa plataforma, o Sistema de Contas da Plataforma de Compras atua como o Provedor de Identidade, enquanto o Serviço de Catálogo de Produtos, o Serviço de Gestão de Pedidos e o Serviço de Suporte ao Cliente são os Provedores de Serviço.

Acesso em: 28 jun. 2024.

Fazendo Login: Lucas clicou no botão de login na página inicial. Ele foi redirecionado para a página de login do Sistema de Contas da Plataforma de Compras, o Provedor de Identidade. Lucas inseriu seu e-mail e senha. A plataforma verificou suas credenciais e o autenticou, emitindo um token. Este token permitiria que Lucas acessasse todos os serviços integrados sem precisar fazer login novamente.

Navegando no Catálogo de Produtos: Com seu token, Lucas foi redirecionado de volta para o Serviço de Catálogo de Produtos, um dos Provedores de Serviço. Ele navegou por vários laptops, leu avaliações e comparou preços. Encontrando o laptop perfeito, ele o adicionou ao carrinho.

Fazendo um Pedido: Lucas então acessou o Serviço de Gestão de Pedidos, outro Provedor de Serviço, para concluir sua compra. Graças ao token emitido pelo Provedor de Identidade, ele foi automaticamente autenticado no Serviço de Gestão de Pedidos. Lucas revisou seu pedido, inseriu seus dados de envio e fez o pedido.

Precisando de Atendimento: Mais tarde, Lucas percebeu que tinha uma pergunta sobre seu pedido. Ele acessou o Serviço de Suporte ao Cliente, mais um Provedor de Serviço, através da plataforma. O serviço reconheceu seu token, e ele foi conectado a um agente de suporte sem precisar fazer login novamente. O agente respondeu suas perguntas, garantindo que Lucas se sentisse confiante sobre sua compra.

Esse caso mostra como Lucas conseguiu autenticar-se uma vez com o Provedor de Identidade (Sistema de Contas da Plataforma de Compras) e acessar vários serviços (Serviço de Catálogo de Produtos, Serviço de Gestão de Pedidos e Serviço de Suporte ao Cliente) de uma plataforma de compras online de forma fluida, aproveitando o modelo de identidade federada, em que há interação entre o provedor de identidade e os agentes confiantes, que provêem o serviço.

Diante das limitações dos sistemas centralizados e federados, especialmente em vista do papel da pessoa identificada, outras estruturas têm sido debatidas. Um exemplo é a estrutura de **identidade centrada na pessoa identificada**. Nesse modelo, vários provedores de serviço podem compartilhar um único provedor de identidade. Porém, não há necessidade de estabelecer uma noção de confiança entre as entidades.

Sempre que uma pessoa tenta acessar um provedor de serviço, ela é encaminhada para o provedor de identidade solicitado, onde se autentica. Em seguida, o provedor de identidade libera os dados de identidade do usuário para o provedor de serviço, onde uma decisão de autorização é tomada com base no perfil do usuário para conceder ou rejeitar a solicitação de acesso ao serviço. Com a ausência de qualquer noção de confiança entre os provedores de serviços, todas as entidades nesse modelo implementam o vínculo informado pelo provedor de identidade.

Confiança no provedor de identidade

Joana é uma paciente que precisa acessar diversos serviços de saúde, como consultas médicas, exames laboratoriais e farmácia. Cada um desses serviços é fornecido por uma organização diferente, mas todos compartilham o mesmo provedor de identidade, chamado SaúdeID.

Joana decide agendar uma consulta com seu médico através do portal de consultas online. Ao tentar acessar o portal, ela é redirecionada para o SaúdeID, onde já tinha cadastro prévio, e faz login utilizando suas credenciais (usuário e senha). Após a autenticação bem-sucedida, o SaúdeID libera os dados de identidade de Joana (como nome, data de nascimento, plano de saúde, histórico médico relevante) de acordo com um perfil específico, e envia essas informações de volta ao portal de consultas. O SaúdeID compartilha informações pessoais dos titulares a depender da entidade solicitante e do contexto que é feita a solicitação. O portal de consultas recebe os dados de Joana e verifica se ela tem o perfil necessário para acessar o serviço de agendamento de consultas. Com base nessas informações, o portal autoriza Joana a agendar sua consulta.

Posteriormente, Joana precisa marcar um exame de sangue. Ao acessar o site do laboratório, ela é novamente redirecionada para o SaúdeID para autenticação. Após o login, o SaúdeID libera os dados necessários ao laboratório, que autoriza Joana a marcar o exame.

Joana também precisa comprar medicamentos prescritos. Ao entrar no site da farmácia, ela é redirecionada para o SaúdeID para autenticação. Após o login, o SaúdeID libera os dados necessários (como a receita médica) para a farmácia, que então permite que Joana compre os medicamentos online.

Nesta estrutura, cada um dos serviços de saúde (portal de consultas, laboratório e farmácia) confia implicitamente no SaúdeID para fornecer dados precisos e válidos de identidade e perfis dos usuários. Não há necessidade de estabelecer relações de confiança explícita entre cada serviço de saúde, todos confiam que o SaúdeID está operando corretamente.

Outra estrutura é a de identidade **descentralizada**, também conhecida como identidade auto soberana. Nela, as pessoas têm poder sobre seus próprios dados de identidade e podem compartilhá-los seletivamente às partes confiáveis sem depender de uma autoridade central.

Essa estrutura pressupõe não apenas a interoperabilidade da identidade de uma pessoa em vários locais e provedores de serviço, com o consentimento do usuário, mas também o verdadeiro controle do usuário sobre essa identidade, criando uma autonomia para a pessoa. Para conseguir isso, uma identidade auto soberana deve ser transportável, ela não pode ficar presa a um provedor ou local, e ela deve permitir que a pessoa escolha quando deseja divulgar dados de identidade para um terceiro, quais dados deseja compartilhar, para qual entidade, e para qual finalidade[46].

Na estrutura descentralizada, uma vez que o usuário tenha consentido com o acesso, o verificador pode autenticar diretamente as identidades ou credenciais digitais na infraestrutura tecnológica - blockchain, por exemplo - sem envolver o provedor de identidade. Isso elimina a necessidade de o verificador interagir com o provedor sempre que a verificação for necessária. Isso é particularmente útil quando o provedor deixa de existir no momento da verificação[47].

Para concretizar esses elementos, os sistemas descentralizados geralmente utilizam tecnologias de blockchain, um tipo de registro distribuído (*distributed ledger*), para permitir a troca segura e ponto a ponto das credenciais verificáveis. Isso porque as características das estruturas são parecidas. O blockchain fornece essencialmente um domínio descentralizado que não é controlado por nenhuma entidade individual. Os dados armazenados em qualquer *blockchain* estão prontamente

---

46 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.

47 PUNIA, Swati, *et al.* **Mapping the Blockchain Ecosystem in India and Australia: Case Studies**. 2023, p. 14. Disponível em: https://ccgdelhi.s3.ap-south-1.amazonaws.com/uploads/final-blockchain-phase-2-report-for-printing-2023---pages-sequence-510.pdf Acesso em: 28 jun. 2024.

disponíveis (propriedade de disponibilidade) para qualquer entidade autorizada (propriedade de acesso)[48]. Diante dessas características, uma estrutura descentralizada de identidade está vinculada a ferramentas de registro distribuídas.

Apesar do registro distribuído ser um dos principais tópicos da estrutura descentralizada, essa solução também pode ser usada em outras estruturas, inclusive a centralizada ou federada, a depender da finalidade. Por exemplo, a tecnologia de blockchain está sendo utilizada para a expedição da CIN, mesmo existindo apenas uma autoridade que exerce papel de provedora de identidade[49]. Nesse caso, a blockchain auxilia as operações de consulta, inscrição e alteração de CPFs para evitar a alteração dos dados e a duplicidade de identidades para uma mesma pessoa.

Essa estrutura busca colocar as pessoas, em vez de autoridades de identificação, provedores ou partes confiáveis, no controle e no centro das transações de identidade. Nesse sistema, é possível que a checagem de identidade ocorra sem o compartilhamento do dado em si, mas apenas da confirmação que as partes confiantes devem checar. Assim, por exemplo, para checar se uma pessoa tem mais de 18 anos, a parte confiante não precisa conhecer a idade exata ou a data de nascimento da pessoa identificada, mas só se ela é tem mais de 18 anos.

Trential na Índia

A empresa desenvolveu e implementou um ecossistema de credenciais verificáveis baseado em blockchain que capacita os cidadãos a ter o controle sobre suas credenciais e permite o compartilhamento de dados de credenciais, preservando a privacidade.

A solução da Trential inclui um gerenciador de credenciais (um aplicativo para

48 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.

49 BRASIL. Serpro. **Governo começa a utilizar o blockchain na emissão da Carteira de Identidade Nacional**. 2023. Disponível em: https://www.serpro.gov.br/menu/noticias/noticias-2023/blockchain-emissao-cin. Acesso em: 28 jun. 2024.

que as organizações criem, gerenciem, emitam e verifiquem dados de identidade confiáveis) e uma carteira (uma maneira segura de os cidadãos receberem, armazenarem e compartilharem todas as suas credenciais digitais em um único aplicativo). A Trential implementou o blockchain para desenvolver um registro de dados imutável e verificável que contém metadados relacionados às credenciais. Isso garante a integridade das credenciais, tornando-as à prova de adulteração e permitindo o compartilhamento de provas de credenciais de forma intransferível.

Como parte da solução, foi criado um registro de diplomas de alunos da universidade IIT Kanpur, e esse banco de dados foi integrado ao ecossistema da Trential. Isso permitiu a verificação dos diplomas dos alunos por terceiros por meio de uma simples leitura de um código QR. Cada diploma é vinculado exclusivamente a suas credenciais no blockchain[50].

3.3 Finalidades do sistema

Outra moldura dos sistemas de identidade está relacionada a suas funções, que tradicionalmente são divididas em duas: uma finalidade fundacional e outra funcional.

Um sistema de identidade **fundacional**, ou legal, tem como objetivo prover uma identidade única e universal para as pessoas, ou seja, qualquer um poderia ser identificado em qualquer espaço por um elemento que só essa pessoa tem. Esse sistema é conhecido como fundacional porque é utilizado como base, fundação, por outros agentes para outros sistemas e finalidades. Ao mesmo tempo, esse sistema é legal, já que também é aquele reconhecido juridicamente por alguma norma ou regulamento como forma de garantir que uma pessoa é sujeito de direitos perante um Estado, uma jurisdição.

Como descrito no tópico anterior, a identidade legal é utilizada para finalidades oficiais de um Estado, de forma a ser um reconhecimento diretamente vinculado a um Estado que a expede. Ainda, em vista da sua centralidade para a garantia de direitos e deveres, um dos objetivos da ONU, previsto na Agenda 2030, é fornecer identidade legal para todas as pessoas.

---

50 PUNIA, Swati, *et al*. **Mapping the Blockchain Ecosystem in India and Australia: Case Studies**. 2023, p. 15. Disponível em: https://ccgdelhi.s3.ap-south-1.amazonaws.com/uploads/final-blockchain-phase-2-report-for-printing-2023---pages-sequence-510.pdf Acesso em: 28 jun. 2024.

Em regra, esses sistemas são formados por registros públicos como registros civis, identidades e registros populacionais, que são criados para fornecer identificação à população em geral para vários tipos de transações. Um sistema de identidade pode ser considerado fundacional na medida em que permite a uma pessoa provar quem ela é utilizando credenciais reconhecidas por lei ou regulamento como prova da sua identidade legal[51]. Como consequência, é comum que identidades fundacionais sejam desenvolvidas e implementadas pelo Poder Público de um país.

Possíveis razões para o desenvolvimento de sistemas de identidade

"Historicamente, o registro e identificação de pessoas pelo Estado ocorria para facilitar o recolhimento de impostos e para garantir que os benefícios do Estado fossem recebidos pelo cidadão. O controle da população a partir do uso de identificação diferiu ao longo do tempo, mas certo é que a demanda por documentos de identidade é um lugar comum no mundo moderno[52]. Especificamente no que diz respeito a sistemas de identidade civil digital, a perspectiva de economia política por detrás do desenvolvimento de uma indústria de segurança destaca o investimento em sistemas de identidade digital, após o atentado do 11 de setembro de 2001 nos EUA[53]. Além dessa visão de um sistema de identidade para preservação da segurança nacional, tem despontado mundialmente uma agenda para a disseminação de sistemas de identidade para desenvolvimento socioeconômico, especialmente com foco em países e regiões mais pobres do mundo, nos quais ainda existe uma porção importante de pessoas ainda sem registro civil"[54].

É a partir desse registro de identidades únicas e confiáveis que o sistema de identidade fundacional passa a poder ser o alicerce para a verificação segura de identidade para usuários do governo e do setor privado. Com base nesse sistema, as autoridades passam a entender pela integridade do processo de prova de identidade, além de permitir a identificar

51 WORLD BANK. **ID4D Practitioner's Guide: Version 1.0**. Washington: World Bank License, out. 2019, p. 12. Disponível em: https://documents1.worldbank.org/curated/en/248371559325561562/pdf/ID4D-Practitioner-s-Guide.pdf. Acesso em: 28 jan. 2024.

52 LYON, David. **Identifying citizens: ID Cards as Surveillance**. Cambridge: Polity Press, 2009.

53 LYON, David. **Identifying citizens: ID Cards as Surveillance**. Cambridge: Polity Press, 2009.

54 MARTIN, Aaron. **Aadhaar in a Box? Legitimizing Digital Identity in Times of Crisis**. Surveillance & Society, [s.l.], v.19, n.1, p. 104-108, 5 mar. 2021. Disponível em: https://doi.org/10.24908/ss.v19i1.14547. Acesso em: 10 mai. 2022.

duplicidades em outros sistemas de identidade, como por exemplo, um registro de transferência de renda ou folha de pagamento pública. A partir de um sistema fundacional, é possível reduzir os casos de fraude[55].

Nova Carteira de Identidade Nacional (CIN)

A CIN é o novo documento de identidade fundacional brasileiro. Ela tem como número único o CPF, em que, com um fluxo oficial de emissão e de dados de identificação em todo o país, seria suficiente para suspender o uso de informações divergentes na identificação do cidadão. Um dos desafios da CIN seria justamente enfrentar a fragmentação e insegurança dos sistemas de identificação civil, os diversos normativos legais e infralegais, a falta de um padrão nacional para verificação da pessoa. A CIN possui uma versão digital, que pode ser acessada pela plataforma gov.br[56].

Como consequência desse sistema fundacional, outros sistemas vão se acoplando sob o pressuposto de que a identidade fundacional é universal e acessível às pessoas. No entanto, esse entendimento chamada atenção para um risco relevante: a exclusão do acesso a serviços públicos de pessoas que não possuem qualquer documento de identidade.

Plataforma gov.br

Ainda sobre o caso do Brasil, a plataforma gov.br, vinculada a um sistema fundacional, evidencia esse risco. Essa plataforma "utiliza a BDICN para a autenticação de seus usuários a partir de um login único, de modo que os cidadãos precisam ter seus dados pessoais catalogados na BDICN para poderem acessar aos serviços públicos digitalizados via gov.br. Para tanto, é necessário que estes tenham algum documento de identificação, o que depende da emissão de

---

55 WORLD BANK. **ID4D Practitioner's Guide: Version 1.0**. Washington: World Bank License, out. 2019, p. 15. Disponível em: https://documents1.worldbank.org/curated/en/248371559325561562/pdf/ID4D-Practitioner-s-Guide.pdf. Acesso em: 28 jan. 2024.

56 BRASIL. Governo Digital. **Identificação do cidadão e carteira de identidade nacional**. Disponível em: https://www.gov.br/governodigital/pt-br/identidade/identificacao-do-cidadao-e-carteira-de-identidade-nacional. Acesso em: 28 jun. 2024.

uma certidão de nascimento - o "documento fundacional" brasileiro. Ficam excluídos do gov.br, portanto, aqueles que não possuem esse documento, sendo essa fatia da população mais numerosa nas regiões Norte e Nordeste. Como consequência, existe um risco iminente de exclusão de acesso a direitos e políticas públicas, como por exemplo os direitos sociais relativos ao trabalho e à seguridade social, como a impossibilidade de emitir a Carteira de Trabalho e Previdência Social (CTPS) e realizar a prova de vida junto ao Instituto Nacional do Seguro Social (INSS), ambos estabelecidos constitucionalmente como direitos sociais"[57].

Já um sistema de identidade **funcional** tem como objetivo expedir e validar credenciais utilizadas para autorizar o acesso a bens, direitos e serviços específicos, não gerais. Uma identidade funcional não se pretende universal, já que ela possui uma elegibilidade limitada a alguns setores ou propósitos, que se valem de processos de identificação para permitir acessos específicos.

Carteira Nacional de Habilitação no Brasil

Um exemplo comum é a emissão da Carteira Nacional de Habilitação pelo Departamento de Trânsito (Detran) de cada estado, que, na teoria, apenas certifica que uma pessoa está habilitada para dirigir um carro. O título de eleitor atesta a possibilidade do seu titular poder exercer seus direitos políticos, como participar das eleições de seu município, por exemplo. No entanto, pessoas menores de 16 anos não podem votar e, por isso, não possuem a identidade de eleitoras, no Brasil, o que torna esse documento não universal. O mesmo ocorre com a CNH, apenas pessoas habilitadas a dirigir veículos são identificáveis por esse sistema.

Nem toda pessoa identificada por uma identidade fundacional, que é universal, tem os acessos a serviços, produtos e direitos permitidos às pessoas que possuem identidade funcional. Ou seja, nem toda pessoa que possui uma identidade fundacional, como a nova CIN, pode dirigir um carro. Ao mesmo tempo, é comum que a identidade funcional tenha como base a fundacional, a exemplo da CNH, em que para emiti-la, é necessário possuir um documento de identidade anterior[58].

57 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, p. 99.

58 DISTRITO FEDERAL. Detran. **Obtenção de Carteira Nacional de Habilitação**. Disponível em: https://www.df.

Geralmente, o Poder Público cria diversos sistemas de identificação funcional para gerenciar a identificação, a autenticação e a autorização para setores ou casos de uso específicos, como votação, tributação, proteção social, viagens, entre outros. Esse é o caso do Brasil, em que temos outros tipos de identidade, com coleta de dados pessoais feita por autoridade específica, como o título de eleitor, gerida pela Justiça Eleitoral, a CNH, emitida pelos Detrans, e a carteira de trabalho e previdência social, documento emitido pelo Ministério do Trabalho.

Em alguns países, particularmente aqueles que não têm um sistema de identificação fundacional, as credenciais de identidade funcional são usadas como prova de identidade de fato para fins além do seu escopo original. Nos Estados Unidos, por exemplo, os números do seguro social e as carteiras de motorista são emitidos como prova de autorização para fins específicos, mas são usados como credenciais de uso geral. Entretanto, os sistemas de identificação funcional normalmente não são considerados sistemas de identificação legal, a menos que sejam oficialmente reconhecidos como servindo a esse propósito[59].

!

Mas como essas molduras operam juntas? Os órgãos governamentais, como autoridades de identificação, registradores civis, Ministérios de Tecnologia da Informação, Interior ou Justiça, geralmente são os principais fornecedores de sistemas básicos de identificação. Além disso, outros órgãos governamentais, por exemplo Ministérios da Proteção Social, Saúde, Educação, Justiça, Impostos, Alfândega, administração eleitoral, dependem desses sistemas básicos para interagir com as pessoas ou são eles próprios fornecedores de sistemas de identificação funcionais. Por fim, outros órgãos governamentais desempenham um papel regulador, supervisionam os sistemas de identificação e também podem estar envolvidos na implementação de componentes específicos ou na definição de padrões para tecnologia e formatos de dados[60].

gov.br/obtencao-de-carteira-nacional-de-habilitacao-cnh/. Acesso em: 28 jun. 2024.

59 WORLD BANK. **ID4D Practitioner's Guide: Version 1.0**. Washington: World Bank License, out. 2019, p. 12. Disponível em: https://documents1.worldbank.org/curated/en/248371559325561562/pdf/ID4D-Practitioner-s-Guide.pdf. Acesso em: 28 jan. 2024.

60 WORLD BANK. **ID4D Practitioner's Guide: Version 1.0**. Washington: World Bank License, out. 2019, p. 12. Disponível em: https://documents1.worldbank.org/curated/en/248371559325561562/pdf/ID4D-Practitioner-s-Guide.pdf. Acesso em: 28 jan. 2024.

Para além disso, sistemas de identidade podem se ocupar de **outras finalidades**, como a condução de processos de identificação para atender regulamentos de combate à lavagem de dinheiro (AML), *due diligence* do cliente (CDD), ou *know your customer* (KYC). É comum que nesses casos, em regra, o setor privado conduza processos de identificação funcional e forneça identificadores derivados diretamente de identidades fundacionais, ou seja, fontes oficiais reconhecidas pelo Poder Público[61].

Outros sistemas de identidade estão relacionados a processos de cadastramento em espaços físicos, redes sociais, lojas, e-mail e e-commerce, por exemplo. Em regra, as pessoas identificadas declaram alguns dados pessoais e a entidade identificadora coleta outras informações, como por exemplo fotos do rosto e a digital da pessoa. Esses sistemas não necessariamente se valem de uma identidade legal para funcionarem, mas é possível que haja a coleta deste identificador.

Porém, cada vez mais, esses sistemas de identidade, especialmente os que atendem a finalidades não fundacionais, tensionam os elementos de uma infraestrutura pública. Não necessariamente qualquer sistema de identidade digital é uma aplicação de IPD. Uma infraestrutura pública tem como objetivo fornecer acesso equitativo a serviços e infraestrutura digitais para todas as pessoas, atendendo um interesse público. Ao mesmo tempo, sistemas não fundacionais, especialmente aqueles operados por entidades vinculadas ao comércio, podem priorizar segmentos específicos de clientes ou ter restrições de acesso com base em seus modelos de negócios, além de identificar barreiras nos mecanismos de interoperabilidade, inclusive por questões concorrenciais.

Ainda, um aspecto fundamental da IPD é a capacidade de integrar vários serviços e componentes digitais em um ecossistema coeso e interoperável. Porém, os sistemas de identidade podem não ter a interoperabilidade ou a padronização necessárias para integrar uma IPD mais ampla.

No entanto, isso não significa que, de alguma forma, esses sistemas não apoiem a infraestrutura. Cada vez mais, para se garantir validade no processo de verificação de identidade, fundamental para se confiar na infraestrutura, o provedor de serviços, agente validador, utiliza múltiplos sistemas de identidade. A soma dessas várias identidades, que podem ter sido coletadas em contextos diversos, importam para tornar o processo redundante e robusto. É diante disso que se passa a falar

---

61 WORLD BANK. **ID4D Practitioner's Guide: Version 1.0**. Washington: World Bank License, out. 2019, p. 12. Disponível em: https://documents1.worldbank.org/curated/en/248371559325561562/pdf/ID4D-Practitioner-s-Guide.pdf. Acesso em: 28 jan. 2024.

em não apenas uma identidade, mas uma camada de identidades que juntas formam a identidade do usuário, assunto que será explorado no último tópico.

4 AS FINALIDADES E AS CAMADAS DAS IDENTIDADES EM UMA IPD

Esta cartilha sedimentou a ideia de que sistemas de identidade são fundamentais para o desenvolvimento de atividades corriqueiras. É por meio de uma identidade válida que as pessoas podem provar quem são de forma segura e, com isso, ter acesso a direitos, bens e serviços. Ainda, a partir de uma identidade fundacional, é possível que outros sistemas funcionais de identidade sejam criados para verificar algum atributo ou característica daquela pessoa já identificada, permitindo um conhecimento ainda mais específico sobre ela.

Essa agenda de identidade tem sido bastante impulsionada pela ONU, Banco Mundial e G20, por meio de diferentes abordagens. A ONU, com o objetivo 16.9, dos ODS, entende que todos os países devem prover uma identidade legal para as pessoas como uma forma de promover sociedades pacíficas e inclusivas para um desenvolvimento sustentável, proporcionar acesso à justiça e construir instituições eficazes, responsáveis e inclusivas em todos os níveis. Para que seja possível atingir esse objetivo, o Banco Mundial entende ser imprescindível o uso de registros que armazenam dados pessoais em formato digital e credenciais que dependem de mecanismos digitais, em vez de físicos, para autenticar a identidade das pessoas[62].

A partir das discussões sobre IPD, o G20 tem destacado essa infraestrutura como um conjunto de sistemas digitais compartilhados, desenvolvidos e utilizados pelos setores público e privado. Essa infraestrutura seria segura e resiliente, construída com base em padrões abertos, permitindo a prestação de serviços em escala[63]. Para a construção dessa IPD, o fluxo seguro de dados, inclusive pessoais e de identidade, é reconhecido como pressuposto para a construção dessa IPD.

No entanto, sistemas de identidade trazem diversos riscos, que podem variar de grau a depender das suas funcionalidades e molduras. Levando em consideração a maneira que são estruturados e implementados, esses sistemas podem se tornar ferramentas de exclusão, discriminação e vigilância[64]. É nesse sentido que a gover-

---

62 WORLD BANK. **World Development Report 2016: Digital Dividends**. Washington, 2016. Disponível em: https://documents1.worldbank.org/curated/en/896971468194972881/pdf/World-development-report-2016-digital-dividends.pdf. Acesso em: 28 jun. 2024. p. 194

63 G20. **G20 New Delhi Leaders' Declaration**. Índia: 10 set. 2023, p. 22. Disponível em: https://www.mea.gov.in/Images/CPV/G20-New-Delhi-Leaders-Declaration.pdf. Acesso em: 28 jun. 2024.

64 PRIVACY INTERNATIONAL. **The Sustainable Development Goals, Identity, and Privacy: Does their implementation risk human rights?** 2018. Disponível em: https://privacyinternational.org/long-read/2237/sustainable-de-

nança, um dos pilares da IPD, ganha destaque durante todo o processo de desenvolvimento das soluções de identidade.

Uma das preocupações levantadas por soluções de identidade é a dificuldade de se estabelecer uma adequada governança da infraestrutura e de suas aplicações, especialmente na arquitetura do fluxo de dados, fundamental para seu funcionamento. Como apresentado anteriormente, os sistemas de identidade possuem funções distintas e podem se organizar em molduras específicas, a depender dos agentes envolvidos, da estrutura do sistema ou das funcionalidades da identidade. Esses aspectos são traduzidos em uma maior complexidade para o funcionamento do sistema, em que há fluxo intenso de dados, para se atingir diferentes funções, além de um maior número de agentes envolvidos e pessoas identificáveis, e possíveis aplicações em diferentes contextos.

Essa complexificação ocorre a partir do desenho de novas molduras para os sistemas, mas também de novas camadas de identidade, ou seja, o processo de identificação não pode ser entendido apenas como a verificação da identidade de uma pessoa, mas como um processo de *disclosure* (*compartilhamento*) de informação entre uma pessoa identificada e um agente identificador. Esse *disclosure* pode ser apenas a validação de que ela é realmente quem diz ser (a partir do cruzamento de biometria, por exemplo), até algo mais complexo como se a transação financeira realizada por ela não traz indícios de ser uma fraude, com base em outras informações pessoais e não pessoais.

Essas funcionalidades trazem maiores imbricações não só do ponto de vista tecnológico, mas também de governança. O framework de IPD, em que essas diversas formas de identificação são interoperáveis e escaláveis, 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, tendo o potencial de amplificação dos riscos.

velopment-goals-identity-and-privacy-does-their-implementation-risk. Acesso em: 28 jun. 2024.

Inferências a partir dos elementos de identidade

João trabalha como segurança noturno de um edifício empresarial e, durante as horas livres, utiliza seu celular para acessar o extrato de sua conta bancária pelo aplicativo do banco. Em uma noite normal de trabalho, ele decide fazer uma transação financeira pelo aplicativo. Para que a transação seja feita com segurança, o banco utiliza algumas informações do dispositivo, do seu padrão de transações e outras informações pessoais para perceber algum indício de fraude. No entanto, esse mecanismo anti-fraude pode prejudicar grupos específicos, como o João, a partir da utilização de dados que buscam identificar a pessoa.

Se na definição de parâmetros indicadores de fraude, dados como geolocalização, local de residência (CEP) e modo de conexão a internet (rede móvel ou Wifi) forem usados e afetarem negativamente uma pessoa que está fazendo uma transação financeira (aumentando a chance daquela transação ser marcada como potencial fraude), pessoas em situação de vulnerabilidade podem ser desproporcionalmente afetadas. Pessoas que não possuem residência fixa, ou que trabalham em períodos noturnos, como João, ou que moram em regiões periféricas, e que possuem acesso à internet apenas por conexão móvel estarão mais propensas a serem identificadas como potenciais fraudadoras..

Por si só, esse aumento na propensão de identificação de fraude pode não ser um elemento que gere um impacto significativo para aquela pessoa. Contudo, compreendendo a identidade a partir de camadas interconectadas, esses atributos funcionais podem ser usados como parâmetros de outros processos de identificação, como em um processo de background check para emprego, ou processo de concessão de crédito, ou de verificação antifraude em programas de assistência governamental. Como consequência, essa marcação inicial do sistema antifraude bancário terá um efeito discriminatório em cascata em vários outros processos de identificação.

Nesse sentido, a interoperabilidade dos diferentes sistemas de identidade funcionais deve ser pensada de forma em que os **riscos não sejam transmitidos entre diferentes sistemas de identificação**. Para isso, um sistema participativo de governança e de auditoria figuram como elementos essenciais em um arranjo de identidade digital no contexto de infraestrutura pública digital.

O processo de identidade conduzido em camadas é justamente a integração de múltiplos sistemas de identidade com níveis próprios de segurança e privacidade. Essas camadas podem incluir identidades digitais básicas para acesso a serviços públicos gerais, bem como identidades mais avançadas e seguras para transações financeiras ou acesso a informações sensíveis ou comportamentais. Assim, a depender dos objetivos do sistema, aquilo que antes eram as molduras da identidade, passam a ser entendidas como camadas e essas passam a ser aplicáveis de forma conjunta.

Camadas de uma identidade com informações saúde

1. 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 expição da carteira de identidade.

2. 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.

3. Ao perder seu emprego, 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.

4. 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, 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.

5 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.

6 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.

A interoperabilidade de informações entre as diferentes camadas que compõem sistemas de identificação podem amplificar situações de discriminação em populações vulnerabilizadas e criar novas formas de discriminação. Portanto, ao se avaliar os riscos de um sistema de identidade em um contexto de IPD, deve-se analisar tanto os riscos próprios da digitalização da identidade, mas também riscos que emergem a partir da interoperabilidade e compartilhamento facilitado de dados em uma mesma infraestrutura.

Identidades digitais passam a ser formadas pela junção de camadas, de forma que o resultado final não é apenas a junção de sistemas isolados dedicados a contextos específicos, mas vínculos e inferências entre esses sistemas. A junção desses dois contextos geradores de risco pode ter consequências que não são meramente a soma dos riscos iniciais. Um exemplo disso está na camada 6, em que uma nova discriminação surge. A incapacidade do usuário se autenticar corretamente (um risco

típico de sistemas de identidade digital) ocorre em virtude da interoperabilidade e do compartilhamento excessivo de dados nessa infraestrutura (um risco típico de sistemas de infraestrutura pública digital).

O elemento contextual no desenvolvimento e no uso de sistemas de identidade não pode ser ignorado, diante da concretização dos princípios de proteção de dados. Elementos de identidade percebidos em contextos isolados estão sendo comunicados a outras camadas de identidade, o que pode dificultar o controle e a gestão dessas identidades feita pelo titular.

Além disso, informações comportamentais passaram a compor a identidade. Ela não é apenas formada por informações que uma pessoa registra sobre ela mesma, mas também por informações que emergem do seu comportamento. Metadados e registros, além de outras formas de dados observados, são gerados a partir de cada interação da pessoa identificada.

Os crescentes estoques de dados que as empresas e os governos mantêm sobre indivíduos e grupos agora são gerados automaticamente a partir do comportamento humano[65]. Sem as pessoas saberem, seus hábitos, preferências e escolhas são cada vez mais rastreáveis e passam a compor essa identidade.

Porém, a convergência dessas identidades, ou ao menos de alguns de seus atributos, em um sistema digital pode criar novos desafios para as pessoas identificadas, principalmente diante da capacidade delas desenvolverem sua personalidade, conhecerem a circulação das suas informações de identidade e exercerem sua autonomia.

Existe um risco eminente das pessoas estarem sob constante vigilância por sistemas que as identificam e somam camadas a identidade delas a partir de dados observados ou informados em um determinado contexto. Nesse cenário, mesmo para realizar uma atividade corriqueira em que a validação de identidade não é necessária, sistemas de identificação são utilizados para monitorar o comportamento das pessoas. Para além da vigilância e falta de autonomia, a forma de percepção da identidade também é um risco, já que todos os elementos rastreáveis de um pessoa passam a ser classificáveis, mesmo que não reconhecidos enquanto categorias válidas pelo sistema.

---

65 PRIVACY INTERNATIONAL. **Identities under our control**. Disponível em: https://privacyinternational.org/taxonomy/term/487. Acesso em: 28 jun. 2024.

Classificação de elementos de identidade

Júlia é uma pessoa não binária e está utilizando um sistema de identidade digital para ela acessar um serviço público O sistema solicita que ela se declare enquanto mulher ou homem, mas ela não se encaixa em nenhuma das categorias. Ao forçar a escolha entre manter a identidade completa ou acessar os serviços básicos, o sistema prejudica a capacidade da pessoa de navegar no mundo com autonomia e dignidade. Essas restrições artificiais marginalizam as pessoas, impedem sua participação na sociedade e as classificam ainda mais como "inválidas". Elas também induzem para uma coleta de dados que normalmente não são necessários para que o sistema funcione adequadamente[66].

!

Em um sentido mais amplo e complexo, identidade não é apenas um conjunto de dados biométricos e biográficos. Ela é formada a partir de uma narrativa construída tanto pela pessoa identificada, quanto por terceiros que interagem e percebem essa pessoa. "A construção da identidade pessoal envolve um constante processo de seleção e interpretação de informações pessoais, ensejando uma disputa entre diferentes narrativas das quais emerge a identidade"[67]. Como consequência, a depender das informações conhecidas e da capacidade de autodeterminação, a identificação digital passa a impactar as formas de ser de uma pessoa.

Ainda, a falta de governança nos dados utilizados para sistemas de identidade também pode acarretar em riscos para os direitos das pessoas acessarem serviços essenciais. A depender de como estruturados, é possível que sistemas de identidade funcionem como barreiras para as pessoas mais necessitadas. Uma pessoa pode ser impedida de acessar serviços por meio do sistema digital porque não tem acesso significativo à tecnologia, porque tem atributos ou experiências específicas

---

66 ACCESS NOW. **The Digital Identity Toolkit**. 2023. Disponível em: https://www.accessnow.org/guide/digital-id-toolkit/#mandatory-use. Acesso em: 28 jun. 2024.

67 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. 41. 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.

que a impedem de interagir facilmente com o sistema ou porque o sistema exacerba os modelos existentes de exclusão ou privação de direitos[68].

Os danos imediatos e agravados pela negação de acesso a serviços essenciais, como serviços bancários, de telecomunicação, energia, água, moradia, saúde ou educação, são quase incomensuráveis. As pessoas passam a estar mais vulneráveis a violações de direitos e abusos a partir da digitalização da identidade e do consequente tratamento desses dados.

A governança desses sistemas é fundamental durante todo o processo de desenvolvimento e implementação, de forma que uma estrutura pouco responsiva coloca o próprio sistema em risco. Ao projetar um sistema de identificação, é necessário que se observe de que forma ele será mantido e aprimorado ao longo do tempo, já que é comum que certos desafios sejam percebidos apenas com o uso do sistema. Logo, não é suficiente que sejam desenvolvidas ferramentas para que o sistema seja implementável. São necessários recursos básicos para mantê-lo funcionando adequadamente, sem que haja interrupções significativas no acesso e ele possa ser aprimorado.

Em vista desses riscos, os sistemas de identidade devem:

- Implementar a proteção de dados como princípio fundamental, exigindo a adoção de abordagens de transparência, especificação de propósito e finalidade e regras de compartilhamento de dados, buscando sempre a minimização desse compartilhamento;
- Buscar abordagens que priorizem o poder de agência das pessoas[69], garantindo sempre o direito à explicação e revisão de decisões tomadas a seu respeito;
- Prevenir a agregação de dados em uma única base centralizada ou a retenção de dados desnecessários, limitando a coleta e o uso de dados pessoais para proteger as pessoas contra o uso indevido de dados;

---

68 ACCESS NOW. **The Digital Identity Toolkit**. 2023. Disponível em: https://www.accessnow.org/guide/digital-id-toolkit/#mandatory-use. Acesso em: 28 jun. 2024.

69 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. 41. 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.

- Introduzir arranjos robustos para garantir que o compartilhamento de atributos e credenciais ocorra de maneira segura e rastreável, além de que os dados sejam precisos, completos, mantidos atualizados e relevantes;
- Garantir ferramentas de prestação de contas dos agentes envolvidos no desenvolvimento dos sistemas, para que eles se responsabilizem pelas práticas, especialmente as que impactam grupos vulnerabilizados;
- Possuir sistemas de governança participativa desde a concepção, garantindo a participação efetiva dos diversos atores interessados, especialmente a sociedade civil e grupos vulnerabilizados que podem ser afetados por sistemas de identidade digital.

Soluções de identidade digitais, enquanto uma das aplicações de IPD, devem observar os pressupostos de uma aplicação baseada em tecnologias abertas e interoperáveis e desenvolvidas a partir de uma governança robusta e com participação multissetorial. Ainda, uma solução de identidade digital deve ser desenvolvida em observância ao interesse público, aos direitos humanos e aos valores democráticos. Esse é pressuposto para garantir-se que a aplicação de identidade estará em conformidade com os parâmetros de uma IPD. Os riscos advindos das aplicações concretas de identidade devem ser trabalhados com base nesses pilares para que seja possível endereçá-los a partir de suas complexidades.

DataPrivacyBR Research

APOIO
ripple