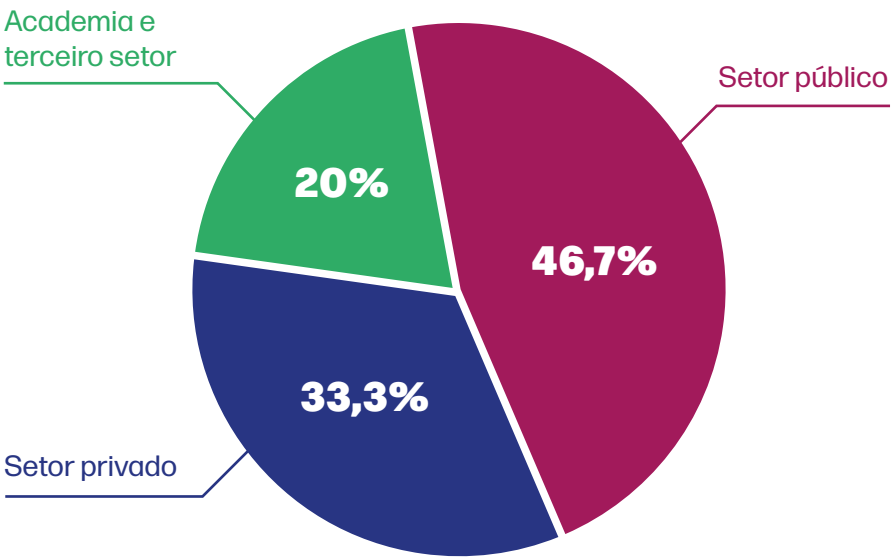
06.
APÊNDICE

6 Apêndice

6.1. Digestão das entrevistas

Entre fevereiro e maio de 2024, a Data Privacy conduziu 15 entrevistas com representantes do setor público, especialmente com representantes da Secretaria de Governo Digital, do Banco Central, do Serpro, além de outros órgãos. Também foram ouvidas empresas do setor privado que atuam no setor de identidades, como a Incognia, Único, entre outras. Do terceiro setor, foram ouvidos representantes da Digital ID CSO Coalition e da Aapti. Também foram entrevistados doutorandos representantes da academia.

Durante essas entrevistas, foram coletadas referências bibliográficas citadas pelos entrevistados, além de registros de temas de destaque na intersecção entre IPD e identidade digital. As entrevistas foram realizadas por videoconferência, não gravadas e semi-estruturadas, isso porque havia um roteiro que variava de acordo com o setor entrevistado e com os enfoques temáticos do entrevistado a partir das perguntas que conduziram a entrevista. A seguir, a Data disponibilizou um gráfico com a distribuição dos entrevistados por setor e um exemplo de roteiro, que poderia variar de acordo com o setor entrevistado e com as respostas da entrevista.



2. Privado

- O que você entende por uma identidade digital? São processos apenas de identificação ou de autenticação e autorização também?
- Quais as aplicações de identidade digital você vislumbra no curto e no longo prazo? Aplicações que já existem e que podem existir. Quais setores estão impactados?
- Quais problemas essa ferramenta pode solucionar?
- Qual o diferencial da solução da de identidade digital privada frente à identidade digital pública (Gov.br)? A nova identidade nacional civil impacta as soluções privadas?
- Como você enxerga que o setor privado pode se "acoplar" ou contribuir para infraestrutura pública digital que está sendo desenvolvida pelo Poder Público?
- Quais os riscos do desenvolvimento de uma identidade digital para as pessoas? Existem riscos como vigilância e uso secundário?
- Quais ferramentas e sistemas de governança podem ser pensados e implementados para evitar esses riscos?
- Qual o papel da tecnologia de blockchain no desenvolvimento de uma identidade digital? Ela é fundamental?
- Qual o papel da biometria para o estabelecimento de uma identidade digital?
- Atualmente, você conhece ferramentas que permitem a auditoria da estrutura de identidade digital por entes terceiros, como a sociedade civil, para mapear e mitigar possíveis riscos?

Após essa rodada de entrevistas, os seguintes pontos foram frequentemente abordados pelos entrevistados, mesmo que de forma divergente:

▪ Identidade e IPD

Em geral, os entrevistados indicaram que identidade é um termo com diversos significados diferentes e complementares. Ela visa garantir que uma pessoa é quem ela diz ser a partir da apresentação e validação de credenciais emitidas por um terceiro, seja Poder Público, seja entidades privadas. A identidade é resultado de uma representação composta por dados biométricos, características biológicas, e outros comportamentos mensuráveis.

Soluções de identidade digital estão sendo pensadas tendo em vista que a sociedade na era digital transformou sua forma de existir, e o governo deve se posicionar frente a essas novas necessidades, diante de valores como a conveniência, transparência, segurança e eficiência.

Para um grupo de entrevistados, o Gov.br é uma identidade digital, o que não implica na unificação de bases de dados, cada gestor continua gerindo as suas próprias bases de dados. A ideia inicial do Gov.br era autenticar e unificar a forma de acesso digital de pessoas já identificadas, mas, com a experiência, outros problemas foram percebidos como solucionáveis a partir da infraestrutura do Gov.br, como o desenvolvimento de uma assinatura eletrônica.

Para um segundo grupo de entrevistados, a identidade é definida pelas suas funções em casos concretos, por isso existem identidades para exercer direitos, atender obrigações legais de Know Your Client, prevenir lavagem de dinheiro e o terrorismo, detectar fraude, realizar log-in em outras entidades, etc.

▪ Biometria

Para um grupo de entrevistados, senhas não são mais uma prática corrente para validar as credenciais apresentadas por uma pessoa, por isso passou-se a usar vários tipos de biometria, como a facial e a comportamental de localização de um device. Assim, a biometria seria a forma menos invasiva de identificar uma pessoa de forma única.

No entanto, outro grupo de entrevistados destacou casos de falha no reconhecimento facial por diferença entre os rostos reais e os rostos usados para treinamento da ferramenta, além da falta de acessibilidade para grupos específicos e para todos os tipos de dispositivos. Essas questões são ainda mais agravadas diante da falta de juízo de necessidade no uso de biometria, o que faz com que haja uma coleta excessiva desse dado, além da falta de transparência e finalidade específica no seu uso.

Esse grupo também destacou os desafios que serão enfrentados na falsificação de biometrias com o uso de aplicações de inteligência artificial, como o caso das deepfakes.

▪ Responsabilidades

Para um grupo de entrevistados, cabe ao poder público desenvolver soluções de identidade fundacional, ele assume papel de protagonismo no desenvolvimento de IPD e identidade digital. Institutos eleitorais e de identificação civil são a base da identidade. Ao mesmo tempo, no governo, há uma oscilação no nível de governança e prioridade que dê sustentabilidade e continuidade às iniciativas digitais.

É possível identificar silos entre as bases de dados do Poder Público, de forma a causar um prejuízo para desenvolvimento de uma IPD, já que falta a definição de um caminho único para o seu desenho. Os projetos paralelos de várias entidades não necessariamente convergem e dialogam para uma solução comum.

Um segundo grupo de entrevistados indica que o ecossistema de identidade não deve ser gerido apenas por um único player. Existe uma dificuldade técnica para manter todo o sistema funcionando, por isso o Poder Público deve assumir posições estratégicas, mas não todas. Nesse sentido, é provável que a função principal do Poder Público seja a manutenção da camada fundacional. A partir disso, o mercado privado explora usos e construção de novas camadas.

▪ Riscos de sistemas de identidade

De forma geral, os entrevistados indicam que soluções de identidade evidenciam um desafio de exclusão do acesso ao Estado a partir de soluções não inclusivas que não comportam todas as pessoas, seja por questões de logística, burocra-

cia, falta de direcionamento às necessidades de determinados grupos ou mesmo pela falta de procedimentos definidos para inclusão de pessoas com sem status legal regular. Assim, uma das barreiras desses sistemas é a falta de letramento digital da população e dos próprios entes que compõem o ecossistema de identidade do Brasil.

Ainda, há uma barreira para viabilizar o compartilhamento de dados pessoais para garantir a minimização desse compartilhamento e também a autonomia dos cidadãos. É possível que haja algum nível de integração com o setor privado quanto às soluções de identidade para garantir-se a sustentabilidade da aplicação, por isso modelos de validação de dados, não de compartilhamento, podem ser possíveis soluções. Além do próprio risco de compartilhamento inadequado de dados, deve-se enfrentar o risco do uso secundário ilegítimo.

Para um segundo grupo de entrevistados, soluções de autenticação de identidade podem apresentar um risco de vigilância e discriminação de usuários que possuem determinados compartamentos, isso porque as pessoas passam a serem identificadas em diversos momentos da sua experiência no digital e passam a formar um padrão entendido como adequado, mas que pode não ser generalizável.

Ainda, a depender de como esses sistemas foram implementados, é possível que seja necessário que uma pessoa se identifique mesmo em serviços em que a identificação não é relevante. Assim, pessoas que não foram identificadas passam a ter uma experiência ainda mais limitada em acessar serviços e direitos, já que perdem acesso a serviços que antes tinham.

Outro risco no desenvolvimento de sistemas de identidade é a falta de interesse público nas soluções criadas a partir dela. Há um risco de que uma política pública de identidade passe a atender finalidade de mercado com riscos não mapeados, sem o devido estabelecimento de salvaguardas e práticas de governança.

A tecnologia possui funcionalidades fixas, que divergem da pluralidade de formas de existir das pessoas. A tecnologia funciona a partir de uma lógica de classificação e ordenação que é contrária à forma fluida do ser humano, suas mudanças e evoluções. Ainda, não seria possível mapear todos os riscos desses sistemas de identidade, tendo em vista o caráter inovador e disruptivo deles.

▪ Práticas de governança e padronização

Segundo um grupo de entrevistados, para que qualquer solução de identidade prospere, é necessário desenvolver ferramentas de governança do tema em diferentes agentes, em vista da complexidade de atores no ecossistema de identidade.

Para um segundo grupo de entrevistados, ferramentas de zero-knowledge são úteis e seguras para que processos de autenticação sejam conduzidos sem precisar compartilhar os dados pessoais. Nesse cenário, há menor fluxo de dados pessoais, mas há maior fluxo de validações, em que a validação é conduzida por um ente que não o emissor da identidade.

Ainda, mecanismos de controle de acesso, hash dos identificadores, prazos de retenção bem definidos e um programa de conformidade à LGPD são pertinentes para garantir que o sistema de identidade seja adequado para os direitos de proteção de dados.

Para um terceiro grupo de entrevistados, a governança desses sistemas deve incluir medidas de educação e prestação de contas, em que os cidadãos e a sociedade civil entenda a tecnologia, seus riscos e implicações, além identificar os agentes responsáveis pela funcionalidades da infraestrutura para que possam atuar de forma colaborativa. Nesse sentido, a falta de respaldo jurídico para governança participativa dos dados deve ser endereçada no desenvolvimento de sistemas de identidade em uma IPD.

Para um quarto grupo de entrevistados, o maior desafio de sistemas de identidade como IPD é a definição de padrões para que a identidade possa circular e ser validada em diferentes aplicações. Segundo esse grupo, a padronização deve ser uma preocupação do Poder Público, mais do que fornecer a infraestrutura em si, já que com a definição de padrões, o privado consegue se acoplar. Porém, esse tema levanta questões concorrenciais e de concentração de mercado que ainda não foram suficientemente alinhadas.

▪ Descentralização e Blockchain

Em regra, os entrevistados apresentaram opinião de que aplicações de identidade devem objetivar estruturas descentralizadas para dar autonomia para o cida-

dão. Estruturas centralizadas poderiam potencializar vulnerabilidades de segurança e vigilância dos identificados.

Com isso, modelos descentralizados poderiam promover maior autonomia para o identificado, porém aumentar autonomia também significa aumentar responsabilidades desse agente no uso e gestão de sua identidade. Os grandes benefícios da blockchain seriam a validação em cadeia e a confiança, já que é por criptografia que se valida as informações e isso impede que terceiros mudem as informações.

Para um grupo de entrevistados, esses temas de autonomia e descentralização estão direcionados para uma visão econômica da privacidade como apresentado no Projeto de Lei Complementar 234/2023, que dispõe sobre o Ecossistema Brasileiro de Monetização de Dados.

Um segundo grupo de entrevistados destacou a experiência da União Europeia em apresentar soluções descentralizadas para atender o mercado digital comum europeu. Esse modelo de identidade passa a estar dentro da blockchain, acabando com a necessidade de existência de vários atores, além da claim para validar a identidade passar a estar na própria cadeia de registros. Sobre soluções de blockchain, esse grupo indica que existem ecossistemas baseados em blockchains, que estão mais avançados, mas também existem outros que estão se baseando nas primitivas criptográficas. Por isso, a blockchain não é a única solução para descentralizar.

Um terceiro grupo indica que ainda não está claro como usar blockchain para verificação de identidade, principalmente do seu impacto para os direitos das pessoas, além de definições procedimentais, como quem vai ter acesso à ledger.

Um outro grupo de entrevistados afirma que a descentralização leva a um modelo de menor armazenamento de informações, mudando a lógica de quanto mais dados pessoais melhor para um modelo de validação. Isso exige uma mudança nos modelos de negócios de vários atores do setor privado, que hoje é de super acúmulo de informações para gerar diferencial competitivo e permitir um uso qualificado dos dados. Ainda, os benefícios de um modelo descentralizado ainda não são suficientemente entendidos e difundidos.

6.2. Digestão da trilha de "Identidade Digital" no evento "Horizontes comuns"

Em 30 de abril de 2024, a Data Privacy realizou o evento "Horizontes Comuns: o papel da infraestrutura pública digital em finanças, identidade e justiça climática", na sede da Dataprev, em Brasília. O evento funcionou como catalisador do debate sobre "infraestrutura pública digital" (IPD), um dos pilares da transformação digital inclusiva do Brasil. Durante a parte da manhã, foram conduzidos dois painéis sobre IPD e na parte da tarde os participantes se dividiram em 3 trilhas dedicadas aos temas de identidade digital, financeiro e justiça climática.

A trilha de identidade digital contou com a participação de, em média, 15 especialistas de diferentes setores, privado, público, academia e terceiro setor, que atuam com temas e aplicações de identidade. Esses profissionais se dividiram em três grupos para permitir o aprofundamento das discussões orientadas por perguntas produzidas pela Data Privacy Brasil. As perguntas foram organizadas em três blocos: o primeiro sobre as iniciativas de identidade, o segundo sobre a definição de IPD e, por fim, sobre os impactos da identidade como aplicação na IPD.

WORKSHOP TRILHA IDENTIDADE DIGITAL

Bloco I - Mapeando iniciativas de ID

1. Quais são as iniciativas de Identidade Digital que você conhece?
2. Essas iniciativas são Identidade Digital?
    - 2.1. CNH Digital
    - 2.2 Conta Gov.br
    - 2.3 Conta em rede social
    - 2.4 Conta em plataforma que pode ser utilizada em outros sites, como a Google e Facebook
    - 2.5 Conta em Instituição Financeira
3. Para quais finalidades essas identidades existem?
4. A identidade tem que ser única, ou seja, uma pessoa não pode ter mais de uma identidade expedida pela mesma organização?
5. Qual o papel da biometria para a identidade digital?

Bloco II - Revisando a definição da IPD

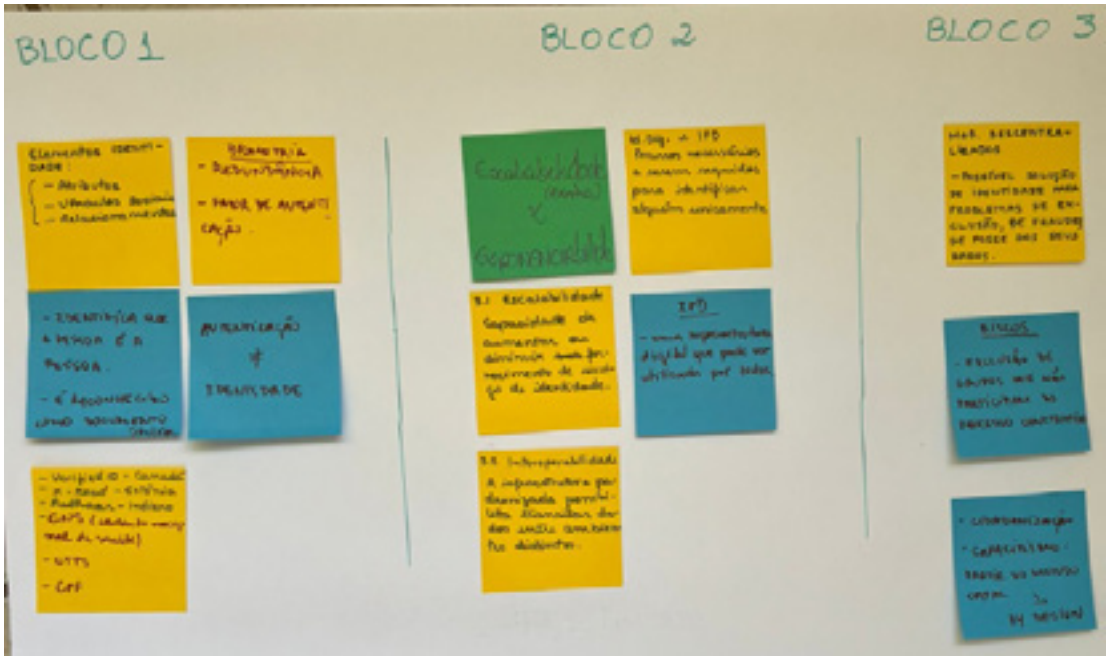
1. O que este grupo entende por "Infraestrutura Pública Digital"?
2. E na identidade digital, o que esse termo significa?
3. Qual a visão do grupo sobre a relação entre IPD e ID a partir dos seguintes temas?
    - 3.1 Escalabilidade
    - 3.2 Interoperabilidade
    - 3.3 Padrões abertos
    - 3.4 Valor público, bem comum e interesse público
    - 3.5 Participação
    - 3.6 Inclusão
    - 3.7 Governança
    - 3.8 Transparência
    - 3.9 Responsabilização

Bloco III - Identificando os impactos da ID

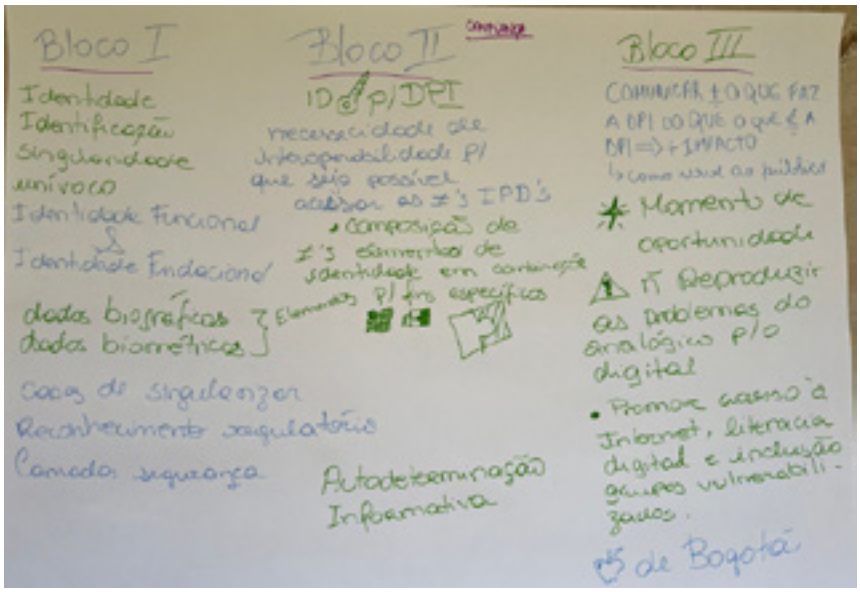
1. Qual a visão do grupo sobre a relação dos seguintes temas com ID?
    - 1.1 Compartilhamento de dados e cruzamento de dados
    - 1.2 Modelos descentralizados que buscam autonomia
2. Qual a visão do grupo sobre os riscos e limites da ID para o desenvolvimento da IPD em relação aos seguintes temas?
    - 2.1 Acesso à internet e literacia digital
    - 2.2 Abertura da tecnologia e interoperabilidade
    - 2.3 Sistema de governança resiliente
    - 2.4 Barreiras econômicas, regulatórias e institucionais
    - 2.5 Grupos vulnerabilizados
3. Quais medidas de governança são aplicáveis ao contexto de ID como IPD? Qual a visão do grupo a respeito das seguintes medidas?
    - 3.1 Princípios aplicáveis no desenvolvimento de uma IPD
    - 3.2 Atores participantes e estruturas habilitadoras pelo setor público, setor privado, comunidade acadêmica e sociedade civil (quem financia, quem regula, quem coordena, quem desenvolve, que define padrões, quem participa do design, quem acompanha, quem recomenda melhorias)
    - 3.3 Corpo decisório diverso e representativo da população durante o desenvolvimento das aplicações, inclusive após a implementação das aplicações
    - 3.4 Relatório, *assessments* e documentos que mensuram impacto da ID públicos e acessíveis
    - 3.5 Responsabilização e *accountability* dos atores
4. Quais os principais consensos e dissensos do grupo?

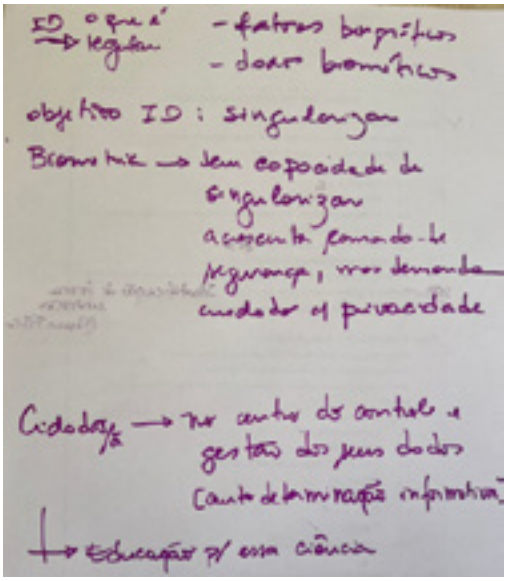
Em um primeiro momento, os grupos debateram e reagiram às provocações dos três blocos, durante cerca de 1 hora. Para que os participantes pudessem organizar suas ideias e formar consensos no grupo, foram disponibilizadas cartolinas, post-its e canetas para registrarem suas impressões, além do debate oral. Os seguintes documentos foram produzidos:

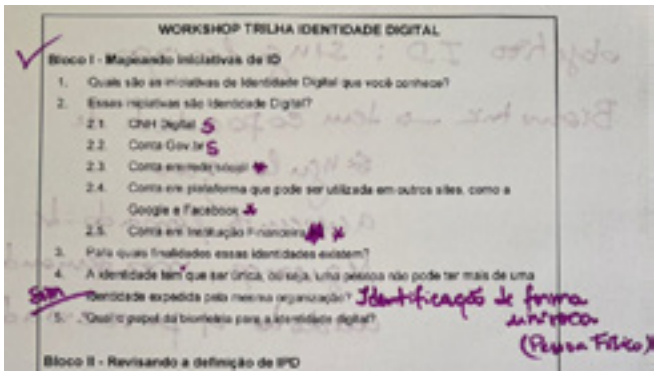
GRUPO 1



GRUPO 2







WORKSHOP TRILHA IDENTIDADE DIGITAL

Bloco I - Mapeando Iniciativas de ID

1. Quais são as iniciativas de Identidade Digital que você conhece?
2. Essas iniciativas são Identidade Digital?
   - 2.1. CNH Digital
   - 2.2. Conta Gov.br
   - 2.3. Conta em rede social
   - 2.4. Conta em plataforma que pode ser utilizada em outros sites, como a Google e Facebook
   - 2.5. Conta em instituição financeira
3. Para quais finalidades essas identidades existem?
4. A identidade tem que ser única, ou seja, uma pessoa não pode ter mais de uma identidade expedida pela mesma organização?
5. Qual o papel da biometria para a identidade digital?

Identificação de forma única (Pessoa Física)

Bloco II - Revisando a definição de IPD

GRUPO 3

Após esse momento, os grupos apresentaram para os outros participantes da trilha as interpretações e possíveis respostas que tiveram às perguntas orientadoras. Assim, foi possível compartilhar as conclusões dos grupos com a trilha, de forma a se comparar as discussões e se perceber as divergências e convergências entre os grupos.

No **primeiro bloco** de perguntas, a respeito das iniciativas de ID, os grupos se debruçaram sobre a finalidade da identidade, seu caráter único, a função da biometria e sobre se alguns exemplos eram identidades digitais ou não. O primeiro grupo destacou a diferença entre autenticação e identidade, sendo este composto por atributos que tornam uma pessoa única, como o nome, a data de nascimento, os vínculos sociais e os relacionamentos que possui, como o lugar que trabalha ou estuda, o estado civil, a filiação e outras pessoas que se relacionam. Para o grupo, a identidade é um documento reconhecido oficialmente, como a CTPS e o CPF, ou seja, a sua confiabilidade deve ser distribuída, a identidade deve ser aceita por todos os agentes que se valem dela. Por isso, soluções como o login Gov.br não seriam identidade por não necessariamente serem reconhecidas em todos os espaços.

O segundo grupo diferenciou conceitos de identificação e identidade, o primeiro vinculado a um processo de acessar espaços com login e senha, como um processo de autenticação. Já a identidade é capaz de singularizar, identificar univocamente uma pessoa frente a um órgão, uma entidade. Essa identidade é composta por elementos biográficos e biométricos, de forma que a privacidade deve ser pensada desde o início do planejamento e da implementação das tecnologias envolvidas no desenvolvimento de um sistema de identidade. Assim, a CNH Digital, o login Gov.br seriam identidades digitais, mas contas de redes sociais e soluções de single sign-on fornecidas por elas não seriam identidade, mas formas de identificação.

Para o grupo, a identidade pode ser classificada em funcional ou fundacional, esta sendo uma primeira manifestação em que outras identidades se apoiam, como a relação entre a carteira de identidade nacional e a CNH ou carteiras profissionais, a exemplo da OAB e do Crea, que dão acesso a funções específicas. Diante disso, a identidade deve contar com camadas de segurança e ser reconhecida por uma regulação.

O terceiro grupo discutiu se para ser considerado identidade digital é necessário ter capilaridade, ser aceito em vários ambientes e ser autenticado. Assim, o login do Gov.br, certificados digitais, contas em redes com soluções de single sign-on, e contas em instituições bancárias seriam soluções de identidade digital, mas a CNH Digital e as contas em rede social não seriam.

Com relação à definição de IPD, objeto do **segundo bloco**, os participantes foram provocados a identificar quais elementos são imprescindíveis em uma infraestrutura e, por isso, definem a própria IPD. Apesar de os membros das trilhas não necessariamente conhecerem os sentidos de uma IPD, esse tema foi desenvolvido nos painéis anteriores, de forma a permitir que os participantes se aprofundassem sobre os elementos indispensáveis ou não à infraestrutura.

Para o primeiro grupo, IPD seria uma infraestrutura digital que pode ser utilizada por todos, de forma a viabilizar os recursos necessários para identificar alguém unicamente. Já o segundo grupo destacou o papel da interoperabilidade como requisito da IPD, seria fundamental que diferentes identidades acessassem as diferentes infraestruturas. A identidade deve poder circular entre as IPD, não sendo essas barreiras para a usabilidade e para o fluxo de dados de identidade.

O terceiro grupo entende que IPD é similar a conceitos de governo como plataforma, sendo uma nova roupagem para um tema mais sedimentado. Assim, seria necessário perceber de que forma conceitos de IPD dialogam com a realidade brasileira, a fim de que se localize geopoliticamente a discussão. Para o grupo, o Estado seria a autoridade responsável pela identidade das pessoas, mas também foram levantadas questões sobre a emissão da identidade como forma de poder centralizado em um agente. Elementos como escalabilidade, interoperabilidade e padrões abertos seriam essenciais para uma IPD.

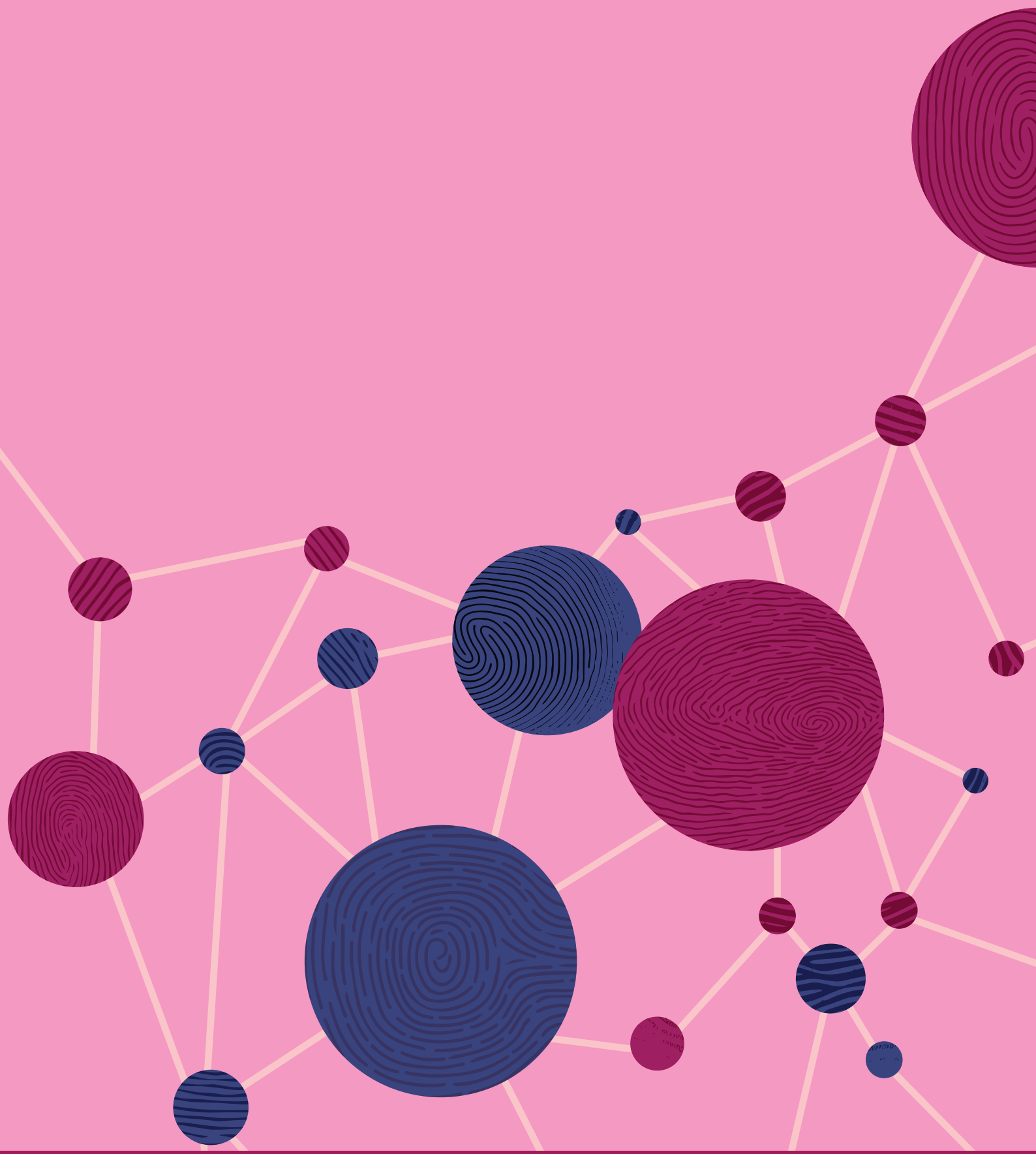
No **terceiro bloco**, o debate foi centrado nos impactos de uma identidade digital como aplicação na IPD, bem como seus benefícios, riscos e limites. O primeiro grupo identificou como risco a possibilidade de exclusão de certos grupos e aspectos interseccionais, como pessoas com deficiência, mulheres, pessoas negras, indígenas e pessoas trans. Isso porque, durante o próprio desenvolvimento da internet, esses grupos foram negligenciados, inviabilizando suas necessidades e características. Ainda, modelos descentralizados de identidade, com registros distribuídos, poderiam ser ferramentas para auxiliar em questões de fraudes,

exclusão e "posse" dos dados pessoais, já que a pessoa identificada passaria a estar no centro da identidade.

O segundo grupo chamou atenção para a implementação de práticas de governança, transparência, literacia digital, e comunicação em linguagem simples para que uma IPD não aprofunde os problemas analógicos. Para o grupo, existe um momento de oportunidade para promover acesso à internet e a inclusão de grupos vulnerabilizados a partir de espaços e ferramentas já existentes. Um exemplo seria as Manzanas del Cuidado em Bogotá, lugar em que pessoas estão disponíveis para ajudar outras a acessarem o digital e, por meio de soluções digitais, para que as pessoas possam acessar outros direitos. A ideia é que o digital é mais uma camada de cuidado, que também é considerado no acesso a outros direitos, e não mais uma barreira.

O terceiro grupo acredita que a descentralização da estrutura seria uma questão de segurança digital do sistema, e não estaria relacionado ao desempenho. Ao mesmo tempo, o desenvolvimento de infraestrutura digital indica para a produção de mais dados, inclusive pessoais, o que facilita o seu compartilhamento e cria novas funcionalidades para esses dados.

Por fim, os grupos compartilharam as suas sínteses e os conhecimentos com os participantes da trilha. Nesse momento, foi possível identificar que os riscos e os limites de sistemas de identidade estão vinculados ao próprio conceito de identidade. Os riscos de não se ter uma identidade inclusiva e universal tensionam o objetivo de construir um sistema de identidade, já que, se os riscos não forem pensados desde o desenvolvimento da identidade, é possível que o sistema não atinja suas finalidades.



REALIZAÇÃO:

DataPrivacyBR Research

APOIO:

ripple