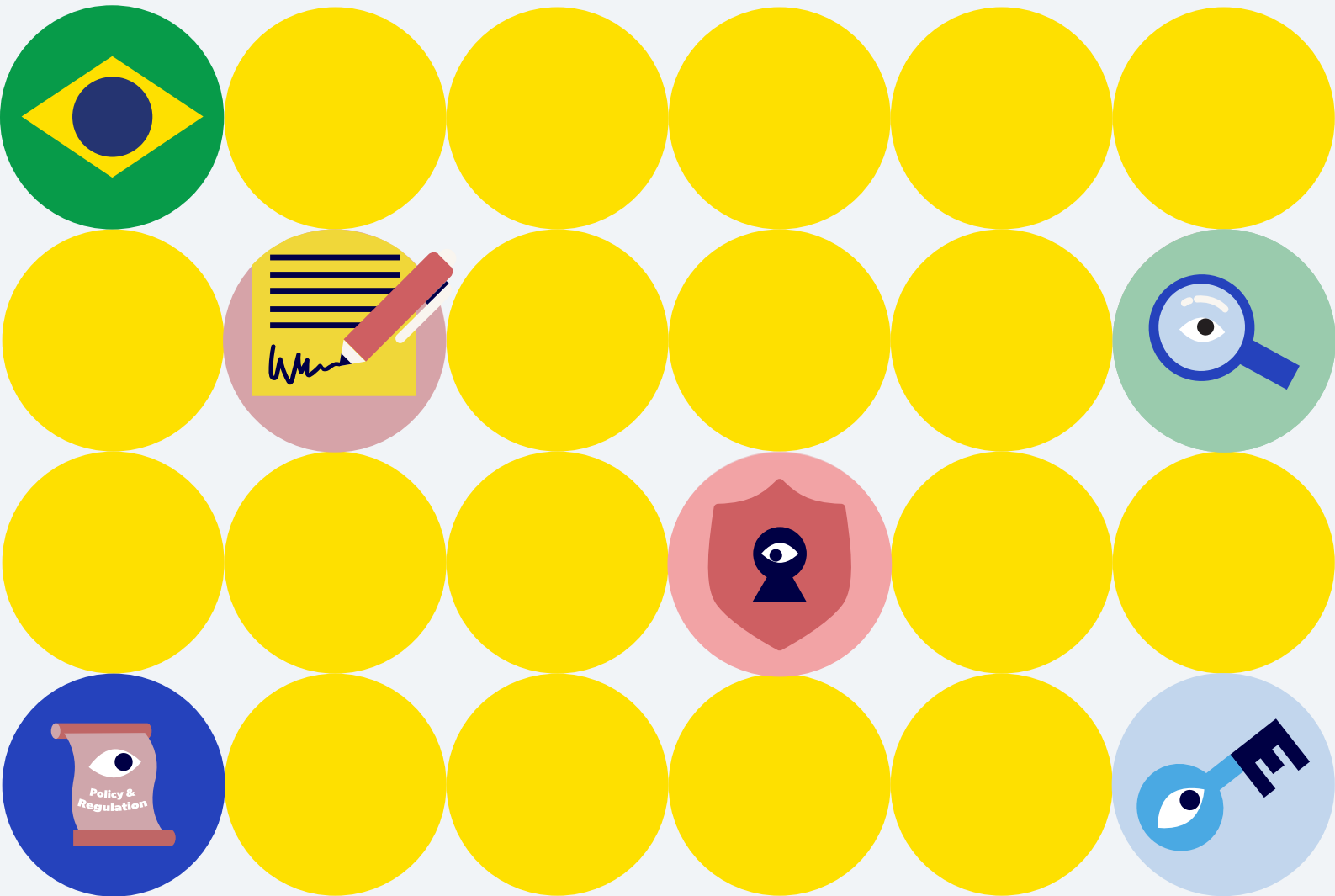
Insights de um exercício de prototipagem
de políticas com empresas Brasileiras

Open Loop | Meta

Guia para a prototipagem de políticas sobre tecnologias de aprimoramento da privacidade (PETs) no Brasil



Index

Apresentação

Os programas Open Loop da Meta no Brasil e no Uruguai, realizados entre 2022 e 2023, representam um marco significativo no avanço das ferramentas e das metodologias de prototipagem de políticas para governar tecnologias emergentes na América Latina, em um contexto no qual a noção de experimentação de políticas e sandboxes regulatórios (regulatory sandbox) parece ter se tornado parte integrante da formulação de políticas nos setores público e privado.

Após um programa bem-sucedido sobre transparência e explicabilidade no México, o Open Loop voltou-se para o Cone Sul para realizar um experimento paralelo sobre tecnologias de aprimoramento da privacidade (PETs, na sigla em inglês) em parceria com equipes de implementação independentes e várias empresas participantes no Brasil e no Uruguai. Esse esforço proporcionou uma excelente oportunidade de aprofundamento nas peculiaridades de cada país, em seus ecossistemas institucionais e de políticas, bem como na natureza dos participantes que estão iniciando sua jornada de adoção de PETs em cada jurisdição. Também ofereceu uma oportunidade única para entender a importância das PETs para a proteção de dados pessoais em todos os setores e para o mapeamento das semelhanças existentes em ambos os contextos em termos de desafios e oportunidades relacionados à adoção e ao uso mais amplo das PETs.

Em síntese, o Open Loop Brasil e Uruguai gerou três resultados importantes: primeiro, os programas contribuíram para aumentar a conscientização e desenvolver capacidades sobre o tema das PETs durante os estágios iniciais do programa; segundo, com um consórcio de empresas, especialistas e formuladores de políticas, o programa promoveu o diálogo entre várias partes interessadas e permitiu a troca de conhecimento em ambos os países (inclusive além das fronteiras), o que provavelmente continuará acontecendo mesmo após a conclusão dessa jornada; e, por fim, o esforço coletivo e colaborativo produziu evidências sólidas e confiáveis que certamente serão utilizadas nos processos de formulação de políticas em toda a região e fora dela.

À medida que demonstramos nossa gratidão a todas as empresas participantes, observadores, pesquisadores e colegas da Meta que nos ajudaram a construir e desenvolver o Open Loop Brasil e Uruguai, aproveitamos esta oportunidade para expressar nossa confiança de que este relatório final representa um primeiro passo importante e decisivo para conectar a inovação tecnológica e política, promovendo uma colaboração mais próxima entre aqueles que desenvolvem tecnologias emergentes e aqueles que as regulamentam na América Latina.

Paula Vargas
Diretora de Política de Privacidade e Engajamento, América Latina

Diego Rafael Canabarro
Chefe de Política de Privacidade, América Latin

Foreword

Em abril de 2024, as Tecnologias de Aprimoramento da Privacidade (PETs) foram classificadas em segundo lugar entre as "10 Principais Tecnologias Emergentes para Enfrentar os Desafios Globais" do Fórum Econômico Mundial. Este reconhecimento ressalta a importância crítica de salvaguardar a privacidade numa era de rápida transformação digital e de rápida evolução das tecnologias baseadas em dados, incluindo a Inteligência Artificial (IA). À medida que o panorama digital se amplia, apresentam-se tanto desafios quanto oportunidades para soluções inovadoras que equilibrem a utilização de dados com a privacidade pessoal.

Como organizações da sociedade civil que operam na campo tecnológico, tanto o Instituto Liberdade Digital quanto o Eon Resilience Lab da C Minds (organização mexicana que explora a interseção entre tecnologia emergente, impacto social e ambiental) estão comprometidas em desenvolver estratégias que minimizem os riscos potenciais das tecnologias emergentes, maximizando ao mesmo tempo o seu impacto social positivo. Ao experimentar estes tópicos, podemos elaborar recomendações sobre políticas centradas no ser humano, com base nas nossas aprendizagens e alinhadas com as práticas e padrões globais.

Tendo em vista as relevantes oportunidades que as PETs representam, é essencial continuar a explorar e compreender como os mercados na América Latina podem continuar a se beneficiar das ferramentas de processamento de dados, protegendo ao mesmo tempo a privacidade. O programa Open Loop proporcionou uma grande oportunidade porque estes exercícios não só servem como mecanismos dinâmicos para preencher a lacuna entre as discussões teóricas e as soluções práticas, como também porque trazem diversas perspectivas ao envolver uma ampla gama de partes interessadas, incluindo governo, academia, indústria e sociedade civil. Estes esforços colaborativos facilitam uma compreensão holística das particularidades das PET em contextos específicos, garantindo que as nossas conclusões se traduzam em recomendações abrangentes e sustentáveis.

No contexto global onde as PETs estão sendo priorizadas, a publicação dos nossos resultados posiciona a América Latina na vanguarda das conversas internacionais. Isto reforça a capacidade da região de acrescentar perspectivas e inovações únicas ao diálogo global sobre tecnologia e proteção de dados. Estas aprendizagens são um passo crucial para garantir que os benefícios da transformação digital sejam realizados de forma ampla e justa, reforçando o papel da região como líder no panorama tecnológico global.

Este relatório não só reflete o nosso compromisso com a implantação responsável da tecnologia, mas também é um recurso vital para indivíduos interessados que procuram explorar as complexidades da IA e da privacidade de dados. Esperamos que as conclusões deste relatório contribuam para ampliar o conhecimento da sociedade sobre PETs, ajudem entidades e governos no processo de implementação dessas tecnologias, promovam espaços e discussões inclusivos e colaborativos e apoiem os formuladores de políticas na elaboração de mecanismos adicionais relacionados à privacidade.

Constanza Gómez-Mont
President and Founder at C Minds

Maria Marinho
Co-fundadora do Instituto
Liberdade Digital

Cláudio Lucena
Universidade Estadual da Paraíba

Apresentação

Em uma era definida pela rápida evolução da tecnologia, com ênfase crescente na inteligência artificial (IA), o desafio de gerir de forma eficiente questões relativas à privacidade ganha cada vez mais destaque. Sistemas de IA processam grandes quantidades de dados pessoais, de forma que a necessidade de proteção da privacidade por meio de ferramentas robustas nunca foi tão crítica. É neste contexto que as tecnologias de aprimoramento da privacidade (PETs) surgem como ferramentas cruciais, oferecendo mecanismos para equilibrar a inovação com os direitos individuais e a confiança da sociedade.

As PETs ajudam a promover transparência e confiança nos sistemas de IA, capacitando os indivíduos com maior controle sobre seus dados e, ao mesmo tempo, promovendo colaborações seguras para o estabelecimento de uma governança de dados efetiva. Desta forma, estas tecnologias também ajudam a promover um ecossistema ético de IA, onde a inovação possa florescer sem comprometer os direitos fundamentais.

O programa Open Loop explorou o potencial positivo na formulação de políticas públicas que promovam as PETs, inclusive como mecanismos de conformidade regulatória. Além da capacidade de endereçar os desafios próprios dos modelos 'tradicionais' de governança de dados pessoais, as PETs também podem facilitar a evolução para novos cenários referentes a sistemas de gestão e governança da IA.

Importante destacar o formato inclusivo com que o programa foi estruturado e implementado. Pesquisadores, participantes e observadores tiveram a oportunidade de contribuir para um entendimento mais amplo sobre o papel das PETs, com o estudo de casos e discussões sobre prototipagem de políticas públicas.

A adoção de tecnologias inovadoras, seguras e previsíveis tem o potencial de ajudar a propiciar segurança jurídica na gestão de dados em soluções de IA, justamente em um momento em que vários países discutem as possíveis alternativas e formatos de regulação, com expectativas de conformidade nem sempre claras. De fato, os trabalhos conduzidos no programa têm a sua relevância amplificada também pelo escopo comparativo entre mais de um país (além dos vários pontos de comparação com o regulamento europeu), o que gera reflexão sobre como as PETs podem ajudar a harmonizar o enfrentamento da gestão da privacidade em diferentes sistemas.

O relatório apresenta dados e evidências de forma acessível, sem comprometer o rigor técnico da metodologia, com conclusões acionáveis que permitem a criação de uma agenda concreta em relação à tecnologia.

Parabenizo o time do programa pela mobilização plural e pelo resultado do trabalho, com a certeza de que este relatório contribuirá para discussões construtivas na formulação de políticas públicas, tanto no campo específico da privacidade, quanto de forma mais ampla em relação à IA.

Eduardo Paranhos
Co-Líder to Grupo de Trabalho de Inteligência Artificial
da Associação Brasileira das Empresas de Software
(ABES). Sócio do escritório EPG Advogados

Sobre o Open Loop

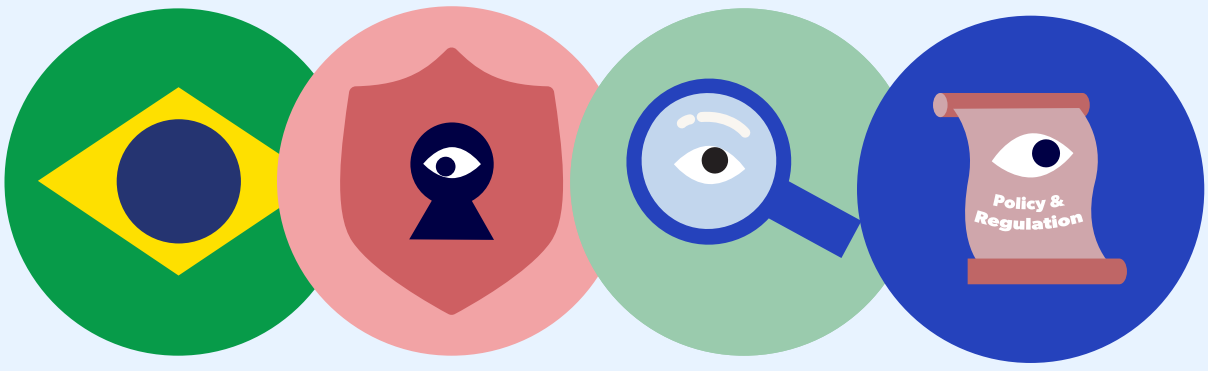
O Open Loop da Meta é um programa global que conecta formuladores de políticas e empresas de tecnologia para ajudar a desenvolver políticas eficazes e baseadas em evidências para IA e outras tecnologias emergentes.

Por meio de uma metodologia estruturada, os participantes do Open Loop criam em conjunto "protótipos" de políticas e testam políticas, regulamentos, leis ou estruturas voluntárias de IA novas ou existentes. Esses esforços de várias partes interessadas apoiam os processos de criação de regras e melhoram a qualidade das orientações e dos regulamentos sobre tecnologias emergentes, garantindo que sejam compreensíveis, eficazes e viáveis na prática.

Este relatório apresenta as conclusões e as recomendações do programa Open Loop Brasil sobre PETs, lançado em setembro de 2022. Esse programa de prototipagem de políticas começou simultaneamente com um programa idêntico no Uruguai, com a intenção de orientar e permitir que as empresas de ambos os países aproveitassem e aplicassem as PETs para ajudar a desidentificar dados e mitigar riscos relacionados à privacidade, inclusive em sistemas de IA. Ambos os programas foram desenvolvidos de forma independente, e cada um tinha o próprio parceiro local responsável por sua implementação. O programa Open Loop Brasil foi implementado no país de setembro de 2022 a abril de 2023 em parceria com o Instituto Liberdade Digital.

Este relatório foi redigido por Maria Marinho, Cláudio Lucena, David Lehr, Laura Galindo, Maartje Nugteren e Diego Rafael Canabarro.

Como citar este relatório?
“Maria Marinho, Cláudio Lucena, David Lehr, Laura Galindo, Maartje Nugteren e Diego Rafael Canabarro. "Orientação para a prototipagem de tecnologias para aprimorar a privacidade no Brasil" (2024), https://openloop.org/reports/2024/05/Brazil_Report_PETs_pt.pdf”



Agradecimentos

O programa Open Loop Brasil foi criado pela Meta, mas desenvolvido e facilitado em colaboração com o Instituto Liberdade Digital.

Gostaríamos de agradecer a participação das organizações observadoras abaixo nessa iniciativa:

O programa Open Loop agradece aos especialistas individuais que representaram as organizações observadoras durante todo o programa: Clara Langevin (C4IR), Eduardo Paranhos (Eixo I da EBIA, Co-Líder do GT de IA da ABES), Loren Spíndola (Eixo I da EBIA, Co-Líder do GT de IA da ABES), Marcelo Guedes (ANDP) e Thiago Moraes (ANPD).

Gostaríamos de expressar nossa gratidão e reconhecimento às empresas que colaboraram com o desenvolvimento desse projeto:

Antares

Beetools

DASA

Mercado Livre

Neoron

NUBANK

Peak Invest

Showkase

Vectra

Um agradecimento especial aos especialistas individuais que representaram as empresas participantes durante todo o programa: Caroline Rocabado (Dasa), Charles Buss (Beetools), Cinthia Baccarin (Mercado Livre), Diego Pereira (Peakinvest), Expedito de Carvalho Junior (Antares Comunicação), Jefferson Araújo (Showkase), Kleberson Santos (Vectras), Matheus Crispim (Neoron), Miguel Isoni Filho (Neoron), Raíssa Moura (Nubank), Nathália Sampaio (Dasa), Raíssa Moura (Nubank), Rawlisson Terrabuio (Beetools) Samantha Santos de Oliveira (Mercado Livre) e Thaís Souza (Peakinvest).

Agradecemos especialmente ao nosso grupo de especialistas, que compartilharam seus profundos conhecimentos e contribuíram para o desenvolvimento da estratégia de pesquisa do programa: Ana Paula Bialer, Ângela Rosso, Carlos Affonso de Souza, Diogo Cortiz, Gustavo Godinho, Maria Cecília Oliveira Gomes, Núria Lopez, Raquel Saraiva, Savyo Morais, Tatiana Coutinho e Wellington Dantas.

Agradecemos também aos nossos parceiros de design da Craig Walker Design and Research, em particular a John-Henry Pajak.

Resumo executivo

O Open Loop é um programa global que conecta formuladores de políticas e empresas inovadoras para ajudar a desenvolver políticas eficazes e baseadas em evidências sobre IA e outras tecnologias emergentes. O principal objetivo desse programa Open Loop consistiu em orientar e permitir que as empresas do Brasil e do Uruguai aproveitassem e selecionassem PETs para ajudar a desidentificar dados e mitigar riscos relacionados à privacidade, inclusive em sistemas de IA.

Para preencher a lacuna entre as expectativas de privacidade e as soluções tecnológicas e capacitar os controladores de dados a processar os dados com foco na privacidade, foi desenvolvido e testado um protótipo de política na forma de um manual técnico para promover os princípios de proteção de dados usando PETs. Este protótipo de política visa apoiar as empresas estabelecendo princípios de proteção de dados, apresentando um processo de três etapas para operacionalizar os princípios de privacidade desde a concepção e, ao mesmo tempo, conectando-as à adoção de PETs.

Este relatório compartilha os resultados desse programa de prototipagem de políticas, que foi implementado no Brasil de setembro de 2022 a abril de 2023 em parceria com o Instituto Liberdade Digital e envolveu nove empresas brasileiras. Todas essas empresas fornecem serviços B2B e/ou B2C e são de tamanhos e setores variados.

O programa investigou:

- Com que grau de eficácia o protótipo de política equilibra a clareza, a viabilidade técnica e a eficiência da política para o público-alvo?
- A familiaridade e o entendimento atual das empresas participantes em relação às PETs.
- Lacunas atuais e desafios de implementação para a adoção de PETs por organizações no Brasil e no Uruguai.
- Boas práticas e aprendizados que contribuem para a adoção bem-sucedida de PETs para ajudar a desidentificar dados e reduzir os riscos relacionados à privacidade.

Nossos resultados mostram que tanto no Brasil quanto no Uruguai:

- As empresas relataram pouca familiaridade com as PETs, especialmente com as modalidades mais avançadas.
- O manual sobre as PETs ajudou as empresas a identificar os riscos à privacidade e as estratégias de mitigação.
- As empresas enfrentam custos excessivos e restrições de recursos humanos.
- A incerteza regulatória foi considerada uma barreira significativa para a adoção das PETs.

Com base nos resultados dos programas Open Loop do Brasil e do Uruguai e no feedback recebido das empresas participantes, as seguintes recomendações são oferecidas aos reguladores e aos formuladores de políticas responsáveis pela governança de dados, privacidade e proteção de dados no que tange às PETs:

1. **Os formuladores de políticas devem adotar uma abordagem flexível e baseada em riscos para o conceito legal de anonimização:** a mensuração do nível de risco deve ser uma avaliação de caráter específico que considere o contexto do tratamento de dados, quais medidas técnicas (como PETs) foram aplicadas aos dados e quais medidas não técnicas (como controles de acesso e restrições legais) foram aplicadas aos dados. Além disso, a avaliação do risco deve se concentrar em saber se as partes que realmente podem ter acesso aos dados poderiam reidentificá-los, considerando todas as proteções que foram aplicadas a eles.

2. **Os formuladores de políticas devem esclarecer que as entidades podem processar dados com o objetivo de reduzir o risco de identificabilidade:** em particular, para jurisdições que se baseiam em leis semelhantes ao RGPD (aquelas que exigem uma base legal para tratar dados), os formuladores de políticas devem esclarecer que: (i) nenhuma base legal é necessária para o tratamento de dados com a finalidade de reduzir o risco de identificabilidade; ou (ii) o legítimo interesse , ou uma base legal semelhante, podem ser prontamente invocados para conduzir o referido tratamento.

3. **Os formuladores de políticas desempenham um papel valioso no avanço dos diálogos entre as diversas partes interessadas sobre as PETs:** essas conversas poderiam não só ajudar a desenvolver a capacidade das entidades de implantar PETs, mas também fazer avançar o desenvolvimento de uma compreensão compartilhada das PETs e de como elas podem ser usadas com eficácia em diferentes casos. Os formuladores de políticas poderiam encorajar discussões para explorar essas complexidades, buscando a participação de órgãos de definição de padrões e associações de todo o setor no processo.

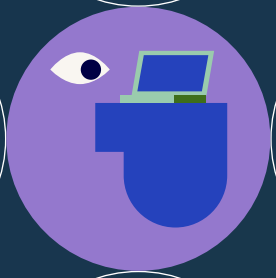
4. **Os formuladores de políticas devem investir diretamente na pesquisa e no desenvolvimento de PETs, bem como na educação pública sobre os benefícios das PETs:** os formuladores de políticas também poderiam financiar a pesquisa e o desenvolvimento para implementações de PETs de código aberto, que poderiam ser usadas mais prontamente por entidades de pequeno e médio porte. Além de pesquisa e desenvolvimento, os formuladores de políticas poderiam investir em campanhas educativas que ajudem a explicar às pessoas como as PETs podem proteger sua privacidade.

5. **Considerações adicionais:** incentivamos os formuladores de políticas a explorar os tópicos acima mais detalhadamente por meio de sandboxes regulatórios.

CAPÍTULO 1

Introdução

1



> Com o avanço das tecnologias que analisam grandes quantidades de dados, também avançaram as tecnologias que criam oportunidades para aumentar a privacidade dos indivíduos. As tecnologias de aprimoramento da privacidade (PETs") têm um potencial significativo para lidar com muitos riscos à privacidade e, ao mesmo tempo, oferecer a toda a sociedade os benefícios advindos de uma análise de dados de ponta.

Nos últimos anos, o reconhecimento desses benefícios levou a um aumento do interesse em PETs, por parte do setor, dos formuladores de políticas e dos defensores da privacidade. No entanto, com o desenvolvimento de discussões mais intensas sobre as PETs, torna-se fundamental que todas as partes interessadas entendam melhor essas tecnologias, os aspectos práticos de seu uso e as maneiras pelas quais as políticas públicas podem incentivar ou desincentivar seu uso.

O programa Open Loop da Meta buscou promover esses entendimentos por meio de iniciativas no Brasil e no Uruguai, reunindo especialistas locais, empresas e observadores em cada país. O objetivo dessas iniciativas foi desenvolver a capacidade das empresas de implantar PETs e, no processo, questionar os desafios que surgiram e como os formuladores de políticas podem enfrentá-los.

Este relatório apresenta as principais conclusões e recomendações sobre políticas resultantes das iniciativas no Brasil e no Uruguai. O restante deste capítulo introdutório apresenta uma breve introdução às PETs, resume o panorama da política global relacionada a essas tecnologias e descreve a metodologia comum aplicada nos programas do Brasil e do Uruguai. O segundo capítulo dá ênfase aos aspectos exclusivos da iniciativa no Brasil, incluindo seus participantes e o cenário da política local. O capítulo três sintetiza as experiências no Brasil e no Uruguai para elaborar um conjunto de conclusões importantes. Por fim, no último capítulo com base nesses resultados são ofertadas recomendações sobre como os formuladores de políticas podem promover a adoção de PETs.

O que são PETs?

PETs são um conjunto extremamente diversificado de ferramentas técnicas que operam de maneiras muito diferentes. De modo geral, PETs são técnicas criptográficas ou estatísticas que preservam o valor informativo dos dados e, ao mesmo tempo, aumentam a privacidade ou a segurança. Mas essa definição ampla engloba muitas técnicas diferentes. Não há uma única maneira correta de categorizar as PETs, mas é possível agrupá-las em quatro tipos:

PETs que alteram os dados: são aquelas, como pseudonimização ou privacidade diferencial, que alteram os dados subjacentes de alguma forma;

PETs que alteram a computação: são aquelas, como a computação multipartidária segura ou a análise federada, que alteram quem calcula uma função nos dados ou como isso é feito;

PETs que protegem os dados: são aquelas, como a criptografia homomórfica, que criptografam os dados ou a mídia na qual eles estão armazenados; e

Machine learning que preserva a privacidade: são aquelas, como dados sintéticos ou ataques adversários, que melhoram a privacidade no machine learning/IA.

Outra possibilidade foi desenvolvida pela OCDE , que agrupa as PETs em quatro categorias diferentes: ferramentas de ofuscação de dados, ferramentas de tratamento de dados criptografados, análises federadas e distribuídas e ferramentas de responsabilidade pelos dados. Vale reforçar que não há uma maneira correta de categorizar as PETs, mas agrupamentos dessa natureza podem fornecer um valor heurístico.

Independentemente de como as PETs são categorizadas, há nuances adicionais que dificultam a discussão e a implementação de PETs. Em primeiro lugar, as PETs variam muito em termos de maturidade. Algumas PETs, como os protocolos de criptografia padrão, existem há décadas, enquanto outras, como a criptografia homomórfica e o aprendizado federado, são ainda mais recentes e ainda estão sendo pesquisadas. Em segundo lugar, como as PETs operam de maneiras diferentes, elas oferecem variados tipos de proteções de privacidade, algumas das quais são mais fáceis de entender do que outras. Por exemplo, é relativamente fácil entender como a remoção de um identificador direto, como o nome de alguém, de um conjunto de dados preserva a privacidade dessa pessoa, mas outras técnicas, como a computação multipartidária segura, melhoram a privacidade de maneiras mais indiretas e menos intuitivas. Por fim, embora as PETs possam ser implementadas isoladamente, na prática elas costumam ser combinadas não apenas com outras PETs, mas também em conjunto com ferramentas não técnicas de aprimoramento da privacidade, como controles de acesso e restrições contratuais ao uso de dados. As discussões técnicas e políticas sobre as PETs devem reconhecer e aceitar essas complexidades.

Panorama das políticas globais

À medida que as PETs avançaram, também cresceu o interesse global nelas. Os governos e as instituições internacionais estão cada vez mais otimistas em relação ao papel que as PETs podem desempenhar no aprimoramento da privacidade e interessados em aumentar os investimentos em PETs em suas jurisdições. A Tabela 1 abaixo apresenta uma visão geral não exaustiva das maneiras pelas quais os formuladores de políticas estão tentando atingir essas metas. É importante ressaltar que a Tabela 1 não inclui exemplos do Brasil ou do Uruguai; os esforços no Brasil serão descritos no Capítulo 2.

Tabela 1. Uma amostra de iniciativas e políticas voltadas para PETs.

Região/Instituição	Iniciativa/Política	Descrição
Estados Unidos	Estratégia nacional para promover o compartilhamento e a análise de dados com preservação da privacidade[3]	O Gabinete de Política de Ciência e Tecnologia da Casa Branca estabeleceu essa estratégia para promover o uso de técnicas como as PETs. Entre outras coisas, ela incentiva a adoção de PETs pelas agências federais, maiores investimentos em pesquisa e desenvolvimento, maior educação sobre PETs e grande colaboração internacional sobre o assunto.
Estados Unidos	Ordem executiva sobre o desenvolvimento e o uso seguro, protegido e confiável da inteligência artificial[4]	Para aumentar a privacidade na IA, a Ordem orienta a formação de uma Rede de Coordenação de Pesquisa sobre PETs, bem como a identificação de oportunidades de uso de PETs pelos órgãos federais.
Estados Unidos	Diretrizes do National Institute of Standards and Technology (NIST) para avaliação de garantias de privacidade diferencial[5]	Essas diretrizes sobre privacidade diferencial foram produzidas pelo NIST para cumprir um requisito estabelecido pela Ordem Executiva.
Estados Unidos	Lei de pesquisas sobre tecnologias que aumentam a privacidade[6]	Esse projeto de lei orientaria o NIST a financiar pesquisas sobre PETs e os órgãos federais a colaborar com os mecanismos das políticas para promover a adoção de PETs, incluindo as diretrizes e os padrões voluntários.

Reino Unido	Orientação preliminar do Information Commissioner's Office (ICO) sobre anonimização, pseudonimização e PETs, e orientação final sobre PETs[7]	O ICO fez uma consulta sobre uma orientação preliminar detalhada em cinco partes, incluindo um capítulo sobre anonimização, e depois publicou uma orientação final sobre PETs com escopo mais limitado, fazendo referência à orientação preliminar para obter detalhes adicionais.
Estados Unidos e Reino Unido	Desafios premiados sobre PETs[8]	Os governos dos EUA e do Reino Unido fizeram uma parceria para financiar o desenvolvimento de soluções PETs para casos de uso específicos.
União Europeia	Revisão da orientação do European Data Protection Board (EDPB)	O EDPB indicou em seu programa de trabalho 2023-2024[9] a intenção de revisar suas diretrizes de anonimização
União Europeia	Decisão do Tribunal Geral da União Europeia sobre o caso SRB vs. EDPS[10]	Essa decisão judicial enfatizou que o contexto é importante para determinar se os dados foram anonimizados e que, quando os dados são compartilhados, é preciso se colocar no lugar do destinatário para avaliar o risco de reidentificação.
Singapura	Sandbox regulatório Personal Data Protection Commission Singapore (PDPC) and Infocomm Media Development Authority (IMDA)[11]	Esse sandbox regulatória avaliou estudos de caso de empresas, incluindo a Meta[12], respondendo às perguntas das empresas sobre a aplicação das leis de proteção de dados
Coreia do Sul	Diretrizes revisadas para dados pseudônimos[13]	Essas diretrizes revisadas abordaram o tratamento de dados pseudônimos, especialmente no contexto da IA.
Internacional	Relatório e workshops sobre PETs da OCDE[14]	O relatório abrangente da OCDE sobre PETs servirá de modelo para workshops que explorarão casos de uso e questões políticas.
Internacional	Equipe de trabalho sobre PETs da ONU[15]	A equipe de trabalho está concentrada em aprimorar o uso de PETs nos escritórios nacionais de estatística dos países.

Embora a Tabela 1 apresente apenas uma visão geral dos esforços relacionados às PETs em todo o mundo, a diversidade de esforços deixa claro que as PETs são um assunto cada vez mais importante para as partes interessadas. Em particular, os governos expressaram um interesse significativo em promover a adoção de PETs, tanto no setor público quanto na sociedade e na indústria em geral. Outra conclusão é que a relação exata entre as PETs e as leis de proteção de dados é incerta e está sendo explorada ativamente pelos órgãos reguladores e tribunais. A maioria das leis de proteção de dados não lida diretamente com PETs, ou seja, não contém disposições que façam referência específica às PETs. Dito isso, a maioria das leis de proteção de dados tem princípios fundamentais, como minimização e segurança de dados, que as PETs podem ajudar a promover. Além disso, a maioria das leis isenta de seus escopos os dados que foram "anonimizados", "desidentificados" ou "dissociados". As PETs podem permitir isso, mas diferentes países estão buscando definir exatamente quais são as condições para a anonimização. Jurisdições como o Reino Unido e Singapura estão adotando uma abordagem flexível e baseada em riscos, e a decisão do Tribunal Geral da UE no caso SRB parece estar direcionando a legislação da UE nesse mesmo sentido. Mas ainda há incertezas significativas sobre o tema. (incluindo um recurso da decisão do caso SRB).

Sobre o protótipo de política

O Open Loop da Meta desenvolveu o **Manual sobre as PETs (o "Manual")** para servir como o protótipo de política do programa. O Manual é um documento educacional que buscou ajudar os participantes do programa a entender mais sobre as PETs, como elas podem reduzir os riscos à privacidade e como podem ser implementadas. Para atingir essas metas, o Manual definiu um processo de três etapas, solicitando aos participantes que fizessem o seguinte:

ETAPA 1

Avaliar riscos

os participantes foram lembrados dos princípios que orientam a proteção de dados e foram solicitados a mapear seus ciclos de vida de dados e avaliar os possíveis riscos à privacidade, considerando a probabilidade de um tratamento de dados não intencional ou inesperado e a magnitude dos danos que poderiam resultar desse tratamento.

ETAPA 2

Identificar estratégias de redução de riscos

após a identificação dos riscos potenciais, os participantes foram solicitados a identificar as estratégias que poderiam empregar para reduzir esses riscos. As estratégias em potencial incluíram aquelas voltadas para os dados (minimização, separação, agregação e ocultação) e aquelas voltadas para a organização ou o processo (informar, controlar, demonstrar e aplicar).

ETAPA 3

Selecionar PETs relevantes

por fim, o Manual pediu aos participantes que selecionassem e avaliassem a aplicação de PETs capazes de responder às estratégias de redução de riscos identificadas na Etapa 2. As PETs disponíveis para seleção incluíram técnicas de desidentificação, privacidade diferencial, dados sintéticos, aprendizado/análise federados, ambientes de execução confiáveis, computação multipartidária segura, técnicas de criptografia e criptografia homomórfica.

Sobre os testes

Esse programa Open Loop empregou uma abordagem de métodos mistos para responder às principais perguntas sobre a experiências das empresas participantes com a aplicação do Manual (veja mais detalhes no Anexo 1). Os resultados apresentados neste relatório foram identificados por meio de respostas a pesquisas online, workshops sequenciais e temáticos e entrevistas semiestruturadas com as empresas participantes.

Em particular, a fase de testes buscou feedback (para cada etapa do Manual) sobre três aspectos importantes de cada etapa:

Clareza

se a etapa foi claramente comunicada e entendida.

Eficácia

se a etapa atingiu sua meta (por exemplo, até que ponto a Etapa 3 permitiu que as empresas identificassem as PETs apropriadas).

Viabilidade

dadas as restrições operacionais e reais, se os participantes puderam agir prontamente de acordo com as prescrições de uma etapa.

CAPÍTULO 2

O programa no Brasil

O programa Open Loop no Brasil foi conduzido com o Instituto Liberdade Digital como o parceiro local responsável pela implementação do programa. Esta seção fornece mais detalhes sobre o porquê e como o programa no Brasil foi conduzido, incluindo como o ambiente de políticas no Brasil era propício para a exploração desses tópicos e quais entidades brasileiras participaram do programa. Esses detalhes para o programa Open Loop no Uruguai podem ser encontrados no relatório do Uruguai.

Panorama das políticas locais

Conforme descrito no Capítulo 1, um dos desafios das discussões sobre políticas relacionadas às PETs é a ligação pouco clara entre as PETs e as leis de proteção de dados. A maioria das leis de privacidade de dados não contém disposições que mencionem explicitamente as PETs ou como elas podem ou devem ser usadas. Em vez disso, essas leis contêm princípios gerais de proteção de dados, como a minimização de dados, que as PETs podem ajudar a alcançar, bem como hipóteses de isenção de incidência da lei em casos de anonimização de dados, que as PETs podem ajudar a concretizar .

A Lei Geral de Proteção de Dados Pessoais ("LGPD") do Brasil segue essa abordagem geral. O Artigo 12 isenta do escopo de dados pessoais os "dados anonimizados", e o Artigo 5º define "dados anonimizados" como "dados relacionados a um titular de dados que não pode ser identificado, considerando o uso de meios técnicos razoáveis e disponíveis no momento do tratamento". Essas disposições são semelhantes, de certa forma, às disposições relevantes do RGPD, cujo Considerando 26 trata como anônimas "as informações que não se referem a uma pessoa física identificada ou identificável ou a dados pessoais tornados anônimos de tal forma que o titular dos dados não seja ou não seja mais identificável". O Considerando 26 também afirma que "para determinar se uma pessoa física é identificável, devem ser levados em conta todos os meios com probabilidade razoável de serem usados (...) pelo controlador ou por outra pessoa para identificar a pessoa física direta ou indiretamente".

Mas há algumas diferenças textuais notáveis entre a LGPD e o RGPD. Primeiro, eles parecem diferir com relação a quais atores são considerados ao avaliar o risco de identificabilidade. A LGPD parece se concentrar em avaliar se o controlador ou o processador de dados possui meios com probabilidade razoável de serem usados para reidentificar os dados. O Artigo 12, § 1º, afirma que "a determinação do que é considerado razoável deve levar em conta fatores objetivos, tais como o custo e o tempo necessários para reverter o processo de anonimização, de acordo com as tecnologias disponíveis, e o uso exclusivo de seus próprios meios" (grifo nosso). O RGPD, por outro lado, considera os meios com probabilidade razoável de serem usados "pelo controlador ou por outra pessoa" (grifo nosso).

Em segundo lugar, a LGPD e o RGPD parecem diferir com base no fato de os meios razoavelmente disponíveis serem aqueles disponíveis no momento do tratamento ou também potencialmente no futuro. A definição de "dados anonimizados" da LGPD considera os meios técnicos disponíveis "no momento do tratamento", enquanto o Considerando 26 do RGPD exige considerar "a tecnologia disponível no momento do tratamento e os desenvolvimentos tecnológicos" (grifo nosso).

A importância dessas diferenças textuais não é clara. Conforme mencionado no Capítulo 1, há uma incerteza significativa em torno de como interpretar o RGPD, resultante, em parte, da decisão do Tribunal Geral da UE no caso SRB e da revisão iminente da orientação sobre anonimização do EDPB. Além disso, a Autoridade Nacional de Proteção de Dados ("ANPD") do Brasil realizou recentemente uma consulta pública sobre a minuta da guia de anonimização e pseudonimização, que foi encerrada em 3 de abril de 2024 . Não está claro como a orientação final abordará essas questões, mas é notável que a versão preliminar do guia, em contraste com algumas interpretações do RGPD, enfatizou que a anonimização não significa reduzir o risco de identificabilidade a quase zero, mas sim reduzi-lo substancialmente, dado o contexto do tratamento de dados.

Considerando todos esses desenvolvimentos, o Brasil está vivendo um momento propício para explorar questões relacionadas a PETs e anonimização. Esperamos que os aprendizados do programa Open Loop sejam úteis à medida que essas conversas sobre políticas no Brasil continuem a se desenvolver.

Sobre as empresas participantes

Nove empresas participaram do programa Open Loop no Brasil. Tratou-se de um conjunto intencionalmente diversificado de empresas, com representantes de tamanhos variados e de diferentes setores. A figura 1 apresenta mais informações sobre as empresas.

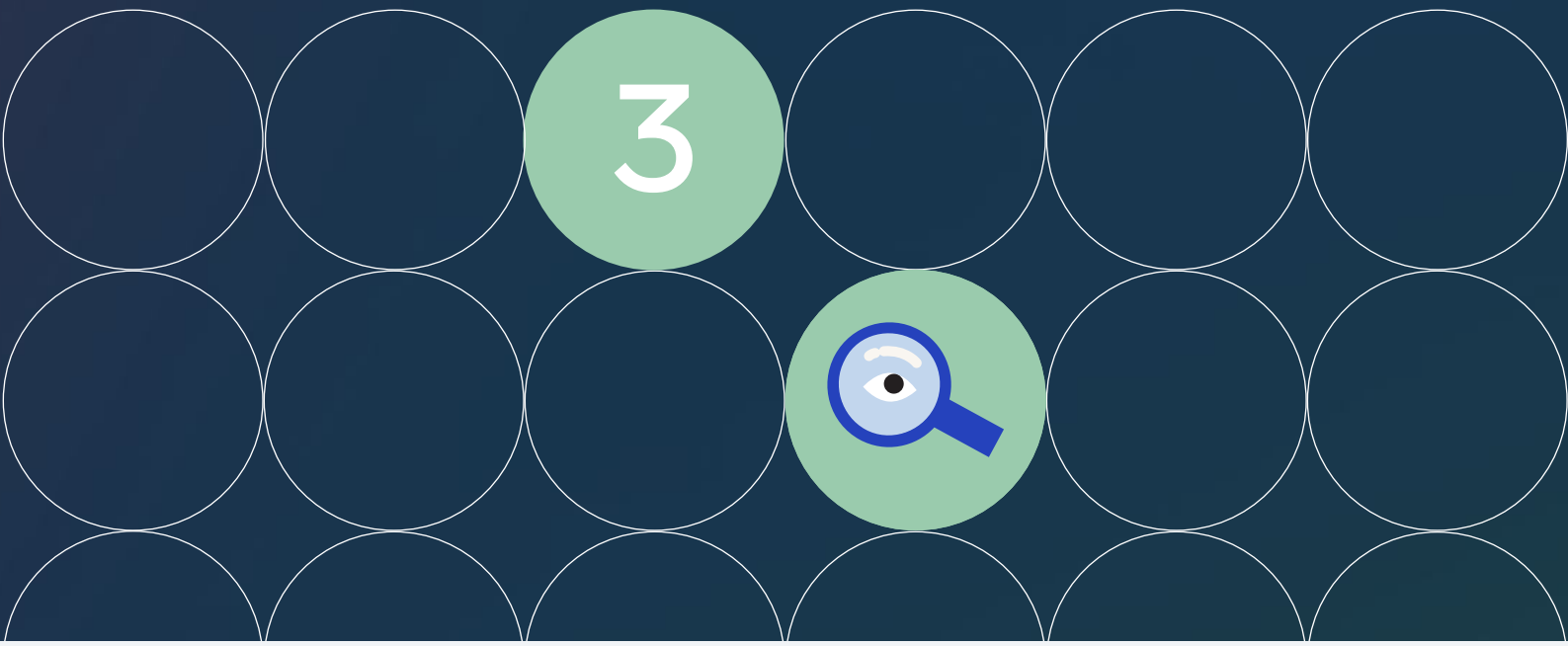
Company	Type - Sector	Business model	Size
Antares Comunicação	Publicidade e marketing digitall.	B2B	Pequena
beetools	Edtech - Escola de ingles no segmento de franchise.	B2B, B2C	Pequena
DASA	Saúde	B2B, B2C	Grande
mercado livre	Marketplace	B2B, B2C	Grande
neoron	TI e serviços de comunicação - marketing digital (Chatbots)	B2B	Pequena
nubank	Fintech	B2B, B2C	Grande
peak invest	Fintech (emprestimos P2P)	B2B	Pequena
SHOWKASE.	Retailtech	B2B (SaaS)	Pequena
VECTRA	Consultoria e serviços em TI	B2B, B2C	Média

Figura 1 — Empresas participantes. As empresas foram divididas por tamanho usando as definições da OCDE: pequena (de 10 a 49 funcionários), média (de 50 a 249 funcionários) e grande (250 funcionários ou mais).

CAPÍTULO 3

Resultados

Em geral, os resultados dos programas Open Loop no Brasil e no Uruguai foram semelhantes. Esta seção apresenta um resumo de alguns dos resultados mais importantes de ambos os programas, extraindo os elementos mais relevantes da pesquisa relacionados à clareza, à eficácia e à viabilidade do Manual. Quando apropriado, são registradas as diferenças importantes nos resultados entre os países.



FINDING

3.1 As empresas relataram pouca familiaridade com as PETs, especialmente as avançadas

DETAILS

Em ambos os países, havia lacunas no entendimento e na familiaridade dos participantes com as PETs no início dos programas. Mas as naturezas dessas lacunas eram diferentes nos dois países. No Uruguai, no início do programa, os participantes foram solicitados a classificar sua familiaridade com as PETs em uma escala do tipo Likert que variava de zero (total falta de compreensão) a cinco (total compreensão). A pontuação média foi de 2,5, indicando um nível relativamente baixo de familiaridade com as PETs. No Brasil, entretanto, muitas empresas tinham pelo menos algum conhecimento sobre PETs, com quase 80% das empresas informando que já estavam usando PETs tradicionais, como técnicas de anonimização ou pseudonimização. No entanto, o mesmo não ocorreu com as PETs mais avançadas, o que sugere uma menor conscientização ou compreensão destas modalidades de PETs.

FINDING

3.2 O Manual sobre as PETs ajudou as empresas a identificar riscos à privacidade e suas respectivas estratégias de mitigação

DETAILS

Em geral, os participantes de ambos os países consideraram o Manual claro e útil. No Brasil, por exemplo, dois terços das empresas afirmaram que a Etapa 1 do Manual foi útil para identificar possíveis riscos à privacidade. É interessante notar que a principal diferença entre essas empresas e aquelas que não consideraram útil a Etapa 1 do Manual foi provavelmente o tamanho; todas as pequenas empresas consideraram útil o conteúdo do Manual, enquanto apenas pouco mais de um terço das grandes empresas tiveram a mesma opinião. Resultados semelhantes foram observados no Brasil para as Etapas 2 e 3 do Manual; a maioria das empresas relatou que a Etapa 2 contribuiu de forma moderada ou significativa para sua capacidade de identificar riscos à privacidade e estratégias de mitigação, e 75% das empresas classificaram o material do Manual na Etapa 3 como relativamente ou extremamente útil.

No Uruguai, as entidades relataram ter obtido aprendizados significativos com o Manual. Uma entidade disse: "Obtivemos insights sobre os riscos comuns que podem surgir nos diferentes estágios do ciclo de vida dos dados." Com relação ao aprendizado sobre medidas de mitigação de riscos, outra entidade disse: "Passamos a entender melhor certas técnicas que atualmente são negligenciadas ou não são consideradas." Dito isso, as entidades no Uruguai relataram que a Etapa 3 (seleção de PETs) foi mais difícil de entender devido à falta de experiência e conhecimento existente sobre PETs.

FINDING

3.3 As empresas enfrentam custos excessivos e restrições de recursos humanos

DETAILS

Embora as entidades do Brasil e do Uruguai tenham considerado o Manual útil e fácil de entender, elas enfrentam desafios significativos na avaliação da aplicação das PETs que selecionaram na Etapa 3. Em particular, as entidades de ambos os países expressaram preocupação com o fato de que a implementação de PETs (especialmente as mais avançadas) exigia custos significativos. Isso inclui custos técnicos, como investimento em infraestrutura de dados e computação nova ou modificada, e custos humanos ou operacionais, como contratação e/ou treinamento de funcionários adicionais.

No Uruguai, as entidades foram perguntadas sobre suas principais preocupações em relação à adoção de PETs, o que resultou em uma lista expressiva. Duas preocupações se destacaram como as mais predominantes, cada uma delas listada por seis entidades: "custos de implementação e manutenção" e "falta de recursos". Vale destacar que apenas três entidades possuíam equipes dedicadas de governança de dados, o que pode ter contribuído para a frequência com que essas duas preocupações foram expressas. No Uruguai, essas preocupações também levaram as entidades a adotar PETs mais simples e fáceis de implementar. Entre as PETs que as entidades poderiam escolher, duas poderiam ser caracterizadas como relativamente menos complexas e mais fáceis de implementar: técnicas de desidentificação e técnicas criptográficas. Elas foram selecionadas por seis e sete entidades, respectivamente. Uma entidade disse: "A desidentificação pode ser viável para o nosso caso, pois se aplica a qualquer conjunto de dados, e o custo de redução, tokenização, hashing ou anonimização é bastante baixo em comparação com outras técnicas mais complexas. Isso também vale para as técnicas criptográficas." As únicas outras modalidades de PETs selecionadas por algumas entidades foram privacidade diferencial, dados sintéticos e ambientes de execução confiáveis, que foram selecionada s por apenas duas, uma e uma entidades, respectivamente.

No Brasil, conforme mencionado anteriormente, a maioria das entidades já estava usando PETs tradicionais e menos complexas, como técnicas de anonimização ou pseudonimização. No entanto, as entidades no Brasil enfrentaram desafios na implementação das PETs, especialmente as mais complexas. Quando perguntadas sobre suas principais preocupações em relação à adoção de PETs, 75% das entidades citaram os custos de implementação e manutenção. Para algumas entidades de grande porte, as preocupações geralmente giravam em torno dos custos relacionados aos recursos humanos (encontrar equipes de engenharia disponíveis) necessários para implementar essas e outras técnicas mais avançadas. Por exemplo, uma entidade declarou: "Para aplicar as PETs, é necessário ter recursos humanos especializados no assunto, pois não é fácil implementá-las."

FINDING

3.4 A incerteza regulatória é uma barreira significativa para a adoção das PETs

DETAILS

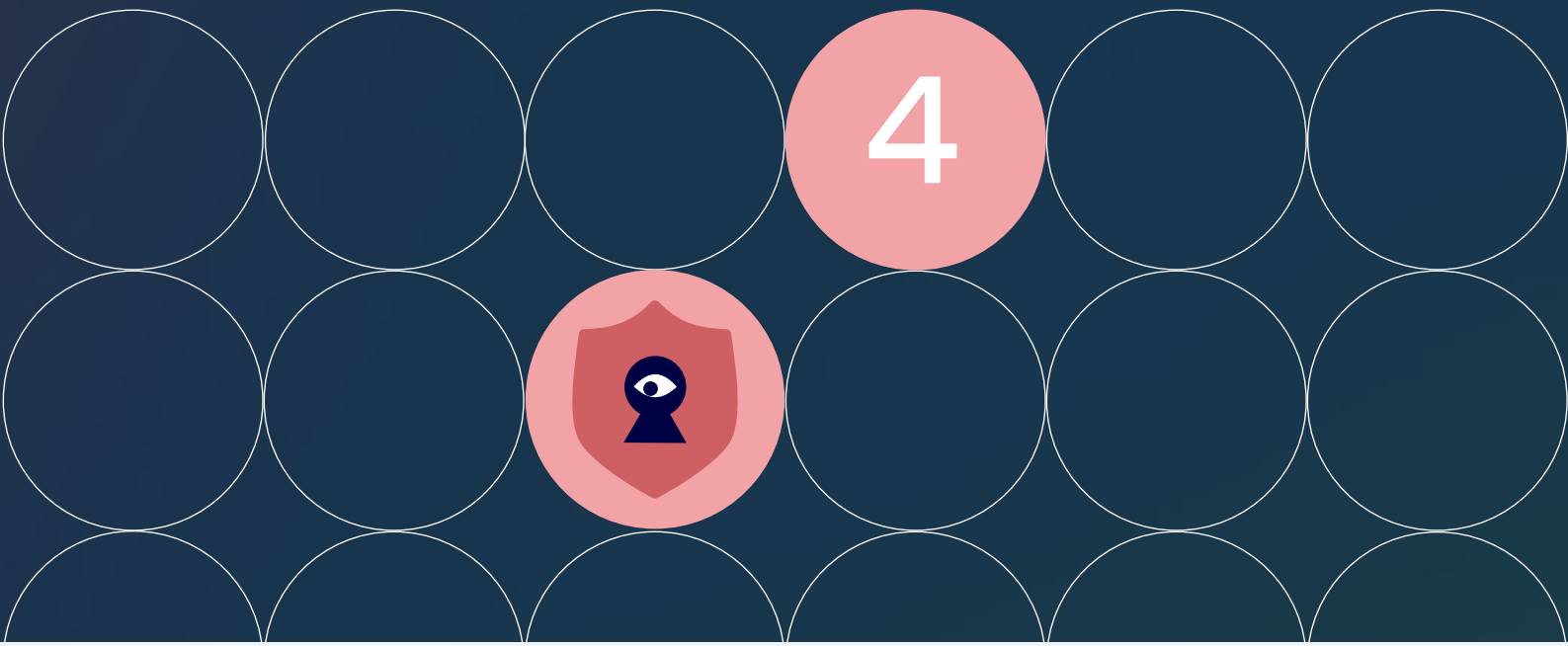
Além dos custos decorrentes da aplicação das PETs, as entidades de ambos os países expressaram o desejo de usar as PETs para ajudar a promover os princípios de proteção de dados, mas a relação exata entre as PETs e as leis de proteção de dados não é clara. No Brasil, 87,5% das entidades entrevistadas citaram a capacidade de atender às expectativas regulatórias como um fator para a implementação de PETs, mais do que qualquer outro fator. No Uruguai, quando as entidades foram questionadas sobre suas principais preocupações em relação à adoção de PETs, a mais frequentemente relatada, além dos custos e da falta de recursos, foi a existência de barreiras regulatórias e legais; quatro entidades relataram essa preocupação. Essa incerteza pode, por si só, criar outro tipo de custo além dos técnicos e operacionais: a necessidade de consultoria jurídica. De fato, uma entidade no Uruguai observou que, além da infraestrutura, seus "principais custos incluem (...) assessoria jurídica e possíveis modificações na aplicação para cumprir as políticas de privacidade".

CAPÍTULO 4

Recomendações

Considerando os resultados dos programas Open Loop em conjunto, as entidades no Brasil e Uruguai estão interessadas em implementar PETs e vislumbram seu potencial para a promoção dos princípios de proteção de dados. No entanto, há barreiras significativas no caminho dessas empresas. Muitas entidades (especialmente as pequenas e médias) não têm familiaridade com as PETs e o conhecimento técnico de como implementá-las. Além disso, a implementação de PETs (sobretudo as mais novas e tecnicamente mais complexas) gera incertezas e custos significativos. As PETs geralmente exigem investimentos financeiros expressivos em novas infraestruturas de dados e poder computacional, bem como funcionários com habilidades técnicas relevantes. Além desses custos, as entidades também enfrentam uma incerteza significativa sobre como seus usos de PETs se relacionam com várias disposições das leis de proteção de dados, desestimulando investimentos dispendiosos em PETs.

Esses desafios representam uma excelente oportunidade para os formuladores de políticas, que, assim como as entidades, estão reconhecendo cada vez mais o valor das PETs e buscando incentivar seu uso. Os resultados dos programas Open Loop fornecem um modelo para isso, identificando as causas básicas das incertezas e dos desafios dos participantes, aos quais os formuladores de políticas poderiam tentar abordar. Nesse sentido, esta seção fornece recomendações específicas e práticas que esperamos que sejam úteis.



RECOMMENDATION

4.1 Segurança regulatória e incentivos para a adoção de PETs

DETAILS

Os formuladores de políticas em todo o mundo têm a capacidade de elaborar ou modificar leis, regulamentos ou interpretações de forma a abordar a incerteza regulatória citada pelos participantes. Em particular, incentivamos os formuladores de políticas a:

Adotar uma abordagem flexível e baseada em riscos em relação ao conceito legal de anonimização

Para muitas entidades, saber que os resultados alcançados pelos usos das PETs podem ser considerados pelos órgãos reguladores como anonimização legal dos dados é um incentivo poderoso. Se os dados são anonimizados por meio do uso de PETs, as entidades podem fazer mais com esses dados. Mas, conforme discutido anteriormente, não está claro como as diferentes jurisdições tratam o conceito legal de anonimização. Algumas entidades, como o ICO do Reino Unido, a PDPC, e a IMDA de Singapura adotaram o que poderia ser considerado uma abordagem flexível e baseada em riscos. Essa abordagem reconhece que a anonimização não precisa significar a redução do risco de identificabilidade a quase zero; pode haver algum risco residual, embora pequeno. A mensuração do nível de risco deve ser uma avaliação específica do fato que considere o contexto do tratamento de dados, quais medidas técnicas (como PETs) foram aplicadas aos dados e quais medidas não técnicas (como controles de acesso e restrições legais) foram aplicadas aos dados. E, conforme observado pelo Tribunal Geral da UE no caso SRB, a avaliação do risco pode se concentrar em saber se as partes que realmente podem ter acesso aos dados poderiam reidentificá-los, considerando todas as proteções que foram aplicadas a eles, e não se qualquer terceiro hipotético com recursos ilimitados e acesso a outros dados poderia fazê-lo. Incentivamos os formuladores de políticas a seguir os passos do ICO do Reino Unido, da PDPC e da IMDA de Singapura e do Tribunal Geral da UE.

Esclarecer que as entidades podem tratar dados com a finalidade de reduzir o risco de identificabilidade

Além da incerteza sobre quando e como o uso de PETs pode anonimizar legalmente os dados, as entidades também enfrentam incertezas sobre se o uso de PETs é um tratamento justificado de dados pessoais em primeiro lugar. Embora isso esteja claramente alinhado com o objetivo das leis de proteção de dados, ou seja, aumentar a privacidade dos indivíduos, muitas leis não afirmam que esse tipo de tratamento é permitido. Incentivamos os formuladores de políticas a resolver essa deficiência.

Em particular, para jurisdições que se baseiam em leis semelhantes ao RGPD (aquelas que exigem uma base legal para tratar dados), os formuladores de políticas devem esclarecer que: (i) nenhuma base legal é necessária para o tratamento de dados com a finalidade de reduzir o risco de identificabilidade; ou (ii) interesses legítimos, ou uma base legal semelhante, podem ser prontamente invocados para conduzir o referido tratamento.

Para ambos os fins, também incentivamos os formuladores de políticas a explorar esses tópicos mais detalhadamente por meio de sandboxes regulatórios. Os sandboxes regulatórios podem oferecer oportunidades cruciais para que tanto os formuladores de políticas quanto às entidades aprendam juntos, especialmente em contextos (como o uso de PETs) que são tecnicamente complexos e novos.

RECOMMENDATION

4.2 Diálogos entre várias partes interessadas sobre boas práticas e padrões

DETAILS

Além de proporcionar segurança regulatória, os formuladores de políticas desempenham um papel valioso no avanço dos diálogos entre as diversas partes interessadas sobre as PETs. Os participantes do programa Open Loop consideraram extremamente valioso poder aprender com especialistas técnicos e em políticas sobre PETs, e os formuladores de políticas de todo o mundo poderiam desenvolver conversas semelhantes em suas jurisdições.

Essas conversas poderiam não só ajudar a desenvolver a capacidade das entidades de implementar PETs, mas também fazer avançar o desenvolvimento de uma compreensão compartilhada das PETs e de como elas podem ser usadas com eficácia em diferentes casos. Como discutido antes, as PETs são um grupo diversificado de técnicas que operam de maneiras muito diferentes e oferecem diversos tipos de proteção à privacidade. Isso significa que o que pode ser considerado uma melhor prática ou padrão para o uso de uma PET dependerá muito do que é a PET e do contexto em que ela está sendo implantada. Os formuladores de políticas poderiam promover diálogos para explorar essas complexidades, buscando a participação de órgãos de definição de padrões e associações de todo o setor no processo.

RECOMMENDATION

4.3 Investimento direto em pesquisa, desenvolvimento e educação

DETAILS

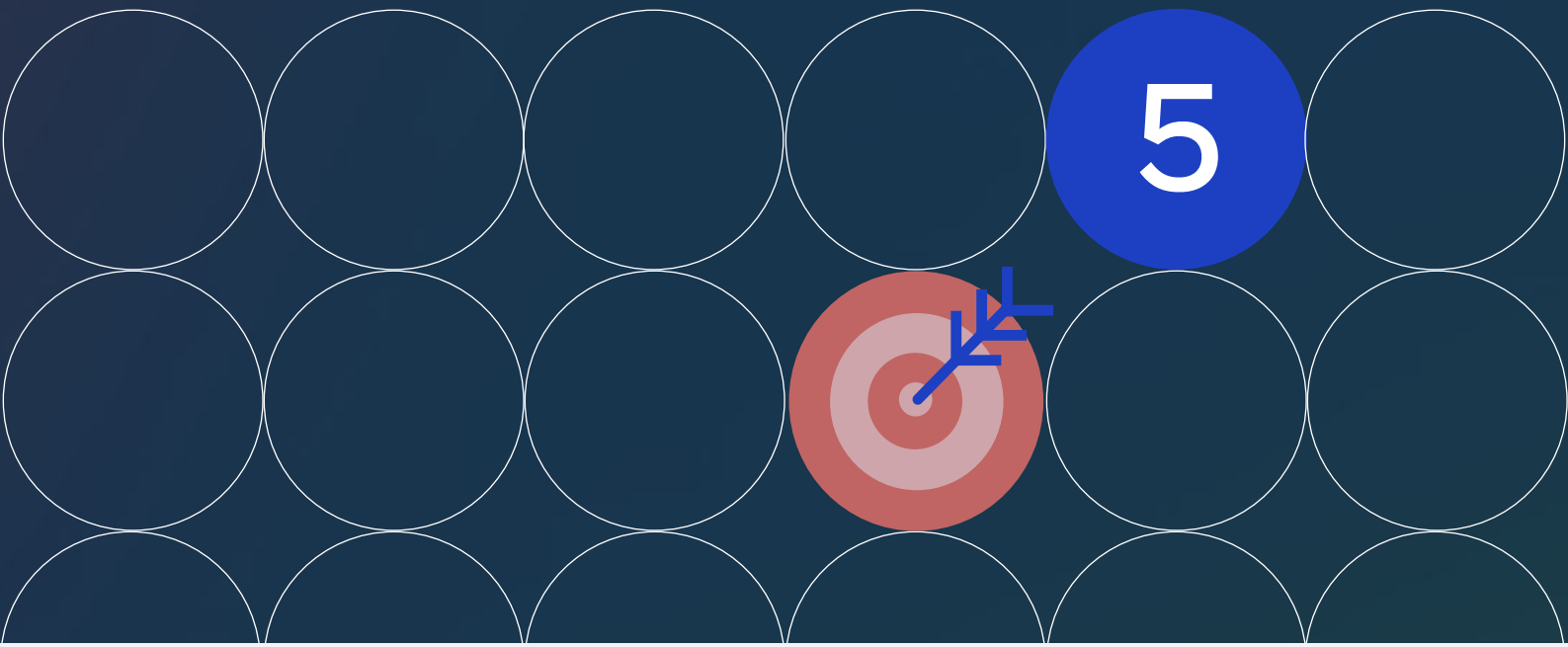
Por fim, incentivamos os formuladores de políticas a investir diretamente na pesquisa e no desenvolvimento de PETs, bem como na educação pública sobre os benefícios das PETs. Os resultados dos programas Open Loop mostraram que muitas entidades (especialmente as pequenas e médias) simplesmente não tinham os recursos e o financiamento para implementar PETs em escala. Esse desafio poderia ser enfrentado com o financiamento direto do governo em pesquisa e desenvolvimento, como fizeram os governos dos EUA e do Reino Unido por meio de seus desafios premiados, fornecendo incentivos diretamente às entidades para desenvolver e implantar PETs. Os formuladores de políticas também poderiam financiar a pesquisa e o desenvolvimento para implementações de PETs de código aberto, que poderiam ser usadas mais prontamente por entidades de pequeno e médio porte.

Além de pesquisa e desenvolvimento, os formuladores de políticas poderiam investir em campanhas educativas que ajudem a explicar às pessoas como as PETs podem proteger sua privacidade. Algumas entidades talvez não explorem as PETs se acharem que seus clientes ou usuários não entenderiam os benefícios de fazê-lo, especialmente quando a implementação de PETs exige grandes recursos. No entanto, uma maior conscientização do público sobre as PETs poderia resolver essa hesitação, tornando mais provável que os indivíduos apreciem os investimentos que as entidades fazem em PETs.

CAPÍTULO 5

Conclusão e próximas etapas

Em suma, os programas Open Loop no Brasil e no Uruguai ajudaram a promover uma maior compreensão das PETs e de como aplicá-las entre as empresas participantes. As sessões de capacitação e o Manual foram considerados úteis, mas os participantes enfrentaram desafios ao avaliar a implementação das PETs. Para muitos participantes, a implementação de PETs foi vista como um processo tecnicamente complicado e caro. E, embora os participantes tenham expressado um desejo maior de usar as PETs para promover os princípios de proteção de dados, não ficou claro como exatamente as PETs se relacionam com as leis de proteção de dados. Além disso, a consultoria jurídica sobre esse ponto foi outro custo a ser considerado. Esses aprendizados devem ser valiosos para os formuladores de políticas, ajudando-os a elaborar regulamentos e programas que aumentem a segurança regulatória, criem diálogos com várias partes interessadas e estimulem a pesquisa e o desenvolvimento dessas tecnologias promissoras.



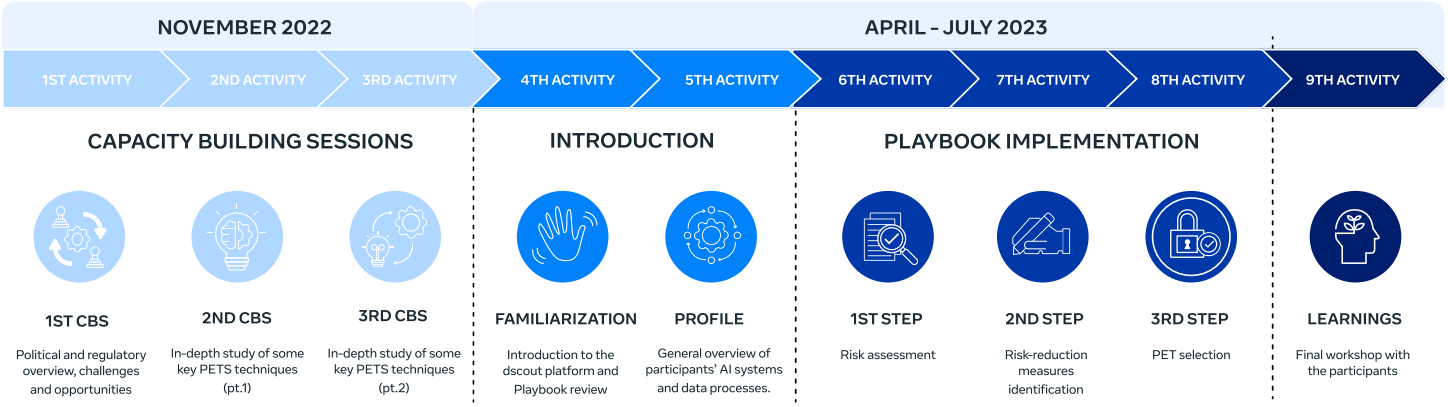
Anexo 1 - Metodologia

Escopo

Os programas Open Loop do Brasil e do Uruguai foram orientados pelas seguintes perguntas de pesquisa principais e abrangentes:

- **PP1: Com que grau de eficácia o protótipo de política equilibra a clareza da política, a viabilidade técnica e a eficiência da política para o público-alvo?**
- **PP2: Qual é a familiaridade e o entendimento atual das empresas sobre as PETs?**
- **PP3: Quais são as lacunas e os desafios de implementação atuais para a adoção de PETs pelas empresas participantes?**
- **PP4: Quais boas práticas e aprendizados podem contribuir para a adoção bem-sucedida de PETs com vistas a ajudar a desidentificar dados e reduzir os riscos relacionados à privacidade?**

Adotamos uma metodologia de pesquisa de método misto, incorporando uma combinação de métodos qualitativos e quantitativos. Coletamos dados de diferentes fontes: investigação documental, entrevistas, pesquisas e workshops. Essa abordagem de método misto nos permitiu triangular os dados e abordar as perguntas da pesquisa de acordo com várias perspectivas (veja a tabela abaixo).



Limitações e considerações:

A abordagem de métodos mistos proposta para este estudo é adequada para tratar das perguntas e dos objetivos da pesquisa. No entanto, as limitações da metodologia devem ser cuidadosamente consideradas ao interpretar os resultados deste relatório.

- **Dados autorrelatados:** a dependência de informações autorrelatadas introduz um possível viés, exigindo uma interpretação cautelosa.
- **Tamanho limitado da amostra:** embora represente diversos setores, o tamanho da amostra pode não capturar todas as nuances do setor ou práticas emergentes.
- **Escopo temporal:** a pesquisa capturou um ponto específico no tempo (de novembro de 2022 a julho de 2023), e as práticas podem evoluir com o tempo.

Essas limitações exigem uma interpretação cuidadosa dos resultados. A triangulação de dados de várias fontes e métodos atenua possíveis vieses. Embora não possa ser generalizada para toda a população, a pesquisa fornece tendências e insights valiosos no âmbito das organizações participantes. Pesquisas futuras podem expandir o escopo e abordar práticas emergentes.

Referências

[1] Del Pozo, C., Nuno Gomes de Andrade, N., & Rojas Arroyo, D. “Prototipo de Políticas Públicas sobre Transparencia y Explicabilidad de Sistemas de Inteligencia Artificial [Public Policy Prototype on the Transparency and Explainability of Artificial Intelligence Systems] (2023), at: https://openloop.org/ reports/2023/10/Public-Policy-Prototype-on-the-Transparencyand-Explainability-of-Artificial-Intelligence-Systems.pdf

[2] OCDE (2023). "Emerging privacy-enhancing technologies: Current regulatory and policy approaches" (Tecnologias emergentes de aprimoramento da privacidade: abordagens regulatórias e políticas atuais, em tradução livre), OECD Digital Economy Papers, No. 351, OECD Publishing, Paris, https://doi.org/10.1787/bf121be4-en.

[3] Conselho Nacional de Ciência e Tecnologia (2023). National Strategy to advance privacy-preserving data sharing and analytics, https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Strategy-to-Advance-Privacy-Preserving-Data-Sharing-and-Analytics.pdf

[4] Casa Branca (30 de outubro de 2023). Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence. Casa Branca. https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/

[5] Near, J., Darais, D., Lefkovitz, N. e Howarth, G. (11 de dezembro de 2023). Guidelines for Evaluating Differential Privacy Guarantees. https://csrc.nist.gov/pubs/sp/800/226/ipd

[6] Privacy Enhancing Technology Research Act, no. 4755, Science, Space, and Technology (2023). https://www.congress.gov/bill/118th-congress/house-bill/4755

[7] Information Commissioner’s Office (19 de junho de 2023) Privacy-enhancing technologies (PETs). Information Commissioner’s Office. https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-sharing/privacy-enhancing-technologies/

[8] U.K.-U.S. prize challenges | Privacy-Enhancing Technologies. (n.d.). Petsprizechallenges.com. Consultado em 2 de maio de 2024, disponível em https://petsprizechallenges.com/

[9] Conselho Europeu para a Proteção de Dados (2023). EDPB Work Programme 2023/2024. https://www.edpb.europa.eu/system/files/2023-02/edpb_work_programme_2023-2024_en.pdf

[10] SRB vs. EDPS, (Tribunal de Justiça da União Europeia, 26 de abril de 2023). https://gdprhub.eu/index.php?title=CJEU_-_Case_T-557/20_-_SRB_v._EDPS#:~:text=EDPS,-From%20GDPRhub&text=The%20European%20General%20Court%20ordered,alphanumeric%20codes%20constituted%20personal%20data.

[11] Infocomm Media Development Authority (n.d.). Privacy Enhancing Technology Sandboxes. Consultado em 2 de maio de 2024, disponível em https://www.imda.gov.sg/how-we-can-help/data-innovation/privacy-enhancing-technology-sandboxes

[12] Infocomm Media Development Authority (n.d.). Digital Advertising in a Paradigm Without 3rd Party Cookies. Consultado em 2 de maio de 2024, disponível em https://www.imda.gov.sg/-/media/imda/files/programme/pet-sandbox/imda-pet-sandbox--case-study--meta.pdf

[13] Kwon, S. (2 de fevereiro de 2024). In the era of artificial intelligence, standards for pseudonym processing for images, videos, voices, and texts have emerged. https://www.pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS074&mCode=C020010000&nttId=9899

[14] OECD (2023).

[15] Comitê de Especialistas da ONU em Big Data e Ciência de Dados para Estatísticas Oficiais. (n.d.). Task Team on Privacy Preserving Techniques — UN GWG for Big Data. Unstats.un.org. Consultado em 2 de maio de 2024, disponível em: https://unstats.un.org/bigdata/task-teams/privacy/index.cshtml

[16] A terminologia exata varia de acordo com a jurisdição, e este relatório usará "anonimizado" ou "anonimização" daqui para frente.

[17] Prorrogadas consultas sobre guia de anonimização e norma de direitos dos titulares (28 de fevereiro de 2024). Autoridade Nacional de Proteção de Dados. https://www.gov.br/anpd/pt-br/assuntos/noticias/prorrogadas-consultas-sobre-guia-de-anonimizacao-e-norma-de-direitos-dos-titulares . Sobre o tema, a ANPD publicou um estudo técnico, disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/documentos-de-publicacoes/estudo_tecnico_sobre_anonimizacao_de_dados_na_lgpd___analise_juridica.pdf