Proteção de dados pessoais por governos digitais: aplicação de PETs para aprimorar a privacidade dos cidadãos

Marta Juvina de Medeiros
Universidade de Brasília (UnB)
Departamento de Engenharia Elétrica
Brasília-DF, Brasil
medeiros.marta@gmail.com

Edna Dias Canedo
Universidade de Brasília (UnB)
Departamento de Ciência da Computação
Brasília-DF, Brasil
ednacanedo@unb.br

Abstract
This article analyzes the role of Privacy Enhancing Technologies (PETs) in protecting personal data and ensuring citizens' privacy in the context of governments that anchor public services on digital platforms. As services digitization advances, the volume and complexity of data processing increases, amplifying risks and intensifying the need for solutions that ensure the privacy and security of citizens' data. PETs are a diverse set of techniques and tools that allow for the processing of personal data, whether sensitive or not, ensuring confidentiality, integrity, and availability without compromising individual privacy, protecting data not only at rest and in transit, but also during use. The article addresses fundamental concepts of privacy and personal data protection, details categories and current examples of PETs, and discusses technical, legal, and organizational challenges for their adoption in public administration. By emphasizing the potential of PETs to mitigate risks and promote ethical data governance, the article presents tools and frameworks that aid in selecting PETs for various treatment scenarios. The article presents a case study based on qualitative documentary analysis of decrees published by the federal executive branch in 2025 that regulate the use of personal data in different segments. Recommendations are made on which PETs should be applied to improve privacy and personal data protection in these segments. The article concludes by pointing out the institutional challenges, the need for training, and the strategic role of PETs in balancing innovation and the protection of fundamental rights in the government digital environment.

Keywords: PETs. Personal data protection. Privacy. Digital governments.

Resumo
Este artigo analisa o papel das *Privacy Enhancing Technologies* (PETs) na proteção de dados pessoais e para assegurar a privacidade dos cidadãos no contexto de governos que ancoram serviços públicos em plataformas digitais. À medida que a digitalização dos serviços avança, o volume e a complexidade dos tratamentos de dados aumentam, potencializando os riscos e intensificando a necessidade de soluções que assegurem a privacidade e a segurança dos dados dos cidadãos. As PETs apresentam-se como um conjunto diversificado de técnicas e ferramentas que permitem processar dados pessoais, sensíveis ou não, garantindo confidencialidade, integridade e disponibilidade, sem comprometer a privacidade individual, protegendo os dados não apenas em repouso e em trânsito, mas também durante o uso. O artigo aborda conceitos fundamentais de privacidade e proteção de dados pessoais, detalha categorias e exemplos atuais de PETs, e discute desafios técnicos, legais e organizacionais para sua adoção na administração pública. Ao destacar o potencial das PETs para mitigar riscos e apoiar a governança ética

dos dados, registra ferramentas e *frameworks* que auxiliam a escolha de PETs para diferentes cenários de tratamento. O artigo apresenta um estudo de caso, fundamentado em análise qualitativa documental e baseado em decretos publicados pelo Poder Executivo federal no ano de 2025 que regulamentam o uso de dados pessoais em diferentes segmentos, para os quais são apontadas recomendações de PETs a serem aplicadas para aprimorar a privacidade e a proteção de dados pessoais. Finaliza apontando os desafios institucionais, a necessidade de capacitação e o papel estratégico das PETs para equilibrar inovação e proteção dos direitos fundamentais no ambiente digital governamental.

Palavras-chave: PETs. Proteção de dados pessoais. Privacidade. Governos digitais.

1. Introdução

Os governos federal, estaduais, distrital e municipais do Brasil, aqui denominados governos digitais, vêm evoluindo seus processos para melhorar a prestação de serviços públicos com o auxílio das tecnologias da informação e comunicação.

No âmbito nacional, o Programa de Governo Eletrônico implementou inovações objetivando aprimorar a qualidade do serviço público; mas foi a partir da publicação da Estratégia de Governança Digital [EGD, 2016] que ocorreu o incremento de um novo paradigma de gestão pública e de prestação de serviços eletrônicos à sociedade pelo Estado brasileiro. A EGD, com sua política de governança digital, tem viabilizado um Estado moderno, simplificado, ágil, com mais transparência e ainda mais avanços no atendimento ao público.

O alcance desses aprimoramentos tornou-se possível em virtude da Internet e do conjunto de tecnologias da informação a ela associadas, impulsionando a inovação em múltiplos setores e viabilizando maior comodidade aos cidadãos e acesso ampliado a serviços públicos – sejam eles concebidos originalmente na era digital ou digitalizados.

Incrementar a disponibilidade de serviços públicos digitais resulta em aumento substancial do volume e da complexidade do tratamento dos dados pessoais, o que pode acarretar impactos negativos à privacidade dos indivíduos por eventuais falhas na governança e na gestão dos riscos de privacidade e de proteção de dados pessoais [Doneda, 2021]. Isso demanda que os governos preservem os benefícios proporcionados pelos serviços digitais aos cidadãos, ao mesmo tempo em que intensifica a necessidade de implementar medidas rigorosas de proteção de dados pessoais em seus processos, serviços e soluções.

Nesse contexto, as *Privacy Enhancing Technologies* (Tecnologias de Aprimoramento da Privacidade), ou PETs, idealizadas para proteger a privacidade dos indivíduos, apresentam-se como um conjunto de tecnologias, abordagens e ferramentas digitais que permitem o processamento de dados e, ao mesmo tempo em que protegem a confidencialidade, a integridade e a disponibilidade dos dados pessoais, preservam a privacidade dos cidadãos e os interesses dos controladores de dados [OCDE, 2023].

As PETs objetivam proteger os dados durante o processamento e efetivo uso, representando um avanço na cibersegurança – pois não impedem que os processos, serviços e soluções realizem suas necessárias funções. Visto não se limitarem mais a proteger os dados apenas em repouso e em trânsito, fornecem segurança de ponta a ponta por proteger os dados em uso [d'Aliberti; Gronberg; Kovba, 2024].

A importância das PETs foi ratificada por governos e órgãos reguladores de proteção de dados pessoais, que identificaram e enfatizaram tal abordagem como solução proeminente para a privacidade e a proteção de dados pessoais [OCDE, 2023], muito em razão da proliferação de aplicações de governo eletrônico como ferramenta para aumentar a efetividade do serviço público [CE, 2007]. Ao exercerem papel crucial para implementar a privacidade desde a concepção (*privacy by design, PbD*), as PETs viabilizam maior conformidade à Lei Geral de Proteção de Dados Pessoais, LGPD [Brasil, 2018], pois asseguram mecanismos para que a proteção da privacidade seja incorporada desde a concepção do produto ou serviço.

Contudo, as PETs não representam uma solução completa e definitiva para todos os problemas de privacidade e proteção de dados pessoais. Sua eficácia depende da utilização conjunta a ferramentas organizacionais e legais, e sua implementação exige um programa de governança em privacidade cuidadosamente estruturado, baseado em gestão de riscos, além de um plano de implementação que acomode as necessidades advindas da contínua prestação de serviços públicos digitais pelos governos.

Neste artigo, discutiremos como as PETs podem auxiliar a aplicação de ferramentas e tecnologias para viabilizar a proteção de dados pessoais, mitigando riscos à privacidade dos usuários de serviços públicos. Na seção 2, trataremos da diferença entre privacidade e proteção de dados pessoais, conceitos que ainda geram diferentes entendimentos; na seção 3, abordaremos a importância das PETs para assegurar privacidade, discorrendo sobre conceitos, histórico e categorias; na seção 4, por sua vez, exibiremos breves informações sobre as principais PETs em uso na atualidade; na seção 5, apresentaremos alguma ferramentas disponíveis que objetivam recomendar o uso de PETs a partir de situações concretas de tratamento de dados pessoais; na seção 6, demonstraremos motivações e desafios para o uso de PETs no âmbito dos governos digitais; por fim, na seção 7 realizaremos um análise qualitativa documental acerca de decretos publicados pelo Poder Executivo federal no ano de 2025, adicionando recomendações sobre possibilidades de uso de PETs para aprimorar a privacidade dos cidadãos.

2. Entre a privacidade e a proteção de dados pessoais

A conceituação de privacidade e proteção de dados pessoais, e consequente distinção entre as duas disciplinas, é crucial para uma análise e compreensão das tecnologias de aprimoramento da privacidade e seus alcances.

2.1. O direito à privacidade

O direito à privacidade tem seu marco inicial no artigo *The right to privacy* [Warren; Brandeis, 1890], que, na defesa da privacidade como uma extensão da proteção jurídica contra danos físicos e difamação, abrangeu principalmente o direito de a pessoa ser deixada só, em paz. Isso porque, diante dos avanços tecnológicos e sociais alcançados até aquele momento, tornou-se necessário garantir ao indivíduo o controle sobre a divulgação de suas informações pessoais, emoções e pensamentos para preservar sua dignidade e bem-estar. A lei tradicional, até então, protegia contra danos físicos e difamatórios, mas carecia de mecanismos específicos para proteger contra a invasão pela então imprensa sensacionalista e por tecnologias como fotografia instantânea, capazes de revelar aspectos reservados da vida privada sem o consentimento do indivíduo [Warren; Brandeis, 1890].

O texto, fundamental para o desenvolvimento contemporâneo do direito à privacidade por influenciar doutrinas jurídicas e políticas públicas relacionadas ao tema,

concluiu que o direito deveria evoluir para proteger eficazmente a privacidade, antecedendo legislações específicas e proporcionando mecanismos civis para reparação do indivíduo, como indenizações e medidas cautelares contra invasões.

Mais de cem anos depois, o conceito de privacidade ainda não é bem compreendido, e sofre de um embaraço de significados [Solove, 2006]. Ao tratar a privacidade como um conjunto complexo de problemas concretos que afetam o indivíduo e a sociedade de múltiplos modos, e não como um conceito unitário e abstrato, Solove propõe uma abordagem taxonômica que se concentra na identificação e detalhamento das atividades que representam problemas de privacidade, apresentando quatro grandes grupos da privacidade sob a ótica de sua violação: coleta de informação (vigilância, interrogatório), processamento da informação (agregação, identificação, insegurança, uso secundário e exclusão), disseminação da informação (violação de confidencialidade, divulgação, exposição, aumento da acessibilidade, chantagem, apropriação, distorção) e invasão (intrusão e interferência nas decisões).

Devido ao dinamismo do conceito de privacidade, sua evolução no tempo ocorre especialmente em face das transformações tecnológicas e do intenso fluxo informacional. A concepção inicial de privacidade, associada ao isolamento, reclusão ou segredo, mostrou-se insuficiente com o passar dos tempos. Isso porque as demandas que moldam o perfil contemporâneo da privacidade estão relacionadas à informação pessoal e condicionadas pela tecnologia, que representa o elemento central a modificar a condição da informação, levando ao surgimento de estruturas jurídicas e sociais para tratar o problema da privacidade [Doneda, 2021].

A privacidade está fortemente ligada à personalidade e ao seu desenvolvimento, sendo um elemento essencial para tal e um pré-requisito fundamental para o exercício de diversas outras liberdades fundamentais em uma sociedade democrática. Isso garante espaço para o indivíduo pensar, desenvolver ideias, experimentar e seguir seu próprio caminho de vida livremente – e desta forma, livre, garantir o desenvolvimento de sua personalidade frente ao avanço do intenso e contínuo monitoramento estatal e do setor privado sobre as pessoas [Doneda, 2021].

Como direito fundamental, essencial para a autonomia e a proteção da dignidade humana, a privacidade cria barreiras e gerencia limites para proteger os indivíduos de interferências injustificadas em suas vidas, sendo a base sobre a qual outros direitos humanos são fundamentados. O direito à privacidade está consagrado nos principais marcos normativos internacionais, incluindo a Declaração de Direitos Humanos das Nações Unidas, de 1948, e o Pacto Internacional sobre Direitos Civis e Políticos, de 1966.

Nesse diapasão, a Constituição Brasileira [Brasil, 1988] trata o direito à privacidade principalmente no inciso X do artigo 5º, que estabelece serem invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas; também protege o sigilo da correspondência e das comunicações telegráficas, telefônicas e de dados. Portanto, assegura proteção ampla da privacidade, considerando aspectos de integridade, dignidade e autonomia pessoal, e estabelece mecanismos para reparação em casos de sua violação.

2.2. O direito à proteção de dados pessoais emerge do direito à privacidade

A disciplina da proteção de dados pessoais nasce a partir de um desdobramento da privacidade, sendo considerada sua continuação por outros meios [Doneda, 2021]. Surge da necessidade de funcionalização da proteção da privacidade para lidar com os desafios

impostos pela tecnologia e o tratamento massivo de informações pessoais, cuja magnitude aumentou consideravelmente na sociedade pós-industrial.

A demanda por uma nova abordagem da privacidade tornou-se evidente com casos emblemáticos: nos EUA, debates sobre o *National Data Center* na década de 1960 revelaram os riscos da coleta massiva de dados pelo Estado [Hauptmann, 2024], levando à compreensão de que poderia ser questionada a concentração estatal acerca do poder informacional; na Alemanha, a sentença sobre o microcenso de 1969 foi crucial, pois desmistificou a ideia de que o tratamento de certos dados pessoais seria irrelevante para a privacidade e estabeleceu o direito à autodeterminação informativa – criando um marco para a disciplina da proteção de dados ao ressaltar que o indivíduo tem o poder essencial de decidir sobre a divulgação e utilização de seus dados pessoais, [Mendes, 2020].

Enquanto a privacidade tradicionalmente visa o isolamento e a proteção contra intromissões diretas, a proteção de dados pessoais é a disciplina moderna que foca no controle, inclusive pelo próprio indivíduo, da informação pessoal em circulação. Com isso, garante a autodeterminação, a não discriminação ilícita e o livre desenvolvimento da personalidade face às complexidades trazidas pela tecnologia e pelo tratamento de dados em larga escala – assegurando, por meio de um regime de deveres, princípios e fiscalização institucional, a proteção dos dados pessoais.

Emergiu, então, a constatação da mudança do direito à privacidade, que passa a focar no eixo pessoa-informação-circulação-controle em substituição ao eixo pessoa-informação-segredo [Rodotà, 2008]. Como uma disciplina sofisticada, a proteção de dados pessoais adapta-se à sociedade da informação para atuar na continuação da privacidade por outros meios, garantindo a efetiva tutela da pessoa sobre seus dados. Representa uma garantia de caráter instrumental para a proteção da personalidade e do livre desenvolvimento do indivíduo.

As *Guidelines* da Organização para a Cooperação e o Desenvolvimento Econômico [OCDE, 1980] e a Convenção 108 do Conselho da Europa [Conselho, 1981] são marcos normativos sobre proteção de dados pessoais, pois estabeleceram princípios comuns e reconheceram referida proteção como um tema de direitos humanos. A Diretiva 95/46/CE [UE, 1995] e o Regulamento Geral de Proteção de Dados (GDPR) [UE, 2016] padronizaram a disciplina no contexto europeu, equilibrando a proteção de direitos fundamentais com a livre circulação de dados.

No Brasil, a proteção de dados pessoais encontra seu principal marco normativo na LGPD – que estabelece princípios para o adequado tratamento dos dados, tais como finalidade, necessidade, transparência e segurança, além de definir dado pessoal como toda informação relacionada à pessoa natural identificada ou identificável. Visto que a tutela exercida exclusivamente pelo titular mostra-se insuficiente diante da assimetria de poder em relação às organizações que processam tais dados, destaca-se a atuação da Autoridade Nacional de Proteção de Dados (ANPD), que exerce funções de fiscalização, regulamentação e aplicação de sanções, garantindo direitos e consolidando-se como elemento central na governança da proteção de dados pessoais no país.

Ademais, o maior reconhecimento nacional acerca da relevância da nova disciplina de proteção de dados pessoais teve seu marco regulatório em fevereiro de 2022, com a Emenda nº 115 incluindo na Constituição Brasileira, entre os direitos e garantias fundamentais dispostos no art. 5º, o direito à proteção de dados pessoais. A Emenda proporcionou maior segurança jurídica e atribuiu à União a competência para organizar, implementar e fiscalizar a proteção de dados pessoais tratados nos contextos digital e físico.

2.3. Riscos à privacidade e à proteção de dados pessoais

Para os indivíduos, os desafios para preservar a privacidade e proteger seus dados pessoais são multifacetados, exigindo também sua tutela em sentido amplo contra diversas formas de controle, vigilância e discriminação ilícita – para além das salvaguardas aplicadas pelos agentes de tratamento de dados pessoais.

Há uma dificuldade crescente dos cidadãos em controlar o fluxo incessante de informações e em compreender as variadas formas de tratamento dos dados, o que pode resultar na perda de autonomia, individualidade e autodeterminação. Ademais, tratamentos inadequados de dados pessoais podem acarretar prejuízos à reputação e à honra; danos à imagem pública, discriminação ilícita e exclusão social; danos psicológicos e subjetivos; impactos profissionais e econômicos; riscos de manipulação e controle, entre outros.

O consentimento, base legal fundamental do tratamento de dados pessoais para assegurar a autodeterminação informativa, muitas vezes revela-se uma ficção – dada a assimetria informacional no tratamento dos dados e a opacidade das consequências para seu titular.

Dados pessoais considerados comuns, quando combinados, podem revelar aspectos sensíveis da personalidade, facilitando a discriminação ilícita e o traçado de perfis comportamentais que criam riscos futuros de dano subjetivo – cujos impactos são, diversas vezes, desconhecidos pelo titular.

O excessivo uso de dados pessoais, seja por incompreensão de seu negativo impacto ou indiferença em relação aos potenciais problemas, leva ao aumento da superfície de ataques e da probabilidade de ocorrência de incidentes de segurança com os dados. Esse fator é potencializado na atualidade pelo crescimento de explorações de vulnerabilidades com o uso de inteligência artificial (IA).

Abordagens tecnológicas tradicionais de preservação da privacidade, como a remoção de atributos identificáveis dos registros de dados pessoais, notadamente falham. Isso porque os dados desidentificados podem muitas vezes ser reidentificados por meio de técnicas como a vinculação de registros, que se utilizam de dados disponíveis publicamente. Casos clássicos de falhas compreendem um ataque famoso a um conjunto de dados hospitalares desidentificados que, com a vinculação de apenas três atributos dos pacientes a registros eleitorais disponíveis publicamente, reidentificou indivíduos [Wood et al, 2018]; em outro, após o *Netflix Prize* liberar dados anonimizados sobre avaliações de filmes, feitas por centenas de milhares de usuários, demonstrou-se a possibilidade de reidentificação de usuários por cruzamento de suas avaliações com informações públicas sobre produções audiovisuais [Narayanan; Shmatikov, 2008].

Diante de tantos riscos, torna-se imperativo adotar estratégias inovadoras e abrangentes de proteção de dados pessoais, capazes de garantir maior segurança e defesa da privacidade.

3. PETs e sua importância no cenário da proteção de dados pessoais

A crescente preocupação com a privacidade e a proteção de dados pessoais tem impulsionado o desenvolvimento de abordagens para mitigar riscos e assegurar direitos dos indivíduos.

3.1. Conceito e finalidades

PETs são técnicas, processos, regulações ou procedimentos que objetivam tutelar os dados pessoais, podendo adotar qualquer meio projetado para atuar na arquitetura da privacidade – impossibilitando, limitando ou mesmo facilitando uma determinada ação relativa ao tratamento dos dados. Possuem foco nos titulares e na mitigação dos riscos a que estão submetidos ao terem seus dados pessoais tratados.

No geral, definições e categorizações sobre PETs são influenciadas pelo contexto em que foram desenvolvidas [Doneda, 2021], refletindo o estado da tecnologia em um determinado momento, ou ainda o objetivo de um estudo ou projeto apoiado por PETs.

No segmento tecnológico, referem-se a uma ampla gama de tecnologias que ajudam a proteger a privacidade do indivíduo, desde ferramentas que proporcionam anonimato até aquelas que permitem que o usuário escolha se, quando e em quais circunstâncias suas informações serão divulgadas. Podem ser usadas em conjunto com outras ferramentas organizacionais e legais para implementar os objetivos de governança de dados, assim como podem depender umas das outras para potencializar o alcance de seus objetivos.

PETs são também conhecidas como soluções de *software* e *hardware* que englobam processos técnicos, métodos ou conhecimento para alcançar uma funcionalidade específica de privacidade ou proteção de dados, ou para proteger contra riscos à privacidade de um indivíduo ou de um grupo de pessoas físicas [ENISA, 2016a], introduzindo novas proteções de privacidade e segurança digital no tratamento dos dados.

Embora o termo seja normalmente utilizado para referir-se a tecnologias ou abordagens que auxiliam na mitigação dos riscos à privacidade e segurança dos dados pessoais, não existe uma definição única para PET. Entretanto, o objetivo é único: buscam conformidade com a legislação e com requisitos éticos e técnicos de privacidade e proteção de dados pessoais.

Como abordagens desenhadas para proteger o processo de dados em uso sem impedir que o sistema cumpra suas funções necessárias, as PETs visam também [d'Aliberti; Gronberg, Kovba, 2024]: permitir que as partes colaborem, garantindo que quaisquer dados compartilhados sejam usados apenas para os fins pretendidos; obter insights a partir de dados pessoais sem revelar o conteúdo sensível dos dados; realizar cálculos confiáveis em um ambiente não confiável; proteger o acesso a modelos compartilhados de IA sem revelar dados confidenciais; adicionar proteções de dados resistentes à tecnologia quântica ao sistema; aumentar a capacidade dos proprietários manterem o controle ao longo do ciclo de vida dos seus dados.

Como as PETs podem variar de uma única ferramenta técnica a uma implementação completa, compreendendo desde normas até aplicação de tecnologias específicas dependendo do contexto, do escopo e da própria operação de processamento, não há uma solução única para todas as situações em que PETs são aplicáveis. Isso porque representam um processo sistemático, que objetiva traduzir em termos práticos e operacionais os princípios da privacidade desde a concepção (PbD) no ciclo de vida dos sistemas de informação nos quais há tratamento de dados pessoais.

É importante ressaltar que, embora o termo PETs e suas definições mais abrangentes tenham se consolidado no início dos anos 2000, técnicas específicas com propósitos de aprimoramento da privacidade existiam antes [Dwork; Roth, 2014]. No *Randomized Response* (Resposta Aleatória), que remonta aos anos 1960, S.L. Warner aborda a coleta de informações sensíveis ao tempo em que protege a privacidade dos participantes, de modo que estes não respondessem a uma pergunta de forma verídica, mas sim

aleatorizassem sua resposta antes de enviá-la – proporcionando negabilidade plausível às respostas apresentadas e protegendo a privacidades dos titulares.

3.2. Histórico e categorias

Um dos primeiros trabalhos a explorar de forma sistemática e interdisciplinar a proteção da privacidade dos indivíduos em ambientes digitais propôs conceitos como a proteção da identidade (*identity protector*) e o uso de técnicas avançadas de anonimização e pseudonimização [*Information and Privacy Commissioner/Ontario*; *Registratiekamer*, 1995]. Ao lançar as bases para o desenvolvimento e a aceitação das PETs como ferramentas essenciais para equilibrar o uso de dados com a proteção de direitos fundamentais, o relatório destacou a importância da integração da privacidade no projeto de sistemas e enfatizou a necessidade da conscientização e educação sobre tais tecnologias.

A demanda por ampliar o anonimato e dificultar o rastreamento de indivíduos fez surgir tecnologias para permitir identidades ocultas no envio de *e-mails*, postagem em grupos de notícias, navegação na *web* e pagamentos *on-line* [Goldberg; Wagner; Brewer, 1997], visto que as pessoas haviam percebido que tudo o que diziam ou faziam *on-line* poderia ser registrado, arquivado e pesquisado, em razão da franca expansão da internet.

Também em consequência das ameaças trazidas por mecanismos comuns de identificação e perfilamento de usuários, PETs como criptografia, protetores de identidade, gerenciamento de *cookies* e *anonymizers* [Jerman-Blazic, 2003] já ofereciam meios promissores para restaurar o equilíbrio entre indivíduos e controladores de dados.

Ao sinalizar como evoluíram no período de dez anos, [Goldberg, 2007] agrupa as PETs em três classes: sistemas de anonimização e pseudonimização de *e-mails*, para proteger as identidades dos remetentes e destinatários de *e-mail*; sistemas de anonimização e pseudonimização interativos, para tentar mitigar a complexidade de proteger a identidade dos indivíduos ao acessar serviços interativos da internet; e sistemas de privacidade de comunicação, para proteger o conteúdo das conversas na internet, sem revelar as identidades dos internautas. Destaca, ainda, quatro propriedades que as tecnologias devem possuir: usabilidade, implementabilidade, eficácia e robustez.

O agrupamento proposto por [Shen; Pearson, 2011] ganha relevo por utilizar a taxonomia de privacidade de [Solove, 2006] – que caracteriza e classifica os danos à privacidade do usuário – para estruturar as PETs que podem ser usadas para mitigar referidos danos em técnicas para: anonimizar (técnicas de comunicação anônimas e técnicas de anonimização variadas); proteger contra invasões de redes; gerenciar identidades (sistemas de credencial, gestão da confiança); processar dados (preservar a privacidade na mineração de dados, gerenciar a privacidade em repositórios de dados); e verificar políticas.

Com o foco em recursos *on-line*, a [ENISA, 2016a] categoriza as PETs por tipo de ferramenta: mensagens seguras, redes privadas virtuais (*virtual private networks*, VPNs), redes de anonimização e ferramentas antirrastreamento (para navegação *on-line*). Embora admita a existência de outras categorias, a Agência segmenta seu estudo em razão da popularidade e do uso crescente dos dispositivos móveis, ao tempo em que disponibiliza a matriz de controle das PETs – que corresponde a um quadro de avaliação e ferramental para apresentação e avaliação sistemáticas de mecanismos de privacidade.

A taxonomia abrangente de [Kaaniche; Laurent; Belguith, 2020] classifica as PETs em três grupos principais, conforme o responsável por proteger a privacidade: técnicas do lado do usuário (*User-Side Techniques*), que exigem que o próprio indivíduo adote medidas

para proteger sua privacidade; técnicas do lado do servidor (*Server-Side Techniques*), que exigem do provedor de serviços a execução de processamento para garantia da privacidade; e técnicas do lado do canal (*Channel-Side Techniques*), cujas segurança e privacidade concentram-se nas propriedades do canal de comunicação entre o usuário e o servidor.

Ao renovar a categorização de PETs formulada previamente em 2002, a [OCDE, 2023] destaca a necessidade de a taxonomia ser neutra em termos de tecnologia e robusta ao longo do tempo, agrupando PETs conforme princípios básicos de suas Diretrizes de Privacidade: ofuscação de dados; processamento de dados criptografados; análise federada e distribuída e ferramentas de *accountability* de dados.

Há, ainda, classificação de PETs entre aquelas que fornecem privacidade de entrada (i-PETs) e de saída (o-PETs) [UNCEBD, 2023], taxonomia fundamental para entender a aplicação da privacidade em diferentes etapas do ciclo de vida dos dados. Embora haja algumas divergências conceituais na categorização das PETs conforme abordagem de entrada ou de saída, ou até em ambas, no geral:

- i-PETs podem reduzir significativamente o número de partes com acesso aos dados pessoais tratados e preconizam que a parte que realiza o processamento não pode: acessar as informações pessoais; acessar valores intermediários ou resultados estatísticos durante o processamento (a menos que o valor tenha sido especificamente selecionado para compartilhamento); ou derivar entradas usando qualquer tipo de técnica (a exemplo de ataques de canal lateral, ou *side-channel atacks*). Exemplos de i-PETs: computação multiparte segura e provas de conhecimento zero;
- o-PETs: mitigam o risco de obter ou inferir informações pessoais a partir dos dados de saída resultantes de uma atividade de processamento, ainda que não tenha sido fornecida privacidade de entrada. É útil para disponibilizar estatísticas anônimas publicamente ou compartilhar os resultados de uma análise com um grande grupo de destinatários. Exemplos de o-PETs: privacidade diferencial e k-anonimato.

4. Algumas PETs do segmento tecnológico

Tecnologias de Aprimoramento da Privacidade representam um conjunto diversificado de ferramentas e abordagens desenvolvidas para proteger os dados pessoais e a privacidade dos indivíduos, ao tempo em que permitem o uso e a análise dos dados para diversas finalidades legítimas. Algumas PETs disponíveis no segmento tecnológico, cujos conceitos são aqui brevemente abordados, são:

Privacidade Diferencial (*Differential Privacy*): destaca-se como uma das mais rigorosas abordagens tecnológicas para a proteção dos dados pessoais, pois oferece garantia matemática de que a presença ou ausência de qualquer indivíduo no conjunto de dados não afeta significativamente o resultado da análise. Isso significa que o resultado não deve ser alterado se dados de uma única pessoa forem adicionados ou removidos do conjunto. Essa característica torna a abordagem imune a ataques que utilizam informações auxiliares, mesmo aqueles que o controlador de dados não poderia prever. Opera introduzindo ruído ou perturbação nos resultados das consultas ou nos próprios dados antes da análise, de forma controlada e quantificável, de modo que, na saída de um algoritmo aplicado a um banco de dados, não é possível inferir se os dados de uma pessoa específica foram incluídos ou excluídos da análise. A quantidade de ruído adicionado é um ponto crucial, representando um equilíbrio entre proteção da privacidade e utilidade dos dados, sendo gerenciado por um

parâmetro denominado *epsilon* (ε), onde valores menores de ε indicam uma proteção de privacidade mais forte, mas resultam em menor precisão dos resultados. Uma de suas características distintivas é a robustez sob composição, que quantifica e gerencia o acúmulo de risco de privacidade mesmo quando múltiplas análises são realizadas sobre os mesmos indivíduos, algo que nenhum outro *framework* conhecido pode medir com precisão [Wood et al, 2018]. Para alcançar essa proteção, são empregadas técnicas e mecanismos tais como: os mecanismos de Laplace e o Exponencial, a Resposta Aleatorizada (*Randomized Response*); a Técnica do Vetor Esparso (*Sparse Vector Technique*) [Dwork; Roth, 2014]. Possui alta complexidade técnica, exigindo conhecimentos aprofundados em matemática discreta e probabilidade. Amplamente útil em processos de *machine learning* (ML), onde pode garantir que a contribuição de cada usuário individual não resulte em um modelo significativamente diferente, pode ser aplicada em diferentes estágios do desenvolvimento de modelos de ML: no nível dos dados de entrada (proteção mais forte), durante o treinamento ou na inferência (proteção mais fraca).

Computação Segura Multiparte (*Secure Multiparty Computation, SMPC*): tecnologia criptográfica que permite a múltiplos agentes colaborem na computação de uma função a partir de suas entradas privadas, sem que nenhum agente precise revelar seus próprios dados ao outro. Este conceito é fundamental para cenários onde a colaboração entre agentes de tratamento de dados pessoais é necessária e a confidencialidade dos dados é primordial, como em análises financeiras conjuntas entre bancos, pesquisas de saúde envolvendo dados de diferentes hospitais, ou até mesmo leilões e votações secretas. Prescinde da necessidade de uma parte confiável central que tenha acesso a todos os dados brutos. Ao distribuir a computação por entre as partes participantes, a SMPC assegura que nenhuma informação privada seja exposta inadvertidamente, mitigando riscos de vazamento ou uso indevido [Lindell, 2020].

Criptografia Homomórfica (*Homomorphic Encryption*): uma das mais visionárias e com grande potencial no tratamento de dados confidenciais, realiza operações computacionais diretamente sobre dados que já foram criptografados, sem a necessidade de descriptografá-los em nenhum momento [CIPL, 2023]. De extrema importância para cenários onde o tratamento dos dados ocorre em ambientes não confiáveis, como a nuvem pública, ou em situações de análise de dados colaborativa onde as partes não desejam compartilhar seus dados brutos, elimina o período de vulnerabilidade em que os dados seriam expostos. Possui limitações como complexidade computacional e de implementação, custos elevados, desempenho, tamanho dos dados criptografados e gestão de chaves em ambientes multiusuários ou distribuídos.

Dados Sintéticos (*Synthetic Data*): envolve a criação artificial de conjuntos de dados que replicam as propriedades estatísticas e os padrões de dados reais, mas que não contêm nenhuma informação original de indivíduos [CIPL, 2023]. Oferece uma solução poderosa para o dilema da privacidade, pois permite que desenvolvedores, pesquisadores e analistas trabalhem com dados que se comportam de maneira semelhante aos dados reais, sem o risco de expor dados pessoais, inclusive sensíveis. Dados sintéticos são valiosos para desenvolvimento e teste de *software*, criação de modelos de IA e condução de estudos e análises estatísticas em ambientes altamente regulados. Sua eficácia depende de sua qualidade, de modo que não introduzam vieses ou artefatos que possam levar a conclusões incorretas ou à revelação inadvertida de informações sensíveis.

Aprendizagem Federada (*Federated Learning*): abordagem inovadora, utilizada para treinar modelos de algoritmos de IA em múltiplos conjuntos de dados localizados e descentralizados, sem a necessidade de que esses dados sejam fisicamente coletados ou

centralizados em um único local. Nessa técnica, os dados pessoais permanecem nos dispositivos ou servidores locais de origem, que recebem cópia do modelo de *machine learning* para treinar o modelo usando tais dados [OCDE, 2023]. Após o treinamento local, as atualizações ou parâmetros do modelo são transmitidas para o servidor central que, por sua vez, agrega as atualizações dos múltiplos dispositivos ou entidades para criar um modelo global aprimorado e mais robusto. Esse modelo global aprimorado é então enviado de volta aos dispositivos para mais uma rodada de treinamento local, repetindo o ciclo e permitindo o aprimoramento contínuo do modelo sem nunca centralizar os dados brutos.

Anonimização: utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo (LGPD). Ao remover atributos identificadores dos dados pessoais para impedir a reidentificação do titular, os atributos restantes não podem ser relacionados a uma pessoa. Embora difícil de alcançar a integral anonimização de um dado pessoal na atualidade, é uma técnica que colabora com a proteção da privacidade.

Pseudonimização: permite que os dados pessoais sejam tratados de forma que não possam ser diretamente atribuídos a um indivíduo específico sem o uso de informações adicionais, que devem ser mantidas separadamente e sujeitas a medidas técnicas e organizacionais rigorosas para garantir que a associação a uma pessoa natural identificada ou identificável seja evitada [EDPB, 2025].

Prova de Conhecimento Zero (*Zero-Knowledge Proof*): protocolo criptográfico que permite a uma parte, denominada provador, convencer uma outra parte, chamada verificador, da altíssima probabilidade da veracidade de uma afirmação – sendo que a comprovação depende de informações secretas conhecidas apenas pelo provador, que não as revela ao verificador para comprová-la [CIPL, 2023]. Por meio do uso de algoritmos matemáticos complexos, a prova é gerada de tal forma que é computacionalmente inviável para alguém que não conhece a afirmação gerar uma prova semelhante ou relacionada. Uma prova de conhecimento zero tem três propriedades principais: completude (se a afirmação que está sendo provada for verdadeira, um verificador honesto ficará convencido desse fato com alta probabilidade); solidez (se o provador não conhece a afirmação, tem muito baixa probabilidade de enganar o verificador); conhecimento zero (o verificador não descobre nada além da validade da afirmação). As provas de conhecimento zero são úteis também para verificar a identidade dos usuários sem revelar informações além do necessário, ajudando assim a prevenir roubo de identidade e fraude.

Ambiente de execução confiável (*Trusted Execution Environment*): ambiente criptograficamente protegido, isolado e que fornece uma plataforma para executar código e uma área para armazenamento dos dados, de modo que possam ser acessados de forma segura. Aplicativos executados fora do ambiente de execução confiável não podem acessar dados dentro dele; em contrapartida, aplicativos executados dentro do ambiente de execução confiável podem acessar os dados fora dele [CIPL, 2023]. Isso porque dentro desse espaço seguro, há possibilidade de especificar e controlar rigidamente quais componentes específicos de *hardware* e *software* estão autorizados a interagir com dados e código. Esta prerrogativa de definir fronteiras claras de acesso e operação assegura que todo o processamento ocorra em um espaço logicamente segregado. Impede-se, assim, que o restante do sistema possa visualizar, acessar ou modificar as informações em trânsito ou em uso ativo. Como fornecem mecanismos para verificar remotamente se as solicitações de segurança e privacidade do usuário foram atendidas, adicionalmente limita o tratamento dos dados pessoais à finalidade previamente definida.

5. Ferramentas disponíveis para recomendação de PETs

Existem *frameworks* que fornecem bases técnicas, legais e organizacionais para apoiar as instituições na adoção da PET mais adequada para diferentes sistemas ou serviços que tratam dados pessoais. Operam auxiliando na identificação e comparação de tecnologias tais como criptografia homomórfica, privacidade diferencial, computação multiparte segura, aprendizado federado e anonimização, todos ressaltando que pode haver mais de uma PET aplicável ao caso concreto.

Nos três *frameworks* analisados, brevemente comentados nesta seção, são apresentadas perguntas, em forma de árvores decisórias ou estruturadas em questionários detalhados, que consideram aspectos como o uso de dados pessoais sensíveis, a aplicação de técnicas de segurança da informação, os riscos a serem mitigados, a governança de dados aplicada e as políticas internas utilizadas. Esses aspectos avaliados propiciam um panorama abrangente para apoiar a escolha das PETs pelas organizações.

5.1. ENISA

A Matriz de Controle de PETs [ENISA, 2016b] é composta de *framework* de avaliação de PETs exclusivamente *on-line* e móveis, conforme Figura 1. Possibilita uma análise criteriosa das capacidades, riscos, maturidade e impacto das PETs da organização. O *framework* abrange Guia Orientativo e questionário contemplando um conjunto de perguntas avaliativas, cujos critérios a serem examinados são:

- genéricos: buscam avaliar as características gerais das PETs aplicáveis a todos os tipos de ferramentas e relacionadas à privacidade e à segurança, com vistas a fornecer uma compreensão geral de como são consideradas no contexto das aplicações. Avaliam maturidade e estabilidade, implementação de política de privacidade e usabilidade;
- específicos: visam aferir características particulares de PETs, explorando detalhadamente os aspectos técnicos sobre mensagens seguras, VPNs, redes de anonimato e ferramentas antirrastreamento (para navegação *on-line*).

ENISA'S PETS CONTROL MATRIX

TOOL/SERVICE NAME		*WEBSITE*	
DEVELOPER		*CONTACT EMAIL*	

Tool/service type *Please click on the yellow cells to select*		*Operating System* *Please click on the yellow cells to select*		*Please introduce the version of the tool/service*	
VPNs		*Android*		version	
Secure Messaging		*iOS*		version	
Anonymizing (networks)		*Windows Phone*		version	
Anti-Tracking		*Windows*		version	
		Mac		version	
		Linux		version	
		Any OS (only for Anti-Tracking)			

GENERIC	SPECIFIC

The ENISA's PETs control matrix can help you analyse and present the different characteristics of a specific privacy-enhancing tool and/or service.

You can choose between four different types of tools/services: VPNs, Secure messaging, Anonymizing networks and Anti-tracking. Based on your choice you will be asked to answer a number of questions particular to the selected tool/service (under Specific tab above). For all cases you will be asked to answer a number of generic questions applicable to all types of tools/services (on Maturity and Stability, Privacy Policy Implementation and Usability under Generic tab above).

A glossary is provided for explanation of technical terms used within the questions.

This document should be filled under Excel versions 2007, 2010, or 2016.

If you would like to learn more about the ENISA's PETs control matrix and the overall framework for assessment of privacy tools, please visit: www.enisa.europa.eu

Figura 1 – Matriz de controle de PETs (fonte: ENISA, 2016b)

5.2. TNO

O *framework* de decisão e a ferramenta *on-line* da [TNO, 2021] auxiliam gestores e especialistas a avaliar desafios específicos e selecionar tecnologias PETs mais adequadas para um caso concreto. Adota uma abordagem com base em necessidades organizacionais e riscos para apoiar a tomada da decisão tecnológica.

A ferramenta, suportada por Guia e Lista de Verificação, inclui uma árvore de decisão interativa que explora opções tecnológicas de acordo com as necessidades da organização. Recomenda PETs tais como computação multiparte segura, aprendizado federado, criptografia homomórfica, dados sintéticos, prova de conhecimento zero e ambiente de execução confiável, conforme extrato demonstrado na Figura 2.

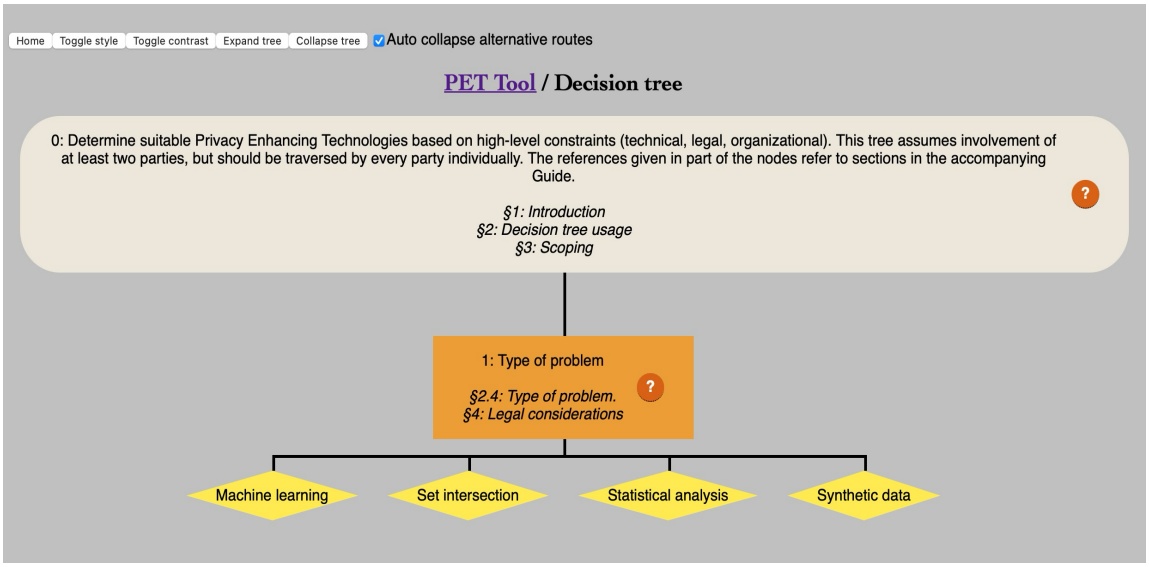

Figura 2 – Extrato da árvore de decisão de ferramentas PET

5.3. DSIT.gov.uk

A ferramenta desenvolvida por [UK-DSIT, 2021] busca incentivar e facilitar a adoção de PETs, principalmente em projetos que envolvam o compartilhamento ou processamento de informações sensíveis. Foca em governança ética, responsabilidade e conformidade legal, especialmente em IA.

Por meio de Guia de Adoção, o material, em sua versão Beta, potencializa a conscientização e compreensão de como as PETs podem ser utilizadas na prática, além de sinalizar algumas de suas limitações. O funcionamento é simples: a partir de respostas sobre o caso concreto, apresentadas pela equipe do projeto a perguntas dispostas na forma de uma árvore de decisão disponível na *web*, são fornecidas recomendações sobre quais PETs, em detalhes, podem ser úteis. Embora não cubra todos os casos de uso de PETs, auxilia na exploração de quais tecnologias podem ser benéficas para o caso concreto. Um extrato da árvore de decisão de recomendação de PETs é apresentado na Figura 3.

A solução também disponibiliza um repositório com casos de uso, objetivando ilustrar casos práticos em que PETs foram utilizadas para resolver problemas reais.

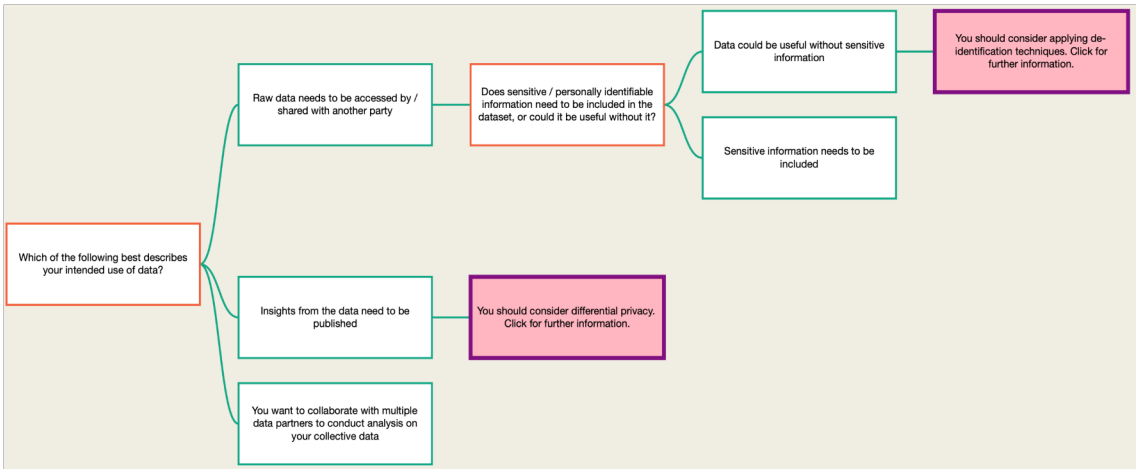

Figura 3 – Extrato da árvore de decisão de recomendação de PETs (fonte: UK-DSIT, 2021)

6. Uso de PETs por governos digitais

6.1. Motivação

A adoção de PETs para aprimorar a privacidade no âmbito dos tratamentos de dados pessoais realizados por governos digitais é impulsionada por diversas motivações, alinhadas principalmente a requisitos legais e éticos, assim como a princípios tais como os da LGPD e do interesse público.

Para além de fomentar a inovação e o desenvolvimento tecnológico, que são fundamentos da disciplina de proteção de dados pessoais brasileira, a adoção de PETs viabiliza o aumento da colaboração entre os entes públicos, permitindo inclusive o tratamento de dados pessoais sensíveis sem, contudo, necessariamente compartilhá-los entre os órgãos.

Os governos digitais brasileiros têm potencial para serem incentivadores do uso de PETs; para tanto, podem utilizar como referência o exemplo do setor público britânico [TRS, 2023] ou apoiarem-se no Programa da ONU sobre estatísticas oficiais da Agenda 2030 para o Desenvolvimento Sustentável, que auxilia com questões metodológicas, promove a capacitação, o treinamento e o compartilhamento de experiências na temática [ONU, 2023].

A seu favor, o Brasil possui um robusto arcabouço legal e regulatório no segmento, que atua como um dos principais catalisadores para a adoção de medidas de aprimoramento da privacidade, a exemplo da LGPD e das resoluções da ANPD. Em paralelo, as iniciativas de modernização da gestão pública e a pressão da sociedade por serviços públicos mais eficientes impulsionam a busca por novas tecnologias que visam aprimorar a privacidade.

6.2. Desafios para a adoção de PETs por governos digitais

Apesar do potencial existente na atualidade, a adoção de PETs pelo setor público brasileiro enfrenta desafios significativos. No Brasil, há uma lacuna entre a disponibilidade de soluções tecnológicas de ponta neste ramo e a sua aplicação prática.

Uma das principais barreiras à adoção de PETs está relacionada à conscientização e ao pleno conhecimento pelo setor público sobre o que representa tal abordagem e como pode impactá-lo [TRS, 2023]. A falta de expertise técnica de profissionais para desenvolver, implementar e comunicar os benefícios das PETs representa um desafio crucial em sua adoção governo britânico, o que se observa no contexto brasileiro.

Embora as PETs sejam promissoras, o risco inerente ao uso de tecnologias relativamente novas e pouco compreendidas pelo setor público é um forte desincentivo à sua utilização. Casos práticos de aplicação de PETs emergentes ainda são escassos no Brasil, o que leva as equipes a manter as técnicas mais tradicionais e consolidadas para a proteção de dados pessoais, como a anonimização.

Limitações oriundas da ainda recente governança de dados nos governos digitais – cujas políticas para aplicação em seus domínios ainda estão em fase de elaboração ou são de recente aplicação [MGI, 2025] [GO, 2024] [SP, 2021] – atenuam, em esfera nacional, a qualidade da infraestrutura para interoperabilidade, desviando o foco da inovação e dificultando a aceitação do uso de novas tecnologias pelos tomadores de decisão da administração pública.

Inobstante os avanços obtidos por governos digitais no desenvolvimento de soluções confiáveis, muitas ferramentas para aprimorar a privacidade ainda não são aplicadas; por serem tecnicamente complexas e exigirem conhecimento especializado, intensifica-se a demanda por capacitação dos servidores públicos para seu uso.

Há, ainda, a necessidade de enfrentar as atuais barreiras para colaboração entre fragmentados entes públicos nas diversas esferas, dispostos em um emaranhado organizacional diverso, que se utilizam de práticas heterogêneas e com diferentes graus de maturidade tecnológica. Alguns recursos computacionais também representam entraves na adoção de PETs por requererem maior capacidade disponível [CIPL, 2023] [TRS, 2023], o que invariavelmente acarreta maiores custos aos projetos – o que, em decorrência, pode ocasionar atrasos na prestação de serviços e impactos à sociedade.

Aspectos legais e de conformidade exigem minimamente a adoção de medidas aptas a proteger os dados pessoais. O Poder Executivo dos entes federados opera em múltiplos setores com regulação específica, o que demanda aos entes públicos navegarem por um cenário regulatório complexo, com a possibilidade de conflito na aplicação conjunta de tecnologias, normas e políticas, perspectivas apresentadas na Figura 4.

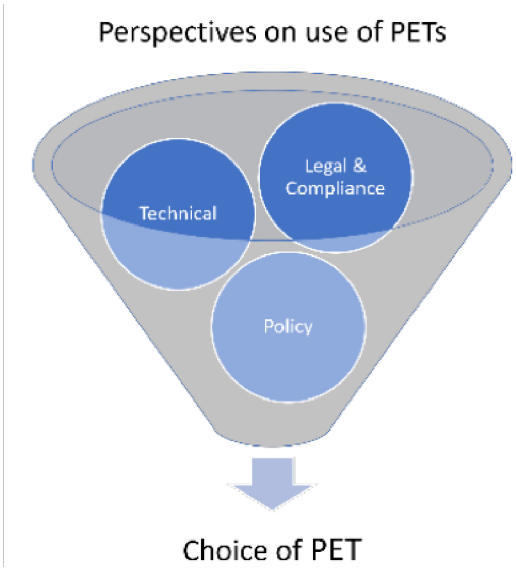

Figura 4 – Perspectivas para abordar a escolha de PETs (fonte: TNO, 2021)

7. Estudo de caso

As normas protetivas de dados pessoais em vigor no Brasil, como a LGPD e as resoluções da ANPD, impõem, além da necessidade de protegê-los, uma constante pressão pela

conformidade no tratamento dos dados. Como visto, as PETs podem colaborar para mitigar riscos nas operações de tratamento de dados pessoais e aumentar a credibilidade das ações governamentais fundamentadas em tais tratamentos.

7.1. Metodologia

O estudo de caso apresentado neste trabalho foi fundamentado em análise qualitativa documental, conforme descrita por [Minayo, 2017], para avaliar oportunidades de aplicação de PETs em tratamentos de dados pessoais estabelecidos em normativos publicados pelo governo federal.

A seleção documental foi realizada sobre os decretos publicados no Diário Oficial da União pelo Poder Executivo federal. Como critérios de inclusão, foram selecionados os decretos regulamentadores publicados no período de 01/01/2025 a 17/08/2025 que possuem expressa referência ao termo "dados pessoais" e comandos que determinam o tratamento de tais dados. Os critérios de exclusão, por sua vez, removeram da seleção os decretos regulamentadores que tratam da criação ou alteração de quadros de órgãos públicos e os decretos de pessoal, estes por conterem tão somente nomeações e exonerações de agentes públicos.

A etapa de análise consistiu na leitura detalhada e interpretação dos decretos selecionados. Foram extraídas informações quanto aos tipos de operação de tratamento de dados pessoais; aos agentes de tratamento envolvidos; à abrangência do tratamento; aos tipos de dados pessoais, inclusive sensíveis; às categorias de titulares, inclusive de pessoas vulneráveis; aos princípios da LGPD explicitados no texto normativo. Ainda como parte da análise, importa destacar que o estudo foi realizado com base unicamente na integralidade textual e na individualidade de cada decreto, não sendo, portanto, consideradas quaisquer relações dos referidos normativos com outras regulamentações em vigor, além da LGPD.

Em seguida à etapa de análise, foram avaliadas quais PETs, abordadas neste trabalho, poderiam minimizar os potenciais efeitos negativos à privacidade dos titulares de dados quando da execução dos tratamentos de dados pessoais decorrentes dos referidos normativos. Assim, para cada PET recomendada, foram explicitadas: a **aplicação**, que descreve as situações concretas e cenários em que a PET pode ser utilizada; a **utilidade**, apontando os benefícios diretos e as contribuições de cada PET para a proteção dos dados pessoais e da privacidade; e (iii) a **justificativa legal**, que indica os dispositivos do normativo analisado que embasaram a recomendação.

Quanto às limitações da análise, entende-se fazer necessária, para maior acurácia na recomendação das PETs, a avaliação de diversas variáveis relativas ao contexto do tratamento dos dados pessoais não disponíveis para este estudo, tais como: problema a ser resolvido, objetivos e respectivos riscos de negócio; volume e qualidade dos dados pessoais; recursos computacionais existentes no ente público; ocorrência de transferências internacionais de dados pessoais; prontidão organizacional para inovação e mudanças; conhecimento dos profissionais envolvidos no projeto; nível de maturidade tecnológica da instituição e recursos financeiros disponíveis.

7.2. Análise de decretos

Na análise ora apresentada, é relevante frisar que para cada cenário de tratamento de dados pessoais disposto nos decretos, pode haver mais de uma PET adequada, conforme as especificidades do contexto e dos objetivos a serem alcançados.

Além disso, outras PETs não mencionadas neste estudo também podem ser aplicáveis e igualmente eficazes, considerando a diversidade e a dinâmica das soluções tecnológicas disponíveis. Destaca-se também que em virtude da similaridade operacional de alguns dos decretos analisados, algumas PETs foram recomendadas para mais de um deles, reforçando a sua versatilidade e aplicabilidade em múltiplos cenários de tratamento de dados pessoais e proteção da privacidade.

Faz-se importante salientar que as recomendações contidas nesta seção possuem caráter exclusivamente educacional, não tendo o condão de induzir qualquer ente público ou instituição privada a adotá-las.

7.2.1. Decreto nº 12.574, de 5 de agosto de 2025. Ementa: Institui a Política Nacional Integrada da Primeira Infância.

A norma estabelece a coordenação integrada das políticas públicas para a primeira infância e abrange a necessidade de tratamento de dados de todas as crianças brasileiras.

Embora os dados pessoais não sejam explicitados, a norma consigna o tratamento de dados relativos a situações socioeconômicas, territoriais e regionais, étnico-raciais, de gênero e de deficiência. Observa-se, portanto, o tratamento não somente de dados de titulares vulneráveis (crianças), mas também de dados sensíveis (a exemplo de características étnico-raciais e de deficiência).

Computação Multiparte Segura	
Aplicação	Elaboração de estudos, indicadores e estatísticas sobre a primeira infância, sem que qualquer órgão tenha acesso completo às bases de dados dos outros órgãos
Utilidade	Permite que os diferentes ministérios coordenadores dos eixos estruturantes (Ministério da Saúde, da Educação, da Assistência Social) colaborem em análises conjuntas para elaborar, por exemplo, indicadores para mensurar a evolução dos padrões de desenvolvimento da criança e para monitoramento dos eixos, sem a necessidade de que qualquer uma das partes revele os dados pessoais sob sua custódia
Justificativa legal	Política intersetorial e articulação federativa (art. 1º, § 1º e art. 2º, VII e VIII); integração de dados e desenvolvimento tecnológico (art. 7º, III); integração de informações (art. 5º, § 3º) e plano de ação estratégico (art. 6º)
Criptografia Homomórfica	
Aplicação	Compartilhamento e processamento seguro dos dados pessoais e estatísticos coletados, integrados e mantidos para monitoramento e avaliação das políticas da PNIPI. Inclui dados sensíveis, socioeconômicos e territoriais compartilhados entre entes federativos (União, Estados, DF, Municípios) e órgãos setoriais
Utilidade	Permite processamento e extração de indicadores e métricas para avaliar o desenvolvimento infantil, sem a exposição dos dados originais no trânsito ou armazenamento, garantindo segurança máxima, sobretudo no ambiente de nuvem e em sistemas integrados

Justificativa legal	Monitoramento e avaliação por meio da coordenação e consolidação integrada de dados (art. 5º, §§ 1º e 2º); integração de dados e desenvolvimento tecnológico (art. 7º, III); observância da Lei nº 13.709/2018 (LGPD) quanto à proteção e tratamento seguro dos dados pessoais (art. 5º, § 6º)
Privacidade Diferencial	
Aplicação	Divulgação pública de dados desagregados para controle social, formulação de políticas e pesquisa acadêmica – minimizando riscos de reidentificação de crianças e famílias, especialmente nos recortes étnico-raciais, sociais e territoriais
Utilidade	Proporciona transparência e acesso à informação socialmente relevante segundo os parâmetros definidos, fortalecendo o monitoramento e a avaliação pública da PNIPI, sem comprometer a privacidade individual
Justificativa legal	Divulgação dos dados protegidos e desagregados (art. 5º, § 5º); promoção da equidade e enfrentamento a discriminações (art. 2º, X); e coordenação do monitoramento e avaliação da PNIPI (art. 7º, IV).

7.2.2. Decreto nº 12.572, de 4 de agosto de 2025. Ementa: Institui a Política Nacional de Segurança da Informação e dispõe sobre a governança da segurança da informação no âmbito da administração pública federal.

O normativo, que cria a PNSI (Política Nacional de Segurança da Informação), é de caráter estrutural, não especificando dados pessoais a serem tratados; no entanto, a PNSI ressalta, como um de seus princípios e de seus objetivos, a proteção de dados pessoais. Contempla ainda recomendações técnicas clássicas de segurança e governança, associadas a controles administrativos e capacitação de pessoas, primordiais e essenciais para a efetividade normativa.

Visto que PETs não se limitam à adoção exclusiva de tecnologias, na aplicação deste Decreto observa-se oportunidades para organizar a implementação de abordagens de privacidade desde a concepção, visando equilibrar inovações com segurança da informação e proteção de dados pessoais, e possibilitar a construção da confiança dos cidadãos na utilização segura dos dados pelos governos digitais.

Controle de acesso e gestão da identidade	
Aplicação	Gerenciamento do acesso aos sistemas e aos dados, incluindo autenticação, autorização e auditoria, assegurando o ciclo de vida seguro da informação
Utilidade	Reduz riscos de acesso indevido, previne violações de política e colabora para atender os princípios da confidencialidade e da responsabilidade institucional para a segurança da informação
Justificativa legal	Responsabilidade pública e gestão de riscos (art. 3º, II e VI)
Educação e Capacitação em Segurança da Informação	
Aplicação	Formação e treinamento dos agentes públicos envolvidos no ciclo de vida dos dados na administração pública
Utilidade	Fomenta a cultura de segurança da informação, reduzindo erros humanos e fortalecendo a conscientização sobre boas práticas de segurança
Justificativa legal	Educação como instrumento para cultura (art. 3º, IV) e promoção de qualificação e cultura continuada (art. 8º, III e IV)
Governança, Normatização e Auditoria	

Aplicação	Estruturação de políticas, normativos, auditorias e avaliação da conformidade para garantir a implementação eficaz da política de segurança da informação em entes públicos
Utilidade	Garante transparência, controle e alinhamento às normas, reforçando a credibilidade e a gestão responsável da segurança da informação
Justificativa legal	Elaboração de políticas, normativos e cooperação internacional (art. 8º, II e VI); auditoria pelo sistema de controle interno (art. 9º) e responsabilidades dos órgãos e entidades (art. 10).

7.2.3. Decreto nº 12.564, de 24 de julho de 2025. Ementa: Regulamenta o art. 2º-I da Lei nº 10.820, de 17 de dezembro de 2003, para dispor sobre os procedimentos e requisitos técnicos para a verificação biométrica da identidade do trabalhador, o consentimento para tratamento de dados pessoais biométricos e o uso de assinaturas eletrônicas e digitais nas operações de crédito consignado com desconto em folha de pagamento para fins de contratação e averbação.

O normativo exige que instituições consignatárias e agentes operadores públicos sigam diretrizes para verificação biométrica da identidade do trabalhador, com prova de vida assegurando sua identidade para descontos em folha de pagamento, objetivando garantir a autenticidade das transações.

Tendo como categoria de titulares os trabalhadores, não explicita qual dado biométrico pode ser utilizado para garantia da operação (se o uso da face, das digitais ou outros mecanismos). Cita explicitamente o princípio da autenticidade e a aplicação de técnica de múltiplo fator de autenticação como mecanismo de segurança da informação.

Prova de conhecimento zero	
Aplicação	Utilizada na etapa de verificação biométrica, viabiliza que o órgão provador confirme que a biometria corresponde a um registro válido sem que o dado biométrico em si seja revelado (ou seja, que a biometria seja enviada ao órgão verificador)
Utilidade	Desnecessidade de expor ou transferir os dados biométricos para a instituição financeira. Isso garante um nível de privacidade superior, pois o dado sensível (a biometria) não é exposto, e atende à necessidade de implementar mecanismos de verificação biométrica com prova de vida, garantindo a autenticidade do contratante de forma mais segura
Justificativa legal	Assegurar a autenticidade do contratante (art. 2º) por meio de verificação biométrica (art. 3º, II, a)

7.1.4. Decreto nº 12.561, de 23 de julho de 2025. Ementa: Regulamenta o art. 1º da Lei nº 15.077, de 27 de dezembro de 2024, para dispor sobre o cadastro biométrico obrigatório para concessão, manutenção e renovação de benefícios da seguridade social de competência da União.

O normativo determina tratamento de dados pessoais de todos os cidadãos que são beneficiários de serviços sociais, sem explicitar o conjunto de dados a ser utilizado no âmbito do cadastro e da verificação biométricos.

A interoperabilidade entre as bases biométricas da Carteira Nacional de Habilitação, identificação civil da Polícia Federal e Identificação Civil Nacional do Tribunal Superior Eleitoral, até que formado o Cadastro Biométrico, é explicitada no Decreto, que consigna também a necessidade de zelar pela segurança, privacidade e proteção dos dados pessoais.

Criptografia Homomórfica	
Aplicação	Proteção do processamento dos dados biométricos nas operações de verificação de autenticidade, mesmo em ambiente compartilhado
Utilidade	Permite validação segura sem exposição dos dados brutos, mitigando riscos de fraudes e vazamentos
Justificativa legal	Art. 2º, § 3º (interoperabilidade) e art. 4º (verificação biométrica)
Computação Multiparte Segura	
Aplicação	Colaboração segura entre órgãos públicos para validação biométrica sem que cada órgão revele os dados pessoais completos que custodia
Utilidade	Garante proteção de dados entre órgãos diversos, preservando privacidade na interoperabilidade
Justificativa legal	Art. 2º, § 3º (interoperabilidade) e art. 4º (verificação biométrica)

7.1.5. Decreto nº 12.560, de 23 de julho de 2025. Ementa: Dispõe sobre a Rede Nacional de Dados em Saúde e sobre as Plataformas SUS Digital e regulamenta o art. 47 e o art. 47-A, *caput*, § 1º e § 2º, da Lei nº 8.080, de 19 de setembro de 1990.

Este decreto cria plataforma de interoperabilidade do ecossistema de dados do Sistema Único de Saúde (SUS), integrada em todo território nacional e com foco na interoperabilidade e no compartilhamento de dados de saúde, administrativos, financeiros e cadastrais relacionados às ações e aos serviços de saúde.

Abrange todas as categorias de titulares de dados pessoais; portanto, inclui também crianças, adolescentes, idosos e todas as demais categorias de vulneráveis. Embora os dados não sejam explicitados no normativo, é informado o tratamento de dados pessoais que revelem informações sobre a saúde física ou mental do titular (portanto, dados sensíveis), no presente, no passado ou no futuro, além de dados cadastrais e financeiros.

A norma cita explicitamente os princípios da segurança da informação, da privacidade e da confidencialidade, da transparência e o uso ético e legal dos dados, além de outros dispostos na LGPD.

Criptografia Homomórfica	
Aplicação	Interoperabilidade de dados pessoais e dados pessoais sensíveis entre diversos agentes de tratamento, garantindo que os dados possam ser analisados sem exposição direta dos dados custodiados por um agente para uso por outro agente
Utilidade	Extração de estatísticas, consultas médicas, auditorias e estudos populacionais, com sigilo reforçado no trânsito e processamento
Justificativa legal	Art. 2º (proporcionalidade), art. 6º (confidencialidade e segurança da informação)
Computação Multiparte Segura	
Aplicação	Situações em que múltiplos agentes precisam colaborar no tratamento dos dados pessoais (ex.: monitoramento de epidemias, cruzamento de bases cadastrais) sem que nenhum agente tenha acesso aos dados completos dos demais
Utilidade	Resguarda a privacidade de pacientes e profissionais de saúde, viabilizando análises interinstitucionais sem exposição indevida

Justificativa legal	Art. 3º (interoperabilidade segura), art. 6º (proteção de dados em cenários de acesso federado e compartilhamento amplo)
Privacidade diferencial	
Aplicação	Divulgação de relatórios, dashboards e estatísticas públicas (inclusive para pesquisa), minimizando o risco de reidentificação de indivíduos a partir de bases anonimizadas
Utilidade	Indispensável para viabilizar o acesso ampliado a informações sobre saúde da população brasileira para toda a sociedade
Justificativa legal	Art. 6º (princípios da privacidade, da confidencialidade e da eficiência), arts. 15 e 16 (disseminação e acesso de informações)

7.1.6. Decreto nº 12.555, de 16 de julho de 2025. Ementa: Dispõe sobre as regras, os critérios e os procedimentos a serem observados pelas pessoas físicas ou jurídicas, de direito público ou privado, para a implementação, a habilitação, a execução e o monitoramento do Programa de Estímulo ao Transporte por Cabotagem - BR do Mar, de que trata a Lei nº 14.301, de 7 de janeiro de 2022, e regulamenta disposições da Lei nº 9.432, de 8 de janeiro de 1997, e da Lei nº 10.893, de 13 de julho de 2004.

O normativo detalha os requisitos para as empresas de navegação e as condições para o afretamento de embarcações, sendo possível deduzir que o tratamento concentrase em de dados pessoais de tripulantes e trabalhadores aquaviários, inclusive dados sobre saúde (sensíveis).

Há previsão para colaboração e compartilhamentos de dados pessoais entre agentes de tratamento do setor público, e também do setor privado.

Computação Multiparte Segura	
Aplicação	Situações que exigem colaboração entre múltiplos agentes, como Ministério de Portos e Aeroportos, Ministério do Trabalho e Emprego e ANTAQ, para análise combinada de dados pessoais, sem que nenhum participante tenha acesso completo aos dados custodiados pelos demais
Utilidade	Resguarda a privacidade na cooperação interinstitucional e viabiliza análises federadas, protegendo a privacidade e evitando exposição indevida entre os diversos entes envolvidos no monitoramento e fiscalização do Programa BR do Mar
Justificativa legal	Art. 5º (fiscalização da admissão de tripulantes brasileiros), art. 4º (tratamento de dados para monitorar o Programa BR do Mar) e art. 28 (comunicação de eventos de saúde)
Privacidade diferencial	
Aplicação	Divulgação de dashboards, relatórios e estatísticas públicas dos dados pessoais tratados no Programa BR do Mar, assegurando que a reidentificação de indivíduos seja minimizada
Utilidade	Fortalece a transparência, o controle social e a prestação de contas públicas sem comprometer a privacidade dos indivíduos envolvidos
Justificativa legal	Art. 22 (acompanhamento do Programa BR do Mar)

8. Considerações finais

O presente artigo analisou o papel das Tecnologias de Aprimoramento da Privacidade (*Privacy Enhancing Technologies*, PETs) como elementos-chave para que serviços públicos digitais estejam em conformidade com os direitos fundamentais à privacidade e à proteção de dados pessoais.

Ao longo deste estudo, foi demonstrado que tais direitos fundamentais devem ser garantidos inobstante o intenso fluxo informacional e as transformações tecnológicas advindas até o momento. Foi sinalizado que o crescimento exponencial do tratamento de dados pessoais, impulsionado pela digitalização e pela disponibilização de serviços nativamente digitais, demandou resposta proporcional para proteger a privacidade.

A apresentação conjunta dos conceitos, histórico, categorização e exemplos práticos de PETs demonstrou que essas abordagens, embora por vezes de aplicação complexa, oferecem soluções viáveis para o tratamento ético e seguro de dados pessoais. Ademais, com as perspectivas situando nos campos tecnológico, organizacional e legal, destacou-se a necessidade de governança de dados robusta, orientada aos riscos para os titulares, e de cultura institucional voltada à privacidade desde a concepção dos sistemas e serviços, ambas atendendo também aos requisitos da LGPD.

Apesar do potencial, a investigação revelou obstáculos existentes para a consolidação das PETs em governos digitais brasileiros, o que leva à sua adoção ainda pouco frequente na atualidade. Entre alguns dos obstáculos, destacam-se a necessidade de maior conscientização acerca dos seus benefícios e aplicabilidade, por algumas serem ainda emergentes, e a exigência de conhecimentos especializados.

Observou-se, por meio do estudo de caso envolvendo decretos federais publicados em 2025, que a aplicação criteriosa de PETs como criptografia homomórfica, privacidade diferencial, computação multiparte segura e prova de conhecimento zero pode mitigar riscos à privacidade em situações concretas, especialmente quando se trata de informações sensíveis ou relativas a grupos vulneráveis.

Por fim, a adoção sistemática e consciente das PETs por governos digitais não constitui apenas um imperativo tecnológico, mas, sobretudo, um compromisso institucional com a promoção da proteção de dados pessoais, da privacidade e da confiança do cidadão no ambiente digital.

9. Referências

1. BRASIL. Lei Geral de Proteção de Dados Pessoais (LGPD). 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 27/07/2025.

2. BRASIL. Constituição da República Federativa do Brasil. Brasília, DF: Senado Federal, 1988. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 20/08/2025.

3. CIPL. Centre for Information Policy Leadership. Privacy-Enhancing and Privacy-Preserving Technologies: Understanding the Role of PETs and PPTs in the Digital Age. 2023. Disponível em: https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/ciplunderstanding-pets-and-ppts-dec2023.pdf. Acesso em: 12/08/2025.

4. CE. Comissão Europeia. Com/2007/00228. 2007. Disponível em https://eurlex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:52007DC0228. Acesso em: 16/08/2025.

5. CONSELHO DA EUROPA. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. 1981. Disponível em: https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum= 108. Acesso em: 29/08/2025.

6. D'ALIBERTI, L., GRONBERG, E. e KOVBA, J. Privacy-Enhancing Technologies for Artificial Intelligence-Enabled Systems. In Proceedings of IWSPA '24, 2024, Porto, Portugal.

7. DONEDA, D. Da privacidade à proteção de dados pessoais: Fundamentos da Lei Geral de Proteção de Dados. São Paulo: Thomson Reuters Brasil, 2021.

8. DWORK, C. e ROTH, A. The Algorithmic Foundations of Differential Privacy. 2014. DOI: 10.1561/0400000042.

9. EDPB. *European Data Protection Board*. Guidelines 01/2025 on Pseudonymisation. 2025. Disponível em: https://www.edpb.europa.eu/system/files/2025-01/edpb_guidelines_202501_ pseudonymisation_en.pdf. Acesso em: 01/08/2025.

10. ENISA. *European Union Agency for Cybersecurity.* Readiness Analysis for the Adoption and Evolution of Privacy Enhancing Technologies. 2016a. Disponível em:

https://www.enisa.europa.eu/publications/pets. Acesso em: 01/08/2025

11. ENISA. *European Union Agency for Cybersecurity*. 2016b. Disponível em: https://www.enisa.europa.eu/publications/pets-controls-matrix/pets-controls-matrix-asystematic-approach-for-assessing-online-and-mobile-privacy-tools. Acesso em: 27/07/2025.

12. EGD. Estratégia de Governança Digital. 2016. Disponível em: https://www.gov.br/governodigital/pt-br/estrategia-de-governanca-digital/. Acesso em: 27/07/2025.

13. GO. Decreto nº 10.609. 2024. Dispõe sobre governança no compartilhamento de dados na administração pública estadual. Disponível em https://legisla.casacivil.go.gov.br/pesquisa_legislacao/110171/decreto-10609. Acesso em: 10/08/2025.

14. GOLDBERG, I. Privacy-enhancing technologies for the Internet III: Ten Years Later. 2007. In A. Acquisti, S. Gritzalis, C. Lambrinoudakis, & S. di Vimercati (Eds.), *Digital Privacy: Theory, Technologies, and Practices*. Auerbach Publications

15. GOLDBERG, I.; WAGNER, D.; BREWER, E. Privacy-enhancing technologies for the Internet. In: Proceedings of the IEE Spring COMPCON. 1997. DOI: 10.1109/CMPCON.1997.584680.

16. HAUPTMANN, E. Rediscovering the Early History of Social Scientific Data Centers in the US. Open Edition Journals. 2024. Disponível em: https://journals.openedition.org/rhsh/9722. Acesso em: 27/07/2025.

17. INFORMATION AND PRIVACY COMMISSIONER ONTARIO; REGISTRATIEKAMER THE NETHERLANDS. Privacy-Enhancing Technologies: The Path to Anonymity Volume 1. 1995. Disponível em: https://collections.ola.org/mon/10000/184530.pdf. Acesso em: 28/08/2025.

18. JERMAN-BLAZIC, Borka. Privacy-Enhancing Technologies - Approaches and Development. Computer Standards & Interfaces. 2003. doi:10.1016/S09205489(03)00003-5.

19. KAANICHE, N., LAURENT, M. e BELGUITH, S. Privacy Enhancing Technologies for Solving the Privacy-Personalization Paradox: Taxonomy and Survey. Journal of Network and Computer Applications. 2020. doi:10.1016/J.JNCA.2020.102807

20. LINDELL, Y. Secure Multiparty Computation (MPC). 2020. Disponível em: https://dl.acm.org/doi/10.1145/3387108. Acesso em: 10/08/2025

21. MENDES, L. S. F. Autodeterminação informativa: a história de um conceito. Revista Pensar. 2020. Disponível em: https://ojs.unifor.br/rpen/article/view/10828. Acesso em: 03/08/2025.

22. MGI. Ministério da Gestão e da Inovação em Serviços Públicos. 2025. Consulta Pública Política de Governança de Dados, Interoperabilidade, Registro de Referência e Compartilhamento de Dados da Administração Pública Federal. Disponível em https:// brasilparticipativo.presidencia.gov.br/processes/politicadedados. Acesso em: 10/08/2025.

23. MINAYO, Maria Cecília de Souza. Análise qualitativa: teoria, passos e fidedignidade. 15. ed. São Paulo: Vozes, 2017.

24. NARAYANAN, A. and SHMATIKOV, V. Robust De-anonymization of Large Sparse Datasets. 2008. IEEE Symposium on Security and Privacy (sp 2008), Oakland, CA, USA, 2008, pp. 111-125, doi: 10.1109/SP.2008.33.

25. OCDE. Organização para a Cooperação e Desenvolvimento Econômico. Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. 1980. Disponível em: https://www.oecd.org/en/publications/2002/02/oecd-guidelines-on-the-protection-of-privacy-and-transborder-flows-of-personal-data_g1gh255f.html. Acesso em: 27/07/2025.

26. OCDE. Organização para a Cooperação e Desenvolvimento Econômico. Emerging Privacy Enhancing Technologies - Current Regulatory And Policy Approaches. 2023. Disponível em: https://www.oecd.org/en/publications/emerging-privacy-enhancingtechnologies_bf121be4-en.html. Acesso em: 27/07/2025.

27. ONU. Organização das Nações Unidas. Marco de Cooperação das Nações Unidas para o Desenvolvimento Sustentável 2023-2027. 2023. Disponível em: https://brasil.un.org/sites/ default/files/2024-07/ONUBrasil_MarcoCooperacao_2023_ 2027.pdf. Acesso em: 10/08/2025.

28. RODOTÀ, S. A vida na sociedade da vigilância: a privacidade hoje. Rio de Janeiro: Renovar, 2008.

29. SOLOVE, D. *A Taxonomy of Privacy*, 154 U. Pa. L. Rev. 477. 2006. Disponível em: https://scholarship.law.upenn.edu/penn_law_review/vol154/iss3/1. Acesso em: 27/07/2025.

30. SP. Deliberação Normativa CGGDIESP-1. Institui a Política de Governança de Dados e Informações. 2021. Disponível em https://diariooficial.imprensaoficial.com.br/ nav_v6/index.asp?c=31384&e=20211231&p=1. Acesso em: 10/08/2025.

31. SHEN, Y., PEARSON, S. Privacy Enhancing Technologies: A Review. 2011. Disponível em: https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi= 6bf9f0a288dd496de6bca96f360702b028fa0b58. Acesso em: 27/07/2025.

32. TRS. The Royal Society. From privacy to partnership: The role of privacy enhancing technologies in data governance and collaborative analysis. 2023. Disponível em: royalsociety.org/privacy-enhancing-technologies. Acesso em: 10/08/2025.

33. TNO. Netherlands Organisation for Applied Scientific Research. Pet Decision Tree. 2021. Disponível em; https://decisiontree.mpc.tno.nl/tree/. Acesso em: 02/08/2025.

34. UK-DSIT. United Kingdon Department for Science, Innovation and Technology. 2021. Disponível em: https://cdeiuk.github.io/pets-adoption-guide/adoption-guide. Acesso em: 02/08/2025.

35. UE. União Europeia. Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data. 1995. Disponível em: https://eur-lex.europa.eu/legalcontent/PT/ALL/?uri=celex: 31995L0046. Acesso em: 27/07/2025.

36. UE. União Europeia. Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data. 2016. Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX% 3A32016R0679&qid= 1754779470335. Acesso em: 27/07/2025.

37. UNCEBD. United Nations Committee of Experts on Big Data and Data Science for Official Statistics. The United Nations Guide on Privacy-Enhancing Technologies for official statistics. 2023. Disponível em: https://unstats.un.org/bigdata/task-teams/privacy/guide/. Acesso em: 15/08/2025.

38. WARREN, S. e BRANDEIS, L., The right to privacy, in: 4 Harvard Law Review. 1890. Disponível em: https://archive.org/details/jstor-1321160/page/n1/mode/2up. Acesso em: 27/07/2025.

39. WOOD, A., ALTMAN, M., BEMBENEK, A., BUN, M., GABOARDI, M., HONAKER, J., NISSIM, K., O'BRIEN, R., STEINKE, T e VADHAN, S. Differential Privacy: A Primer for a Non-Technical Audience. Vanderbilt Journal of Entertainment & Technology Law. 2018. DOI: 10.2139/ssrn.3338027.