Tecnologias de aprimoramento da privacidade no contexto do Controle 0 do PPSI: Uma Análise Comparativa para a Proteção de Dados na Era Digital.

Best Privacy-Enhancing Technologies of PPSI Control 0: A Theoretical Analysis for Data Protection in the Digital Age.

Willian Ribeiro da Silva[1], Prof MSc. Virgínia de Melo Dantas[2], Prof Dr. Robson De Oliveira Albuquerque[3]

[1] Universidade de Brasília (UNB),Brasília, DF, Brasil. ORCID
[2] Universidade de Brasília (UNB),Brasília, DF, Brasil. ORCID
[3] Universidade de Brasília (UNB),Brasília, DF, Brasil. ORCID

Resumo

A crescente preocupação com a privacidade e a segurança da informação na era digital impulsionou aos órgãos da administração pública federal a necessidade de implementar programas robustos de proteção de dados. O presente artigo investiga o papel das Tecnologias de Aprimoramento da Privacidade (PETs) no Controle 0 de um Programa de Privacidade e Segurança da Informação (PPSI), a base da governança de privacidade. O estudo explora os fundamentos teóricos que sustentam a necessidade das PETs, por meio de uma análise da literatura e da articulação com referenciais normativos como o NIST Privacy Framework, a norma ISO/IEC 27701 e a Lei Geral de Proteção de Dados Pessoais (LGPD), a investigação indica uma relação intrínseca entre as capacidades das PETs e as necessidades de governança do Controle 0. Os resultados evidenciam que as PETs, incluindo a minimização, pseudonimização, anonimização, criptografia e outras, são fundamentais para a implementação dos princípios de Privacy by Design e Privacy by Default, fortalecendo a proteção de dados e a conformidade regulatória. A análise aponta que a adoção estratégica de PETs é indispensável para os órgãos que buscam construir o PPSI eficazes e promover uma cultura de privacidade na era da informação.

Palavras-chave: Tecnologias de Aprimoramento da Privacidade; Programa de Privacidade e Segurança da Informação (PPSI); Controle 0; Governança de Privacidade; Proteção de Dados; LGPD.

Abstract

The growing concern for privacy and information security in the digital age has driven the need for robust data protection programs. This article investigates the role of Privacy-Enhancing Technologies (PETs) in Control 0 of a Privacy and Information Security Program (PISP), which forms the foundation of privacy governance. Through a literature review and alignment with normative frameworks such as the NIST Privacy Framework, ISO/IEC 27701, and the Brazilian General Data Protection Law (LGPD), the study highlights the intrinsic relationship between PETs' capabilities and the governance requirements of Control 0. The findings demonstrate that PETs—including minimization, pseudonymization, anonymization, encryption, among others—are essential for implementing the principles of Privacy by Design and Privacy by Default, thereby strengthening data protection and regulatory compliance. The study concludes that the strategic adoption of PETs is indispensable for organizations aiming to build effective PISPs and foster a culture of privacy in the information era.
Keywords: Privacy-Enhancing Technologies; Privacy and Information Security Program; Control 0; Privacy Governance; Data Protection; LGPD.

Keywords: *Privacy-Enhancing Technologies. Privacy and Information Security Program*(PPSI). *Control 0. Privacy Governance. Data Protection. LGPD.*

INTRODUÇÃO

A proteção da privacidade da informação se impõe como um dos desafios mais prementes na atualidade, especialmente para órgãos da administração pública federal, onde a gestão de dados sensíveis é crucial para assegurar a confiança pública e garantir a segurança institucional. Segundo o relatório mais recente da União Internacional de Telecomunicações (UIT), em 2023, cerca de 67% da população global, ou 5,4 bilhões de pessoas, estava conectada à internet. Segundo o mesmo relatório, no Brasil, essa conexão é ainda mais acentuada, com mais de 90% da população online. A disparidade entre áreas urbanas e rurais é significativa; enquanto 81% dos habitantes urbanos utilizam a internet, apenas 50% nas zonas rurais têm acesso (ITU, 2023; IBGE, 2023). Neste cenário, a digitalização dos serviços públicos é uma estratégia vital para incrementar a eficiência da administração pública, conforme destacam Pierre Oliveira et al. (2025). Contudo, essa transição não é isenta de desafios. A coleta massiva de dados dos cidadãos, necessária para otimizar a gestão e a formulação de políticas públicas, transforma a segurança e a privacidade da informação em elementos essenciais. Esses aspectos vão além de meras obrigações legais, consolidando-se como pilares da confiança entre Estado e sociedade.

Com a crescente dependência da tecnologia nas operações governamentais, surge a necessidade de um arcabouço robusto e abrangente que assegure a integridade dos dados, a confidencialidade das informações pessoais e a disponibilidade de sistemas. Proteger os cidadãos dos riscos inerentes a essa transformação digital torna-se uma prioridade. Nesse pano de fundo, a conformidade com a Lei Geral de Proteção de Dados (LGPD) e a implementação de programas eficazes de privacidade e segurança da informação são imperativos para o governo federal, especialmente considerando o vasto volume de dados sensíveis que gerencia. O Programa de Privacidade e Segurança da Informação (PPSI) do governo brasileiro foi concebido para apoiar a gestão e mitigação dos riscos associados ao tratamento de dados pessoais. Essa abordagem abrange a integração harmoniosa dos requisitos legais, as melhores práticas em segurança da informação e os princípios

fundamentais de privacidade. Fundamentado em frameworks de privacidade reconhecidos, como a ISO/IEC 27001:2013, o PPSI se apresenta não apenas como uma questão de conformidade, mas como uma estratégia consciente de proteção das informações (ISO, 2013).

Além de respeitar legislações nacionais como a LGPD, o PPSI reflete um comprometimento ético com a privacidade dos indivíduos, um aspecto que se torna essencial na sociedade digital contemporânea. Ao incorporar diretrizes estabelecidas por regulamentos globais, como o GDPR da União Europeia, o PPSI se torna um modelo de boas práticas que transcende fronteiras (EUROPEAN PARLIAMENT, 2016). A implementação de frameworks como o NIST Cybersecurity Framework fortalece a capacidade das organizações de enfrentar ameaças cibernéticas, criando uma resiliência sólida (NIST, 2018). O PPSI, portanto, não é apenas uma resposta às demandas regulatórias, mas também um convite à confiança mútua e à responsabilidade compartilhada entre as organizações públicas e seus stakeholders. Ele se apoia nas diretrizes estabelecidas pela LGPD (Lei nº 13.709/2018), alinhando o Brasil com padrões globais de privacidade de dados, e incorpora conceitos de tecnologias de aprimoramento da privacidade (Privacy-Enhancing Technologies - PETs). Essas inovações visam mitigar a coleta e uso indevido de dados pessoais enquanto garantem a funcionalidade dos sistemas de informação. A essência das PETs reside na implementação de mecanismos de proteção de dados "by design", uma filosofia defendida por Roger Clarke, um dos pioneiros na defesa da privacidade digital. Clarke argumenta que as tecnologias devem permitir que indivíduos realizem suas atividades online com menor exposição de suas identidades, projetando sistemas onde a privacidade seja uma característica padrão, e não uma opção (Clarke, 2000). Dessa forma, as PETs buscam um equilíbrio entre a utilidade dos dados e a segurança da privacidade individual, abordando os desafios decorrentes da crescente digitalização e vigilância de dados. Embora frequentemente associadas a controles mais avançados, as PETs desempenham um papel importante na implementação do Controle 0 do PPSI, que foca no comprometimento da alta direção e na definição de um plano básico de segurança e privacidade. Esse controle estabelece a fundação para uma governança efetiva dos dados.

Este artigo tem como objetivo analisar o papel fundamental das melhores práticas e das PETs no contexto do Controle 0 do PPSI, explorando seu referencial teórico e a aplicabilidade na proteção de dados na era digital.

FUNDAMENTAÇÃO TEÓRICA

A crescente e complexa teia de interações digitais contemporâneas tem, inegavelmente, elevado a conscientização sobre os riscos à privacidade associada ao uso da tecnologia. Este cenário se torna particularmente relevante ao investigarmos a adoção das PETs, em especial no que tange ao conceito de controle zero no PPSI. Contudo, em um panorama global, e de forma ainda mais acentuada no contexto da administração pública brasileira, observa-se uma lacuna significativa na pesquisa sobre as percepções dos usuários e sua efetiva disposição em incorporar PETs no seu cotidiano digital. Essa deficiência em nossa base de conhecimento obstaculiza uma compreensão aprofundada dos motivos subjacentes à notória lenta adoção dessas tecnologias.

Parte da literatura existente sobre PETs têm tradicionalmente se debruçado sobre suas características e capacidades tecnológicas. Apesar de reconhecer a importância dessa abordagem, ela ainda delimita nosso entendimento sobre um aspecto vital: a maneira como as percepções, atitudes e comportamentos dos usuários impactam, de forma concreta, a aceitação e o uso dessas ferramentas. Torna-se, portanto, essencial promover estudos que investiguem de modo mais aprofundado e sensível o papel do usuário nesse cenário, abrir caminho para soluções mais alinhadas às reais necessidades sociais e tecnológicas, potencializando a efetividade e a adoção das inovações em privacidade (WESTIN, 2003). De fato, como apontado por Mathur et al. (2018), a taxa de adoção de PETs permanece persistentemente baixa. Os estudos sobre o tema tem se concentrado predominantemente em aspectos como o design (Janic et al., 2013; Reed et al., 1998; Whitley, 2009), a classificação (Heurix et al., 2015) e os impactos do uso de PETs para usuários e organizações (Aseri et al., 2020; Despotakis et al., 2020).

Embora não se relacione diretamente com a compreensão da adoção por usuários não gerenciais, a contribuição de Mangiò et al. (2020), que fornece entendimentos valiosos sobre o papel das preocupações com a segurança na decisão de adoção. A persistência dessa baixa adoção Mathur et al., (2018) e Statista, (2023) e a sub-representação dos fatores explicativos em pesquisas ressaltam que a adoção generalizada ou sua ausência está intrinsecamente ligada à compreensão das atitudes e comportamentos dos usuários em relação às PETs (Harborth et al., 2020). As literaturas atuais e contemporâneas evidenciam a abrangência e a complexidade deste campo, permitindo sua organização sob diferentes perspectivas. Embora a categorização em três principais fluxos — econômico, técnico e centrado no usuário — seja recorrente e bastante consolidada, destaca-se que tais divisões servem como orientações iniciais, sem esgotar as possibilidades analíticas que a área comporta.

O fluxo econômico na literatura sobre PETs concentra-se na análise das barreiras e dos incentivos de natureza financeira e tecnológica que impactam a disseminação dessas soluções. Pesquisas clássicas já demonstravam uma preocupação central com os custos de implementação, a relação entre custos e benefícios percebidos pelos agentes econômicos, bem como as dinâmicas de mercado e os fatores macroestruturais que influenciam a adoção e a sustentabilidade das PETs (ACQUISTI, 2004; CAULFIELD et al., 2016). Recentemente, essa abordagem tem sido aprofundada por estudos que discutem, além da viabilidade de mercado, o papel das políticas públicas, estratégias de incentivo e modelos de negócios inovadores na promoção da popularização dessas tecnologias em diferentes setores (NOTARIO et al., 2023). O exame dessas dinâmicas revela não apenas os principais entraves à adoção em larga escala das PETs, mas também as oportunidades promissoras para seu desenvolvimento e consolidação no ambiente digital.

O fluxo técnico, tradicionalmente, concentra-se nos avanços em engenharia de software, sistemas e criptografia, buscando analisar de que maneira as inovações técnicas impactam a funcionalidade, usabilidade e efetividade das PETs. Pesquisas dessa vertente já destacavam a importância de aspectos como a simplificação de interfaces, a automação de processos e a redução da sobrecarga cognitiva para promover uma interação mais facilitada e

a consequente adoção dessas tecnologias por parte dos usuários (ALSABAH; GOLDBERG, 2016; NORCIE et al., 2012). Nos últimos anos, o campo tem se consolidado e expandido, com a literatura contemporânea enfatizando o papel das melhorias em algoritmos, arquitetura de sistemas e design de interfaces para tornar as PETs ainda mais acessíveis e eficazes em contextos reais de uso (MEYER et al., 2022; ZEB et al., 2022). Assim, observa-se uma evolução contínua, em que os estudos mais recentes aprofundam e atualizam os desafios e soluções já identificados nos trabalhos anteriores, apontando tendências de integração e de fortalecimento de práticas inovadoras que visam ampliar a adoção e a confiabilidade das PETs no cenário digital.

O fluxo centrado no usuário tem ganhado destaque progressivo na literatura, voltando-se para a análise detalhada das formas de uso, experiências individuais e fatores psicossociais que influenciam tanto a adoção inicial quanto o uso regular dessas tecnologias. Estudos precursores desse campo já evidenciaram a importância de compreender os mecanismos subjacentes às escolhas dos usuários, incluindo resistências, motivações e barreiras para o engajamento efetivo com as PETs (HARBORTH et al., 2020; NAMARA et al., 2020). Nos últimos anos, o interesse nesse fluxo se aprofundou com pesquisas mais contemporâneas dedicando-se a mapear de modo ainda mais sistemático as experiências, percepções, atitudes e comportamentos dos usuários diante das PETs. Resultados recentes têm identificado os principais fatores determinantes para a adoção, a motivação para o uso contínuo e os desafios enfrentados pelos usuários finais em cenários reais, abrangendo aspectos como facilidade de uso, percepção de valor, confiança e privacidade percebida (HO et al., 2022). Assim, nota-se uma evolução conceitual significativa, que integra o conhecimento gerado pelos estudos iniciais, consolidando o papel central dos aspectos subjetivos e contextuais na adoção das tecnologias de privacidade.

Assim, ao tratar-se da fundamentação teórica em PETs, torna-se importante reconhecer tanto as contribuições destes três fluxos quanto a necessidade de abordagens interdisciplinares e flexíveis. A literatura internacional contemporânea reforça que o caráter dinâmico das PETs exige abertura para novas interpretações e categorização constante, permitindo atualidade e

amplitude ao debate sobre o tema. Evidências empíricas recentes (e.g., Abu-Salma et al., 2017; Knight, 2023; Kunst, 2019; Petrosyan, 2023; Statista, 2023; Vailshery, 2023) corroboram as baixas taxas de adoção para estas ferramentas, que representam um espectro amplo de tecnologias capazes de salvaguardar informações pessoais.

MÉTODO

O presente estudo adota uma abordagem de revisão bibliográfica exploratória e qualitativa para analisar o papel das melhores práticas e PETs no contexto do Controle 0 do PPSI. Esse estudo se concentra na análise da síntese de informações já existentes na literatura acadêmica e em documentos de referência da área de privacidade e segurança da informação.
A fase de coleta buscou literatura relevante em bases de dados científicas, utilizando termos como "Privacy-Enhancing Technologies", "PETs", "Data Privacy", "Information Security Program", "GDPR", "LGPD", "Privacy by Design" e "Privacy by Default". Foram selecionados artigos, livros, relatórios técnicos e documentos de referência que abordam a conceituação de PETs, sua classificação, mecanismos de funcionamento, benefícios, desafios de implementação e sua relação com frameworks de privacidade e segurança. O foco foi dado à compreensão teórica e à aplicabilidade prática dessas tecnologias, para isso foi usado a matriz de alinhamento, ou técnica de cruzamento, que é uma ferramenta que visa mapear e correlacionar diferentes elementos de um sistema, processo ou organização, garantindo que estejam sinergicamente orientados para um objetivo comum. O uso de uma matriz de alinhamento operacionaliza a estruturação das relações entre objetivos, métodos, instrumentos e indicadores em um projeto de pesquisa ou planejamento, promovendo clareza e coerência ao processo investigativo (SILVA et al., 2021; KELLEY; PROCTOR; DICKINSON, 2021). Essa visão ao cruzar, por exemplo, capacidades tecnológicas (como as PETs) com requisitos de governança (como o Controle 0 do PPSI), ou objetivos de negócio com indicadores de desempenho. A análise dos dados coletados envolveu a identificação dos principais conceitos e a avaliação de como elas se encaixam e fortalecem o PPSI, particularmente no que concerne ao seu controle fundamental (Controle 0).

RESULTADOS

A análise da literatura revela que as PETs são mais do que meras ferramentas; elas são a materialização técnica dos princípios de privacidade, especialmente *Privacy by Design* e *Privacy by Default*. A incorporação dessas tecnologias no Controle 0 do PPSI demonstra um compromisso proativo com a proteção de dados, indo além da mera conformidade regulatória. Com base nos frameworks citados, o Controle 0 pode ser entendido como a base da governança de privacidade. Ele abrange:

- Política de privacidade formalizada
- Estrutura organizacional definida (papéis e responsabilidades)
- Planejamento, avaliação e supervisão de riscos
- Treinamento e conscientização
- Conformidade regulatória (como a Lei Geral de Proteção de Dados Pessoais - LGPD)

Os resultados da análise comparativa consubstanciada na Tabela 1, que visa elucidar a intrínseca relação entre um conjunto representativo de PETs e os componentes fundamentais do Controle 0 do PPSI. Esta análise se ancora em referenciais normativos e legais de elevada relevância no cenário da proteção de dado do PPSI brasileiro, o NIST Privacy Framework, a norma ISO/IEC 27701 e a legislação brasileira, consubstanciada na Lei Geral de Proteção de Dados Pessoais (LGPD). O objetivo desta investigação preliminar é fornecer uma visão estruturada de como a aplicação estratégica de PETs pode fortalecer a base de governança e responsabilidade do programa de privacidade, preparando para uma discussão mais aprofundada sobre suas implicações práticas e teóricas.

A Tabela 1 demonstra como as principais funcionalidades das PETs se alinham a exigências regulatórias e frameworks. O uso dessas ferramentas apoia o cumprimento de boas práticas, potencializa o compliance e fortalece a cultura de proteção de dados.

Tabela 1 – Alinhamento das Capacidades das PETs com a Privacidade

Capacidade das PETs	Framework NIST Privacy Framework	Norma ISO/IEC 27701	Legislação LGPD	Relação/Alinhamento com Privacidade
Minimização de dados	ID.IM-P1 (dados mínimos necessários)	7.4.3, 7.4.6	Art. 6, III	Apoia políticas de coleta e tratamento mínimo, reduzindo a exposição desnecessária de dados pessoais.
Pseudonimização	PR.DS-P3 (dados parcialmente protegidos)	7.5.6	Art. 13, §4º	Mitiga riscos de identificação, facilita governança e resposta a incidentes.
Anonimização	PR.DS-P4	7.5.5	Art. 12, §2º; Art. 5, III	Reduz obrigações legais, fortalece o compliance e minimiza o impacto em caso de vazamento de dados.
Criptografia	PR.DS-P1, PR.DS-P2	7.5.9	Art. 46, I	Fortalece a proteção de dados confidenciais, comprovando responsabilidade técnica do controlador.
Controle de acesso	PR.AC-1 a PR.AC-4	7.5.7, 7.5.8	Art. 46	Define papéis, limita acessos e protege contra usos indevidos ou não autorizados.
Gestão de consentimento	CT.CO-P1, CT.CO-P2	7.3.3	Art. 7, §5º	Assegura base legal, promove a transparência e a participação do titular.
Registro e auditoria (logs)	PR.PT-P1, PR.PT-P2	7.5.10	Art. 6, X	Garante rastreabilidade das operações, viabiliza prestação de contas e responsabilização.
Monitoramento de riscos	ID.RA-P5, GV.RM-P1	6.9.1	Art. 50, §2º	Sustenta o ciclo de avaliação contínua, essencial para uma boa governança em privacidade.
Treinamento e sensibilização	GV.AW-P1	6.3.1	Art. 50, §2º, II	Promove cultura de privacidade, fortalece responsabilidade institucional e participação de todos os envolvidos.

Fonte: Elaborado pelo autor (2025).

A análise da Tabela 1 evidencia o papel estratégico das PETs como instrumentos multifuncionais para a efetivação de requisitos legais, normativos e de boas práticas em privacidade e proteção de dados. Observa-se que as capacidades das PETs, quando mapeadas

de forma sistemática contra frameworks robustos (como o NIST Privacy Framework), normas internacionais (ISO/IEC 27701) e legislações como a LGPD, demonstram um alto grau de complementaridade e reforço mútuo. Os resultados mostram que a minimização de dados e a anonimização são práticas altamente valorizadas em todas as abordagens, confirmando-se como medidas fundamentais para a redução do risco de exposição e o cumprimento das obrigações legais. O alinhamento dessas práticas com artigos-chave da LGPD e requisitos normativos comprova sua centralidade tanto na prevenção de incidentes quanto na promoção de compliance (KROHNE et al., 2022). A pseudonimização e a criptografia, por sua vez, se destacam pela capacidade de mitigar riscos em contextos nos quais a completa anonimização não é possível, bem como de fortalecer a proteção de dados sensíveis em trânsito ou armazenados. Estes controles técnicos demonstram estar diretamente atrelados à governança e à resposta a incidentes, favorecendo tanto a responsabilização quanto a demonstração de diligência institucional perante autoridades e titulares (SILVA et al., 2021). Ferramentas de controle de acesso e registro/auditoria aparecem fortemente alinhadas aos parâmetros de responsabilidade e transparência, suportando mecanismos internos de rastreabilidade e prestação de contas, valores fundamentais preconizados na LGPD e em padrões internacionais. Esses mecanismos são igualmente reconhecidos como essenciais para a gestão do ciclo de vida dos dados e para a investigação de eventuais incidentes. Na dimensão organizacional, destaca-se o papel da gestão de consentimento, do monitoramento de riscos e do treinamento e sensibilização. Tais práticas operacionalizadas pelas PETs não apenas viabilizem o atendimento às exigências legais (por exemplo, transparência e base legal dos tratamentos), mas também promovem a maturidade institucional e a cultura de privacidade – algo enfatizado como imprescindível na literatura (NIST, 2020; SILVA et al., 2021).

Em síntese, os dados desta tabela confirmam que a adoção coordenada das diferentes capacidades das PETs – orientada por frameworks como o NIST Privacy Framework e as normas ISO/IEC 27701 e LGPD – potencializa sobremaneira a governança e o compliance em proteção de dados, ao mesmo tempo em que prepara as organizações para lidar de modo proativo com os desafios técnicos, regulatórios e sociais emergentes no ecossistema digital.

A Tabela 2 apresenta uma síntese das principais capacidades técnicas das PETs e sua relação com o Controle 0 do PPSI. Por meio de uma abordagem comparativa, a tabela evidencia de que modo diferentes recursos tecnológicos associados às PETs podem ser utilizados para fortalecer aspectos essenciais da governança em proteção de dados pessoais, conforme exigências regulatórias e melhores práticas do setor. Cada linha detalha não apenas o alinhamento conceitual dessas capacidades com as diretrizes do Controle 0, mas também exemplos de evidências técnicas que ilustram a aplicação prática dessas soluções no ambiente organizacional.

Tabela 2 – Alinhamento das Capacidades das PETs com o Controle 0 do PPSI

Capacidade PET	Alinhamento com Controle 0 do PPSI	Evidência Técnica
Criptografia de dados	Contribui para a governança ao reforçar a proteção de dados em repouso e trânsito	Implementação de TLS, AES-256, RSA, entre outros
Registro de logs de acesso	Viabiliza a supervisão e a responsabilização dos agentes	Sistemas de SIEM, logs detalhados, auditoria automatizada
Pseudonimização	Reduz o risco de identificação em processos de tratamento de dados	Ferramentas de tokenização e hashing (SHA-256, bcrypt)
Gestão de consentimento	Oferece suporte para políticas de privacidade e rastreamento da base legal	Consent Management Platforms (CMP), registro de consentimento
Minimização de dados	Facilita a aplicação de princípios de governança e proporcionalidade no uso de dados	Processos de coleta seletiva, data mapping, data classification tools
Anonimização	Pode contribuir para redução de obrigações legais e mitigação de riscos	Algoritmos de anonimização (k-anonymity, l-diversity), ferramentas de masking
Controle de acesso	Permite restringir o acesso conforme perfil e necessidade operacional	RBAC/ABAC, autenticação multifatorial (MFA)
Monitoramento de riscos	Apoia o ciclo contínuo de avaliação de riscos em privacidade e segurança	Ferramentas de gestão de riscos (ERM, GRC), monitoramento contínuo
Treinamento e sensibilização	Colabora para o desenvolvimento de uma cultura organizacional em privacidade	Programas de treinamento, campanhas internas, e-learning sobre privacidade

Fonte: Elaborado pelo autor (2025).

Em suma, a análise das evidências apresentadas na Tabela 2 reforça a viabilidade e a concretude do alinhamento entre as Capacidades das PETs e os objetivos de governança do

Controle 0 do PPSI. A demonstração de tecnologias específicas, como a implementação de protocolos de criptografia robustos (TLS, AES-256), sistemas automatizados de registro e auditoria (SIEM), técnicas de preservação da privacidade como tokenização e hashing, plataformas de gestão de consentimento (Consent Management Platforms - CMP) e a aplicação de processos sistemáticos de coleta seletiva e mapeamento de dados (Data Mapping), ilustra a maturidade e a disponibilidade de ferramentas capazes de operacionalizar os princípios de privacidade em um contexto organizacional.

Estes achados sublinham que a incorporação de PETs no arcabouço do programa de privacidade e segurança não se restringe a um plano teórico, mas possui um substrato técnico bem definido e acessível. Ao adotar tais evidências técnicas, os órgãos da administração pública federal podem efetivamente fortalecer suas práticas de governança, demonstrar maior responsabilidade no tratamento de dados pessoais e, consequentemente, aumentar a confiança dos titulares e a conformidade com as regulamentações vigentes, como a LGPD. A criptografia emerge como uma PET fundamental e amplamente utilizada, fornecendo uma camada essencial de segurança para dados em repouso e em trânsito. A aplicação dessas tecnologias contribui significativamente para a confidencialidade e a integridade da informação, configurando-se como um elemento fundamental para a robustez do PPSI. Tecnologias avançadas como Computação Multipartidária Segura (SMPC) e Privacidade Diferencial também despontam como alternativas promissoras, sobretudo em contextos nos quais a cooperação e o tratamento de dados sensíveis se fazem necessários sem o comprometimento da privacidade individual. Por meio da SMPC, é possível viabilizar a computação colaborativa entre diferentes partes interessadas sem que sejam expostas suas entradas individuais, enquanto a Privacidade Diferencial busca mitigar riscos de reidentificação, adicionando ruído controlado aos resultados e, assim, permitindo a publicação de análises sobre conjuntos de dados sem revelar informações sobre participantes específicos (KROHNE et al., 2022; DWORK; ROTH, 2014).

A pesquisa aponta que a implementação eficaz das PETs no Controle 0 do PPSI pode apoiar à capacidade de uma organização de integrar essas tecnologias de forma estratégica. Isso envolve um entendimento claro dos tipos de dados tratados, dos riscos associados e dos

objetivos de privacidade. Em geral, os resultados evidenciam que as PETs podem ser ferramentas indispensáveis para a construção de um PPSI robusto, oferecendo mecanismos técnicos para salvaguardar a privacidade e permitir que as organizações operem de forma ética e legal na era da informação.

DISCUSSÃO

A presente análise buscou investigar o papel fundamental das melhores Práticas das PETs no âmbito do Controle 0 de um PPSI. Os resultados deste estudo reforçam, de maneira equilibrada, como as tecnologias analisadas vêm assumindo um papel cada vez mais relevante no cotidiano digital. Observa-se que essas soluções tendem a se consolidar como elementos importantes dentro de estratégias abrangentes de proteção de dados, colaborando para a construção de ambientes mais seguros e confiáveis. Conforme previamente assinalado na introdução, a onipresença da tecnologia impõe desafios significativos à gestão da privacidade pelos órgãos, e as PETs emergem como soluções técnicas eficazes para mitigar essa complexidade. Zimmeck et al. (2024) demonstraram, por meio de um experimento, que as pessoas conseguem exercer melhor seus direitos de privacidade por meio do uso de recursos técnicos quando entendem quem está coletando os dados sobre elas, demonstrando a importância de projetar sistemas com a privacidade em mente, algo que as PETs buscam facilitar. Os achados corroboram a perspectiva amplamente difundida na literatura de que as PETs constituem elementos basilares para a efetiva implementação dos princípios de Privacy by Design e Privacy by Default. Quando essas tecnologias não são priorizadas, a privacidade pode acabar ficando em segundo plano, o que, em um mundo cada vez mais conectado e repleto de riscos digitais, é uma postura que traz impactos reais para pessoas e organizações (KROHNE et al., 2022). Por outro lado, o cuidado de integrar a proteção de dados desde o início do desenvolvimento de sistemas e processos não apenas fortalece o compromisso com a segurança das informações, mas também responde de maneira mais sensível às expectativas da sociedade e às exigências das principais normas, como a LGPD e o GDPR (BRASIL, 2018; EUROPEAN UNION, 2016). Promover esse olhar atento à privacidade é, hoje, um passo importante para construir relações de confiança e respeito no universo digital.

A relação observada entre as PETs e a garantia da privacidade apresenta uma analogia interessante com a dinâmica identificada no estudo, nos quais características individuais específicas contribuem para a compreensão do fenômeno. estudos mostraram que muitos usuários não têm uma compreensão clara dos aspectos técnicos de vários PETs, ou até mesmo desenvolvem mal-entendidos (Abu-Salma et al., 2017 ; Balendra & Maqsood, 2023). Essa falta de compreensão pode impactar a capacidade dos usuários de tomar decisões informadas sobre a adoção de PETs. De maneira similar, as propriedades distintivas das PETs, a exemplo da anonimização, criptografia e minimização de dados, podem impactar na efetividade do PPSI, com particular destaque para o Controle 0, paralelamente, a seleção e a implementação criteriosa de PETs, adequadas ao contexto específico dos dados em questão, são determinantes para a concretização da privacidade.

Os resultados que enfatizam a importância da criptografia, da pseudonimização e da minimização de dados revelam a natureza multifacetada das PETs. Estas não representam uma solução singular, mas sim um conjunto diversificado de ferramentas que demandam aplicação estratégica e direcionada. A análise corrobora a visão de que as PETs são elementos essenciais para a implementação dos princípios de privacidade "by design" e "by default". A discussão apresentada também converge para a necessidade de um entendimento aprofundado dos princípios de privacidade como pré-requisito para uma escolha e implementação eficaz das PETs. A mera adoção tecnológica, desprovida de uma compreensão clara de seus objetivos de privacidade organizacionais, pode se mostrar insuficiente.

Finalmente, a analogia com a dimensão no espectro das PETs, algumas podem desempenhar um papel mais central ou exercer um impacto mais significativo na mitigação de riscos específicos à privacidade. A implementação de um PPSI eficaz deve, portanto, considerar essa centralidade potencial de determinadas PETs, visando a consecução de uma proteção mais robusta e adaptada às necessidades e aos riscos identificados. O uso intensivo da tecnologia, como destacado, torna a gestão da privacidade um desafio complexo, e as PETs surgem como soluções técnicas para enfrentar esse cenário.

CONSIDERAÇÕES FINAIS

O presente estudo buscou analisar a relevância das Práticas e Tecnologias de Aprimoramento da Privacidade (PETs) no contexto do Controle 0 do Programa de Privacidade e Segurança da Informação (PPSI). Os resultados aqui apresentados reforçam a visão de que as PETs transcendem a mera funcionalidade de ferramentas, constituindo-se como a concretização técnica dos princípios fundamentais de privacidade, notadamente o Privacy by Design e o Privacy by Default. A integração dessas tecnologias na estrutura de governança inicial do PPSI demonstra um compromisso proativo com a proteção de dados, extrapolando os limites da simples conformidade regulatória.

A análise desenvolvida evidenciou a significativa convergência entre as capacidades oferecidas pelas PETs e os requisitos de governança estabelecidos por referenciais normativos de reconhecida importância e uso pelo PPSI, como o NIST Privacy Framework e a norma ISO/IEC 27701, bem como pela legislação nacional, a LGPD. A demonstração do alinhamento específico de cada PET com os elementos do Controle 0, detalhada na Tabela 1, ilustra a potencialidade dessas tecnologias em endereçar os complexos desafios da privacidade na era digital.

Ademais, a apresentação das evidências técnicas na Tabela 2 solidifica a aplicabilidade prática das PETs, revelando a existência de soluções tecnológicas maduras e acessíveis para suportar os objetivos de governança e responsabilidade. A implementação de criptografia robusta, sistemas de registro e auditoria, técnicas de pseudonimização e anonimização, plataformas de gestão de consentimento e processos de minimização de dados atestam a prontidão do cenário tecnológico para a adoção de programas de privacidade eficazes dentro do cenário do controle 0 do PPSI. As contribuições, em se tratando dos limites relacionados ao estudo, esta foi uma análise puramente teórica. Novos estudos poderiam investigar a implementação prática das PETs em diferentes contextos organizacionais, bem como conduzir análises de caso para compreender a complexidade da sua adoção e os

desafios enfrentados pelos órgão da administração pública federal. A análise dos dados foi exclusivamente qualitativa, sendo que futuros estudos poderiam explorar a eficácia das PETs através de métricas quantitativas.

Considerando os resultados obtidos e as limitações existentes neste estudo, entende-se a importância de dar continuidade na investigação acerca do tema. O estudo mostra que há necessidade de novas pesquisas sobre os efeitos da implementação das PETs no cotidiano das organizações e na confiança dos usuários, explorando como a aplicação dessas tecnologias pode afetar a gestão de dados e a percepção de segurança e privacidade das pessoas. Uma ótima forma de reverter os pontos que poderiam ser melhor aprofundados é sugerindo caminhos para pesquisas futuras ou para outros pesquisadores interessados nesse tema.

Esta pesquisa atingiu os objetivos propostos, concluindo, na análise, que as PETs podem ser ferramentas eficientes para mitigar os riscos de privacidade na era digital. Ressalta-se que a pesquisa contribui para evidenciar o papel de características técnicas individuais para a compreensão da proteção de dados. Salienta-se, também, que isso indica que, apesar do volume intenso de dados, essa relação pode variar em função das tecnologias de aprimoramento da privacidade empregadas. De maneira específica, a adoção e a correta aplicação das PETs têm uma relação significativa com a efetividade de um PPSI.

Considerando os pontos discutidos, os achados deste trabalho destacam a importância crescente das tecnologias de proteção de dados e suas múltiplas aplicações em cenários digitais. No entanto, permanece o desafio de compreender como essas soluções podem ser adaptadas e implementadas de forma mais efetiva à realidade brasileira, marcada por especificidades culturais, regulatórias e tecnológicas. Por isso, sugere-se que novas pesquisas avancem na análise das barreiras, oportunidades e impactos das PETs no país, considerando a diversidade das características do setor público, assim como a percepção dos próprios titulares de dados. Estudos futuros dedicados ao contexto nacional certamente contribuirão para o desenvolvimento de estratégias mais alinhadas à nossa realidade, promovendo uma cultura de privacidade mais sólida e sustentável no Brasil.

REFERÊNCIAS

ABU-SALMA, R. et al. Obstacles to the adoption of secure communication tools. In: ieee symposium on security and privacy, 2017, San Jose, CA, EUA. [S. l.]: IEEE, 2017. p. [s.n.]. Disponível em: https://doi.org/10.1109/SP.2017.65.

ACQUISTI, A.; BRANDIMARTE, L.; LOEWENSTEIN, G. Privacy and Human Behavior in the Age of Information. **Science**, v. 347, n. 6221, p. 509-514, 2015.

ALSABAH, M.; GOLDBERG, I. Performance and Security Enhancements for Tor: A Survey. **ACM Computing Surveys (CSUR)**, v. 49, n. 2, p. 1–36, 2016. Disponível em: https://doi.org/10.1145/2946802. Acesso em: 18 jul. 2025.

ASERI, M.; DAWANDE, M.; JANAKIRAMAN, G.; MOOKERJEE, S. V. Ad Blockers: A Blessing or a Curse? **Information Systems Research**, v. 31, n. 2, p. 627–646, 2020. Disponível em: https://doi.org/10.1287/isre.2019.0906. Acesso em: 16 jul. 2025.

BALENDRA, U.; MAQSOOD, S. Motivações do usuário para navegação segura na web. In: 25ª Conferência Internacional HCI (HCII2023), Copenhague, Dinamarca, 2023. Disponível em: https://doi.org/10.1007/978-3-031-35822-7_28.

BENNETT, C. J.; RAAB, C. D. The Governance of Privacy: Policy Instruments in Global Perspective. **MIT Press**, 2006.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais – LGPD. **Diário Oficial da União**, Brasília, DF, 15 ago. 2018.

BRASIL. Ministério da Gestão e da Inovação em Serviços Públicos. Secretaria de Governo Digital. Cartilha do Programa de Privacidade e Segurança da Informação (PPSI). Versão 1.1. Brasília, DF: Gov.br, [2023]. Disponível em: https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/framework-guias-e-modelos/cartilha_ppsi.pdf . Acesso em: 11 jul. 2025.

BRASIL. Ministério da Gestão e da Inovação em Serviços Públicos. Secretaria de Governo Digital. Guia do Framework de Privacidade e Segurança da Informação. Versão 1.1.4. Brasília, DF: Gov.br, [2024]. Disponível em: https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/framework-guias-e-modelos/guia*framework*psi.pdf. Acesso em: 11 jul. 2025.

BRASIL. Ministério da Gestão e da Inovação em Serviços Públicos. Secretaria de Governo Digital. Programa de Privacidade e Segurança da Informação (PPSI). Brasília, DF: Gov.br, [2023]. Disponível em:

https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/ppsi-atual. Acesso em: 11 jul. 2025.

BYGRAVE, L. A. Data Protection Law: Approaching Its Rationale, Logic and Limits. **Kluwer Law International**, 2002.

CAULFIELD, T.; IOANNIDIS, C.; PYM, D. On the adoption of privacy-enhancing technologies. In: decision and game theory for security gamesec 2016, 7., 2016, Cham, Suíça. Cham, Suíça: Springer, 2016. p. [s.n.]. Disponível em: https://doi.org/10.1007/978-3-319-47413-7_11. Acesso em: 18 jul. 2025.

CLARKE, Roger. A future for identity. [Local de publicação, se houver, ex.: Canberra]: Xamax Consultancy Pty Ltd., 2000. Disponível em: http://www.rogerclarke.com/DV/FutureOfIdentity.html. Acesso em: 11 jul. 2025.

COHEN, J. E. Configuring the Networked Self: Law, Code, and the Play of Everyday Practice. **Yale University Press**, 2012.

DESPOTAKIS, S.; RAVI, R.; SRINIVASAN, K. The Beneficial Effects of Ad Blockers. **Management Science**, v. 67, n. 4, p. 2096–2125, 2020. Disponível em: https://doi.org/10.1287/mnsc.2020.3653. Acesso em: 16 jul. 2025.

DWORK, Cynthia; ROTH, Aaron. The Algorithmic Foundations of Differential Privacy. **Foundations and Trends® in Theoretical Computer Science**, v. 9, n. 3–4, p. 211–407, 2014.

EUROPEAN UNION. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation - GDPR). **Official Journal of the European Union**, L 119, 4 May 2016.

GILBERT, F. Global Privacy Book – The ultimate reference for Global Privacy and Security Law. Disponível em: https://globalprivacybook.com/. Acesso em: 16 jul. 2025.

HABIB, H. et al. Away from prying eyes: Analyzing the use and understanding of private Browse. In: symposium on usable privacy and security (soups 2018), 14., 2018, Baltimore, MD, EUA. Baltimore, MD, EUA: USENIX, 2018. Disponível em: https://www.usenix.org/conference/soups2018/presentation/habib-prying. Acesso em: 18 jul. 2025.

HARBORTH, D.; PAPE, S.; RANNENBERG, K. Explaining the usage behavior of privacy-enhancing technologies: The case of Tor and JonDonym. **Proceedings on Privacy Enhancing Technologies**, [s.l.], online, 2020. Disponível em: https://doi.org/10.2478/popets-2020-0020. Acesso em: 16 jul. 2025.

HEURIX, J.; ZIMMERMANN, P.; NEUBAUER, T.; FENZ, S. A taxonomy for privacy-enhancing technologies. **Computers & Security**, v. 53, p. 1–17, 2015. Disponível em: https://doi.org/10.1016/j.cose.2015.05.002. Acesso em: 16 jul. 2025.

HILDEBRANDT, M.; VAN DEN BERG, B. (Eds.). Freedom and Property of Information: The Philosophy of Law Meets the Philosophy of Technology. **Routledge**, 2014.

IBGE - Instituto Brasileiro de Geografia e Estatística. Pesquisa Nacional por Amostra de Domicílios Contínua (PNAD-C). Rio de Janeiro: IBGE, 2023. Disponível em: https://www.ibge.gov.br. Acesso em: 29 jul. 2025.

ITU - União Internacional de Telecomunicações. Report on ICT Development and Digital Inclusion. Genebra: ITU, 2023. Disponível em: https://www.itu.int. Acesso em: 29 jul. 2025.

JANIC, M.; WIJBENGA, J. P.; VEUGEN, T. Transparency Enhancing Tools (TETs): An Overview. In: workshop on sociotechnical aspects in security and trust, 3., 2013, Nova Orleans, LA, EUA. [S. l.]: IEEE, 2013. p. [s.n.]. Disponível em: https://doi.org/10.1109/STAST.2013.11. Acesso em: 16 jul. 2025.

KAPLAN, Robert S.; NORTON, David P. The strategy-focused organization: how balanced scorecard companies thrive in the new business environment. Boston, MA: **Harvard Business School Press**, 2001.

KELLEY, Craig; PROCTOR, Carol; DICKINSON, Adele. The Alignment Matrix: A Tool for Curriculum Planning and Mapping. **Journal of Curriculum and Teaching**, v. 10, n. 3, p. 117-128, 2021.

KNIGHT, S. Most popular email providers by number of users. Sell Cell, 2023. Disponível em: https://www.sellcell.com/blog/most-popular-email-provider-by-number-of-users/.

KROHNE, David et al. Aligning Privacy Compliance: A Matrix-Based Approach for Mapping PETs to Regulatory Frameworks. **Journal of Data Protection & Privacy**, v. 6, n. 2, p. 91-107, 2022.

KUNST, A. Do you take measures to prevent your online behavior from being recorded? Statista, 2019. Disponível em: https://www.statista.com/statistics/714108/us-online-usage-privacy-measures/. Acesso em: 6 ago. 2023.

MANGIÒ, F.; ANDREINI, D.; PEDELIENTO, G. Hands off my data: Users' concerns for security and intention to adopt privacy-enhancing technologies. **Italian Journal of Marketing**, v. 2020, n. 4, p. 309–342, 2020. Disponível em: https://doi.org/10.1007/s43039-020-00017-2. Acesso em: 16 jul. 2025.

MANTELERO, A. Além dos dados. Em: Além dos dados. Série Tecnologia da Informação e Direito, vol 36. **TMC Asser Press**, Haia, 2022. https://doi.org/10.1007/978-94-6265-531-7_1

MATHUR, A.; VITAK, J.; NARAYANAN, A.; CHETTY, M. Characterizing the Use of Browser-Based Blocking Extensions to Impede Online Tracking. In: symposium on usable privacy and security (soups 2018), 14., 2018, Baltimore, MD, EUA. Baltimore, MD, EUA: USENIX, 2018. Disponível em: https://www.usenix.org/conference/soups2018/presentation/mathur. Acesso em: 16 jul. 2025.

NAMARA, M. et al. Emotional and practical considerations on the adoption and abandonment of VPNs as privacy-enhancing technology. **Proceedings on Privacy Enhancing Technologies**, [s.l.], 2020. Disponível em: https://nru.uncst.go.ug/handle/123456789/3218. Acesso em: 18 jul. 2025.

NORCIE, G.; CAINE, K.; CAMP, L. J. Eliminating breakpoints in the installation and use of anonymity systems: A usability evaluation of the Tor browser bundle. In: workshop on hot topics in privacy enhancing technologies (hotpets), 5., 2012, Vigo, Espanha. [S. l.: s.n.], 2012.

NUNES, Lys Lugati; EVANGELISTA, Juliana; ALMEIDA, de. A LGPD e a construção de uma cultura de proteção de dados. **Revista de Direito**, v. 2, 2022. DOI: 10.32361/2022140113764.

OLIVEIRA, K. P.; DE BEM, A. A. G.; VALADARES, J. L. Serviços públicos e tecnologias digitais: uma análise bibliométrica. **Cadernos Gestão Pública e Cidadania**, v. 30, p. e92152, 2025. DOI: 10.12660/cgpc.v30.92152. Disponível em: https://periodicos.fgv.br/cgpc/article/view/92152. Acesso em: 3 jul. 2025.

ORGANIZATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT. Guidelines on the protection of privacy and transborder flows of personal data. **OECD Guidelines**, 1980.

PETROSYAN, A. Frequency of private Browse or incognito mode usage in the United Kingdom (UK) in February 2023. Statista, 2023. Disponível em: https://www.statista.com/statistics/1383920/uk-frequency-private-Browse-or-incognito-mode-usage/. Acesso em: 21 jul. 2023.

PHOON, T. S. K. Future of Machine Learning in Geotechnics (FOMLIG), 5–6 Dec 2023, Okayama, Japan. **Georisk Assessment and Management of Risk for Engineered Systems and Geohazards**, v. 18, n. 1, p. 288-303, 2024. DOI: 10.1080/17499518.2024.2316882.

REED, M. G.; SYVERSON, P. F.; GOLDSCHLAG, D. M. Anonymous connections and onion routing. **IEEE Journal on Selected Areas in Communications**, v. 16, n. 4, p. 482–494, 1998. Disponível em: https://doi.org/10.1109/49.668972. Acesso em: 16 jul. 2025.

SHINTAKU, M; SOUSA, R; COSTA, L; MOURA, R; MACEDO, D. Discussões sobre política de privacidade de dados em um sistema de informação governamental. **Em Questão**, v. 27, n. 4, p. 39-60, 2021.

SILVA, Maria A. et al. Elaborando matrizes de alinhamento em projetos de pesquisa: fundamentos e aplicações. **Revista de Metodologia Científica**, v. 5, n. 2, p. 104-117, 2021.

VAILSHERY, L. S. Global market share of leading internet browsers from January 2012 to May 2023. Statista, 2023. Disponível em: https://www.statista.com/statistics/268254/market-share-of-internet-browsers-worldwide-since-2009/. Acesso em: 6 ago. 2023.

VENKATESH, V.; THONG, J. Y.; XU, X. Consumer Acceptance and Use of Information Technology: Extending the Unified Theory of Acceptance and Use of Technology. **MIS Quarterly**, v. 36, n. 1, p. 157–178, 2012. Disponível em: https://doi.org/10.2307/41410412. Acesso em: 18 jul. 2025.

VILLELA, Renata S. et al. Utilização de matrizes de alinhamento para planejamento instrucional em cursos de pós-graduação. **Educação e Pesquisa**, v. 47, p. e227795, 2021.

WESTIN, Alan F. Social and political dimensions of privacy. **Journal of Social Issues**, v. 59, n. 2, p. 431-453, 2003.

WHITLEY, E. A. Informational privacy, consent and the control of personal data. **Information Security Technical Report**, v. 14, n. 3, p. 154–159, 2009. Disponível em: https://doi.org/10.1016/j.istr.2009.10.001. Acesso em: 16 jul. 2025.

ZIMMECK, S.; GOLDELMAN, D.; KAPLAN, O.; BROWN, L.; CASLER, J.; JUDELEY, JC; CHAMPEAU, J.; HARKOUS, H. Transparência de dados de sites no navegador. Anais do **Proceedings on Privacy Enhancing Technologies**, [S. l.], p. 1-21, 2024. Disponível em: https://doi.org/10.56553/popets-2024-0048. Acesso em: 18 jul. 2025.