Privacy-Enhancing Technologies in Digital Public Services: Bridging Legal Demands and Sociotechnical Design

Marta Juvina de Medeiros, Edna Dias Canedo

[1]University of Brasília (UnB), Department of Computer Science
Brasília, DF, Brazil

medeiros.marta@gmail.com, ednacanedo@unb.br

Abstract. ***Research Context****: Digital government increasingly relies on large-scale data processing for public services. Ensuring citizens' privacy while enabling data-driven value creation is a critical challenge for Information Systems (IS) in the public sector.* ***Scientific and/or Practical Problem****: Traditional safeguards (e.g., access control, anonymization) are insufficient against reidentification risks and inter-organizational data sharing demands. Public agencies lack actionable guidance to select and deploy Privacy-Enhancing Technologies (PETs) fitting legal, organizational, and technical constraints.* ***Proposed Solution and/or Analysis****: We synthesize categories and application patterns of PETs (Differential Privacy, Secure Multiparty Computation, Homomorphic Encryption, Federated Learning, Trusted Execution Environments, Synthetic Data) and analyze their suitability to government scenarios. We provide policy-to-PET mapping using recent Brazilian federal decrees.* ***Related IS Theory****: Grounded in* Sociotechnical Systems *(alignment of people, processes, and technologies),* Privacy by Design *as a strategy, and* Information Governance *for accountability, transparency, and risk management.* ***Research Method****: Concept-centric analysis of PETs and their governance implications; document analysis of 2025 executive decrees mentioning personal data; analytic generalization to derive PET selection rationales for public-sector IS.* ***Summary of Results****: We (i) clarify privacy vs personal data protection for design, (ii) categorize PETs by function and lifecycle stage (data in use, input/output privacy), (iii) derive PET recommendations for inter-agency collaboration, secure analytics, and transparency (e.g., MPC/HE for cross-entity processing; Differential Privacy for open statistics), and (iv) identify capability and governance gaps (skills, interoperability, stewardship).* ***Contributions and Impact to IS area****: We bridge PETs' technical capabilities with IS governance needs in digital government, offering a rationale for PET selection under regulatory, organizational, and sociotechnical constraints. The study advances responsible innovation in IS, informs public-sector architectures, and aligns with Brazil's GranDSI-BR (2016–2026) by addressing ethics, transparency, and societal impacts of intelligent IS.*

1. Introduction

Digital transformation has redefined how governments interact with citizens, with public services increasingly mediated by digital platforms and intelligent information systems [Venson et al. 2024]. In Brazil, federal, state, and municipal governments hereafter referred to as digital governments have progressively adopted information and com-

munication technologies (ICT) to enhance transparency, efficiency, and citizen experience. This movement, initially reinforced by the Digital Governance Strategy (EGD) [da Gestão e da Inovação em Serviços Públicos 2016], aligns with the global shift towards data-driven governance, but it also raises pressing challenges regarding privacy, security, and ethical use of personal data [Porto et al. 2025, Rocha and Canedo 2025, Braz and Canedo 2025, Spósito et al. 2025].

The expansion of digital services has led to unprecedented growth in the *volume*, *variety*, and *complexity* of personal data processing [Spósito et al. 2025a]. While offering clear benefits to citizens and organizations, this scenario amplifies risks to privacy and intensifies the need for robust governance models [Mahmodi Parchini et al. 2025]. Traditional safeguards, such as anonymization or access control, are insufficient in contexts of large-scale integration and inter-organizational data sharing [Shahriar et al. 2025]. From an Information Systems (IS) perspective, addressing this problem demands a sociotechnical approach that integrates people, processes, and technologies. Citizens, as data subjects, require autonomy and trust; organizations must establish transparent and accountable data governance; and technological mechanisms must ensure that services remain both innovative and privacy-preserving [Saraiva et al. 2025].

Unlike the private sector, public organizations operate under constitutional principles of legality, transparency, and public interest, which impose additional constraints on the design and operation of digital services [Pedrosa et al. 2025]. In the Brazilian context, public agencies are required to share data across institutions to support public policies, while simultaneously ensuring compliance with the LGPD and sector-specific regulations[Spósito et al. 2025]. This dual requirement creates unique challenges for the implementation of Privacy by Design, as technical solutions must be aligned not only with data protection principles but also with organizational, legal, and inter-institutional governance structures[Azevedo and Canedo 2025]. As a result, approaches and technical solutions commonly adopted in the private sector cannot be directly transferred to public digital services without careful adaptation.

Privacy-Enhancing Technologies (PETs) emerge as a promising class of solutions to reconcile innovation with fundamental rights. PETs encompass techniques such as Differential Privacy [Dwork and Roth 2014, Nissim and Wood 2017], Secure Multiparty Computation [Lindell 2020], Homomorphic Encryption [Kurth 2023], Federated Learning [Co-Operation and Development 2023], and Trusted Execution Environments (TEEs) [Kurth 2023]. Unlike traditional approaches that protect data only at rest or in transit, PETs extend protection to data in use, enabling secure computation, collaborative analytics, and responsible information sharing. They directly support the principle of Privacy by Design [Andrade et al. 2022], reinforcing compliance with Brazil's General Data Protection Law (LGPD) [Brasil 2018] and international frameworks such as the General Data Protection Regulation (GDPR) [Parliament and Council 2018].

Nevertheless, PETs are not a silver bullet. Their effectiveness depends on the convergence of legal, organizational, and technical measures. Implementing PETs in digital governments requires overcoming barriers such as lack of technical expertise, fragmented governance structures [Lemieux and Werner 2023, Razi et al. 2025, Saniei 2020], and limited capacity for interoperability across public agencies [Kamm et al. 2023]. These challenges highlight the strategic role of PETs in shaping not only technological infras-

tructures but also organizational processes and cultural attitudes towards responsible innovation in IS [Calvi et al. 2024].

Despite the increasing regulatory emphasis on privacy and data protection, recent assessments indicate that the adoption of Privacy-Enhancing Technologies (PETs) in Brazilian public digital services remains limited and uneven. Reports from oversight bodies and regulatory authorities highlight that privacy requirements are often addressed through procedural or legal measures, with little guidance on how to operationalize them through concrete technical solutions (e.g., oversight reports from Brazilian regulatory and audit bodies)[Spósito et al. 2025, PÚBLICOS 2024]. This gap between regulatory expectations and practical implementation underscores the need for systematic approaches that translate legal obligations into actionable technical and organizational mechanisms.

This study investigates how PETs can strengthen privacy and data protection in the context of Brazilian digital governments. We analyze concepts and categories of PETs, present current examples, and examine their alignment with sociotechnical principles of IS. Furthermore, we conduct a case-based analysis of federal executive decrees published in 2025 that explicitly regulate personal data processing, deriving recommendations for PET adoption. In doing so, the paper contributes to the **GranDSI-BR 2016–2026** by addressing the grand challenge of ensuring ethics, responsibility, and social impact in the development of intelligent information systems for public administration.

To address this gap, this paper makes the following contributions. First, it systematically analyzes recent Brazilian federal regulations related to digital government and data protection, identifying concrete obligations that affect the design and operation of public digital services. Second, it establishes a structured mapping between these regulatory requirements and Privacy-Enhancing Technologies, bridging legal, organizational, and technical perspectives within a sociotechnical Information Systems framework. Third, it derives practical implications for public managers, system designers, and policymakers, offering guidance on how PETs can support the operationalization of Privacy by Design in complex, inter-organizational public-sector environments.

The remainder of this paper is organized as follows. Section 2 reviews the background and related work on privacy, LGPD compliance, and PETs. Section 3 details the research method, including the regulatory mapping, PETs categorization, and cross-analysis. Section 4 reports the case-based results derived from Brazilian federal executive decrees (2024–2025), presenting PET recommendations and their legal hooks. Section 5 discusses implications for Information Systems theory and digital government practice, relating the findings to international frameworks and the Brazilian context. Section 6 examines threats to validity (construct, internal, external, and reliability). Finally, Section 7 concludes and outlines avenues for future work.

2. Background and Related Work

The consolidation of data privacy and personal data protection is a global concern, with direct implications for Information Systems (IS). In Brazil, the General Data Protection Law (LGPD) [Brasil 2018], inspired by the European Union's GDPR [Parliament and Council 2018], established a comprehensive framework for processing personal data. It introduced principles such as purpose limitation, necessity, transparency, and security, while also creating the National Data Protection Authority (ANPD). In

2022, Constitutional Amendment nº 115 elevated personal data protection to a fundamental right, reinforcing its centrality to digital government initiatives. However, studies show that Brazilian developers and organizations still face difficulties in interpreting and operationalizing the LGPD, due to lack of practical guides, limited training, and prioritization of functional over non-functional requirements [Peixoto et al. 2025, Rocha and Canedo 2025, Spósito et al. 2025b, Matos et al. 2025].

Although privacy is constitutionally guaranteed (Article 5 of the Brazilian Constitution) [1], the rapid growth of digital platforms has exposed structural weaknesses. Developers report barriers such as insufficient methodological support, absence of standardized tools, and the complexity of translating legal provisions into software requirements [Peixoto et al. 2025, Rocha and Canedo 2025, Spósito et al. 2025b]. Initiatives such as taxonomies of privacy requirements aligned with ISO/IEC 29100 and LGPD [Ferrão et al. 2024], privacy patterns catalogs [Neves Camêlo and Alves 2023], and automated compliance tools have been proposed, yet adoption in industry remains limited [Spósito et al. 2025b]. These challenges indicate the need for socio-technical approaches that combine law, organizational processes, and technical design.

Privacy-Enhancing Technologies (PETs) provide technical mechanisms to operationalize legal and organizational requirements. Recent surveys [Razi et al. 2025] identify four key categories of PETs widely used to strengthen privacy in IS: 1) **Data Anonymization**: Techniques such as k-anonymity, l-diversity, and t-closeness aim to prevent re-identification while balancing privacy and utility. Tools like ARX and sdcMicro are applied in domains such as healthcare and government statistics; 2) **Data Encryption**: Symmetric and asymmetric cryptography, together with advanced techniques like Homomorphic Encryption, Attribute-Based Encryption, and Proxy Re-encryption, ensure confidentiality during storage, transmission, and processing [Kurth 2023]; 3) **Synthetic Data Generation**: Generative models (GANs, VAEs, copula-based approaches) create artificial datasets that preserve statistical properties of real data without exposing individuals, enabling applications in healthcare, finance, and AI model training; and 4) **Differential Privacy**: Introduces mathematically calibrated noise into queries or datasets, providing quantifiable guarantees against re-identification even in large-scale analytics [Dwork and Roth 2014].

Other emerging approaches include Federated Learning, Trusted Execution Environments (TEEs), and privacy-preserving machine learning frameworks (e.g., PySyft, TensorFlow Privacy) that enable computation on distributed or encrypted datasets while maintaining privacy guarantees [Andrade et al. 2022, Razi et al. 2025].

The adoption of PETs in IS is closely linked to frameworks and methodologies from Requirements Engineering. Approaches such as PriS, LINDDUN, SQUARE, STRAP, and Secure Tropos provide systematic ways to elicit, analyze, and validate privacy requirements [Spósito et al. 2025b]. Privacy by Design (PbD) principles [Andrade et al. 2022] advocate embedding privacy into the architecture of IS, shifting from "privacy-by-policy" to "privacy-by-architecture". Despite promising results in academic settings, their industrial application remains incipient in Brazil, reflecting the broader challenge of aligning theory, regulation, and practice in sociotechnical contexts.

[1] https://www.planalto.gov.br/ccivil_03/Leis/L4320.htm

In this sense, PETs act not only as technological enablers but also as governance instruments, reinforcing accountability, transparency, and trust in digital public services. Their systematic adoption is essential for bridging the gap between compliance with LGPD and the effective protection of citizens' privacy in digital government ecosystems [Saraiva et al. 2025].

From an Information Systems perspective, PETs should not be understood merely as isolated technical mechanisms, but as sociotechnical artifacts whose effectiveness depends on organizational processes, governance arrangements, and institutional capabilities. In public digital services, their adoption requires coordination across agencies, alignment with legal interpretations, and integration into service design and data management practices. This reinforces the need for approaches that go beyond cataloging technologies and instead connect PETs to concrete regulatory and organizational requirements.

While these studies provide important insights into privacy regulation and the technical capabilities of PETs, they largely remain at either a conceptual or technological level, offering limited guidance on how legal requirements can be systematically translated into actionable design decisions in public-sector digital services.

2.1. Tools and the Use of PETs in Brazilian Digital Governments

Recent initiatives have provided structured frameworks to support the choice and recommendation of PETs for different processing scenarios. Examples include: (i) the ENISA PETs Control Matrix [ENISA 2016], which evaluates online and mobile privacy tools through generic and specific criteria such as maturity, usability, and technical properties; (ii) the TNO Decision Tree [TNO 2021], which guides organizations via an interactive process to identify applicable PETs (e.g., secure multiparty computation, federated learning, synthetic data, homomorphic encryption); and (iii) the UK-DSIT Adoption Guide [Department for Science and Technology 2025], which emphasizes ethical governance and provides recommendations based on concrete use cases. These frameworks illustrate international efforts to systematize the decision-making process regarding PET adoption, highlighting both technical features and organizational aspects.

In Brazil, however, the effective use of PETs by digital governments remains incipient. Motivations for their adoption are clear compliance with the LGPD, alignment with ethical and legal principles [Porto et al. 2025], and the promotion of innovation and inter-institutional collaboration but important challenges persist. Among them are the lack of technical expertise within the public sector, limited awareness of PETs' potential, scarcity of national case studies, fragmented governance structures, and concerns about the risks of adopting emerging and complex technologies [Saraiva et al. 2025]. Additionally, infrastructural limitations and the heterogeneity of public agencies hinder interoperability and coordinated adoption. As a result, governments often resort to traditional measures such as anonymization, while more advanced PETs remain underutilized.

Thus, while Brazil possesses a robust regulatory framework, including the LGPD and ANPD resolutions, the translation of these norms into practical PET adoption still requires capacity building, methodological support, and a cultural shift towards embedding privacy-by-design into public information systems. Addressing these challenges is essential for enabling digital governments to act as promoters of PET adoption and to reinforce citizens' trust in public digital services.

In summary, existing research has extensively discussed privacy principles, regulatory frameworks, and individual PETs, but there is a lack of systematic approaches that bridge these dimensions in the context of public digital services. In particular, prior studies rarely establish traceable links between concrete legal obligations and the selection or combination of PETs, nor do they address the organizational and governance implications of such mappings. This gap motivates the present study, which aims to operationalize Privacy by Design by aligning regulatory requirements with PETs within a sociotechnical Information Systems perspective. These limitations reinforce the need for approaches that explicitly map regulatory obligations to PETs in a traceable and context-aware manner.

3. Research Method

This study adopts a qualitative research design grounded in document analysis and concept-centric synthesis. The objective is to investigate how Privacy-Enhancing Technologies (PETs) can support compliance with Brazilian data protection regulation in the context of digital government. The focus on decrees published in 2025 reflects the most recent regulatory cycle of Brazilian digital government, allowing the analysis to capture current policy priorities and unresolved challenges related to the operationalization of privacy requirements.

The corpus is composed of three complementary sources: (i) **Brazilian legislation and regulation**, including the LGPD (Law No. 13.709/2018) [Brasil 2018], Constitutional Amendment nº 115/2022 [2], and resolutions issued by the National Data Protection Authority (ANPD)[3]; (ii) **Federal Executive Decrees published in 2025**[4], which explicitly mention personal data processing and information security in the context of digital government; and (iii) **Scientific and technical literature on PETs**, including international frameworks such as ENISA's PETs Control Matrix [ENISA 2016], TNO Decision Tree [TNO 2021], and the UK-DSIT Adoption Guide [Department for Science and Technology 2025]. The research followed three main steps:

1. **Regulatory mapping:** systematic extraction of obligations, principles, and guidelines from the LGPD, constitutional provisions, ANPD resolutions, and selected decrees. The objective was to identify explicit requirements (e.g., confidentiality, transparency, accountability) and implicit needs (e.g., interoperability, secure sharing) that could be operationalized through PETs. This stage produced a structured matrix of regulatory demands.
2. **PETs categorization:** review and synthesis of PETs according to recent surveys and technical reports, grouping them into functional categories such as anonymization, differential privacy, synthetic data generation, federated learning, and homomorphic encryption. For each category, we characterized strengths, limitations, and potential applicability to government contexts. This step resulted in a taxonomy of PETs tailored for digital public services.
3. **Cross-analysis:** alignment between the regulatory demands identified in Step 1 and the technical capabilities organized in Step 2. This stage aimed to generate actionable PET recommendations by linking specific legal/organizational provisions to PETs that could support compliance. The analysis produced mapping

[2]https://www.planalto.gov.br/ccivil_03/constituicao/Emendas/Emc/emc115.htm

[3]https://www.gov.br/anpd/pt-br

[4]https://www4.planalto.gov.br/legislacao/portal-legis/legislacao-1/decretos1/2025-decretos

tables indicating which PETs address which regulatory clauses, and under what conditions they could be deployed in Brazilian digital government ecosystems.

Figure 1 illustrates the overall research design, highlighting the inputs, analytical stages, and expected outcomes.

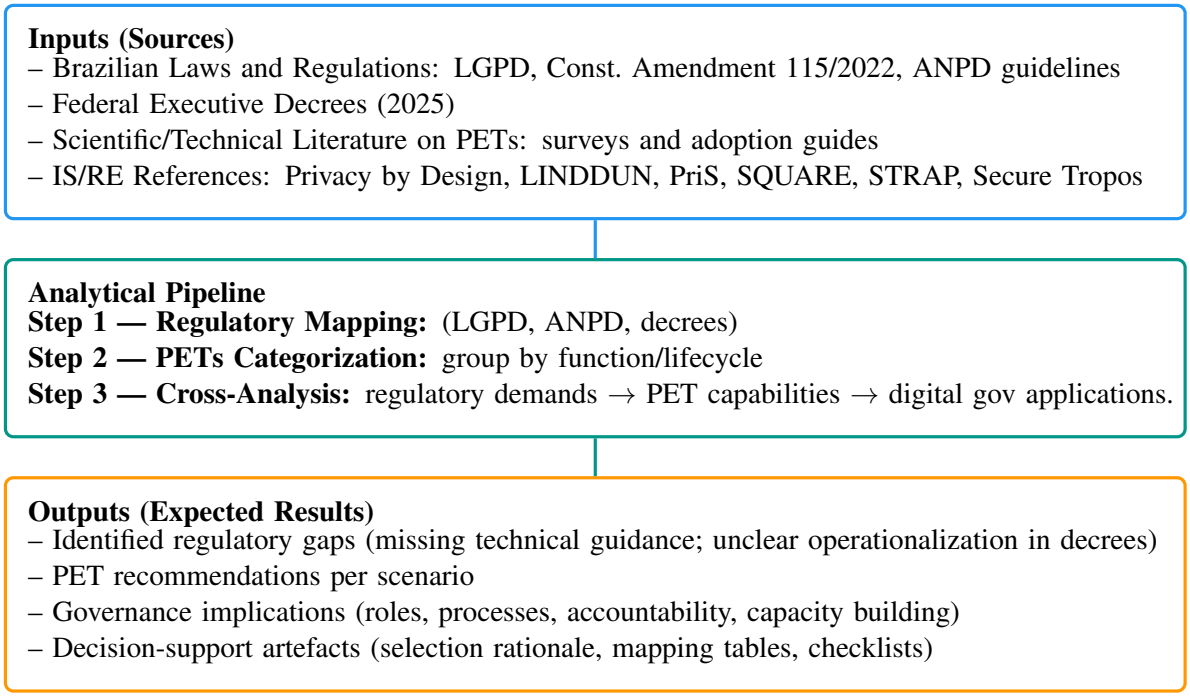

Figure 1. Research method: inputs, analytical pipeline, and expected outputs.

The cross-analysis followed a qualitative, concept-centric approach, aiming at analytical alignment rather than quantitative scoring. The resulting mappings should therefore be interpreted as contextual PET recommendations, not prescriptive technical mandates. This approach is consistent with Information Systems research, as it focuses on the alignment between regulatory requirements, technological capabilities, and organizational decision-making in digital government contexts.

4. Results

Following the protocol in Section 3, we examined federal executive decrees published in Brazil's *Diário Oficial da União* between Jan. 1 and Aug. 17, 2025, selecting only those that explicitly mention the term "personal data". Decrees of appointment/exoneration and those merely creating or altering organizational charts were excluded. The analysis was performed on the full text of each decree in isolation (besides LGPD), and all PET recommendations are educational in nature and context-dependent (organizational maturity, datasets, risk, infrastructure, etc.)

The following subsections present the analysis of selected federal executive decrees. For each decree, we describe the regulatory context, identify privacy-relevant data processing scenarios, and derive PET recommendations grounded in legal provisions and organizational requirements. The tables synthesize these mappings, highlighting the relationship between PETs, their practical utility, and the corresponding legal justification.

4.1. Decree No. 12.574, of August 5, 2025: National Integrated Policy for Early Childhood

This decree establishes the National Integrated Policy for Early Childhood (PNIPI), focusing on the coordinated management of public policies for all Brazilian children. Although the decree does not explicitly mention the term *personal data*, it requires the processing of information related to socioeconomic, territorial and regional situations, as well as ethnic-racial, gender, and disability characteristics. Consequently, it involves the processing of data concerning vulnerable data subjects (children) and sensitive categories (e.g., ethnic-racial and disability data).

The combination of vulnerable and sensitive data heightens the risks of discrimination and re-identification, making compliance with the LGPD particularly challenging. PETs are therefore essential to enable secure integration, sharing, and analysis of such data across agencies while maintaining privacy protection. The PET recommendations derived from this analysis are summarized in Table 1.

Table 1. PET recommendations for Decree No. 12.574/2025 (National Integrated Policy for Early Childhood).

PET	Application	Utility	Legal Justification
Secure Multi-Party Computation (SMPC)	Joint elaboration of studies, indicators, and statistics on early childhood without agencies accessing each other's raw data	Enables ministries (Health, Education, Social Assistance) to collaborate securely in monitoring child development without revealing the datasets under their custody	Intersectoral coordination and federative articulation (Art. 1, §1; Art. 2, VII-VIII); data integration and strategic action plan (Art. 5, §3; Art. 6; Art. 7, III)
Homomorphic Encryption (HE)	Secure sharing and processing of sensitive, socioeconomic, and territorial data for monitoring and evaluation of PNIPI	Ensures confidentiality of data in transit and storage, particularly in cloud and integrated systems, while enabling computation over encrypted datasets	Monitoring and evaluation with integrated data (Art. 5, §§1-2; Art. 7, III); LGPD compliance (Art. 5, §6)
Differential Privacy (DP)	Public dissemination of disaggregated data for social control, policy-making, and academic research	Minimizes re-identification risk, strengthens transparency, and enables public monitoring of PNIPI without compromising individual privacy	Publication of protected data (Art. 5, §5); promotion of equity and anti-discrimination (Art. 2, X); coordinated monitoring and evaluation (Art. 7, IV)

These PET recommendations illustrate how PETs can support intersectoral collaboration while mitigating risks of discrimination and re-identification in policies involving

vulnerable populations.

4.2. Decree No. 12.572, of August 4, 2025: National Information Security Policy

This decree establishes the National Information Security Policy (PNSI), providing structural guidelines for information security governance within the federal public administration. Although the decree does not specify concrete categories of personal data to be processed, it explicitly includes the protection of personal data as one of its principles and objectives. The text also outlines classical PET recommendations of information security and governance, such as administrative controls and personnel training, which are fundamental for effective implementation.

Because PETs are not limited to technological tools alone, this decree creates opportunities to embed privacy-by-design approaches from the outset, balancing innovation with information security and personal data protection. Such measures contribute to building citizens' trust in the safe use of their data by digital governments. The PET recommendations are summarized in Table 2.

Table 2. PET-related recommendations for Decree No. 12.572/2025 (National Information Security Policy).

PET/Measure	Application	Utility	Legal Justification
Access Control and Identity Management	Management of access to systems and data, including authentication, authorization, and auditing	Reduces risks of unauthorized access, prevents policy violations, and supports the principles of confidentiality and institutional accountability for information security	Public responsibility and risk management (Art. 3, II and VI)
Education and Training in Information Security	Training of public agents involved in the data lifecycle in federal administration	Fosters a culture of information security, reduces human errors, and raises awareness of best practices	Education as an instrument for culture (Art. 3, IV) and promotion of qualification and continuous culture (Art. 8, III and IV)
Governance, Standardization, and Auditing	Development of policies, regulations, audits, and compliance assessments to ensure effective implementation of the PNSI	Ensures transparency, accountability, and alignment with established standards, reinforcing credibility in public information security governance	Development of policies, regulations, and international cooperation (Art. 8, II and VI); auditing by the internal control system (Art. 9); responsibilities of agencies and entities (Art. 10)

This decree reinforces that PET adoption in digital government depends not only on cryptographic mechanisms, but also on governance structures, training, and accountability processes.

4.3. Decree No. 12.564, of July 24, 2025: Biometric Verification in Payroll-Deducted Credit Operations

This decree regulates Article 2-I of Law No. 10.820/2003 to establish procedures and technical requirements for biometric identity verification of workers, their consent for the processing of biometric personal data, and the use of electronic and digital signatures in payroll-deducted credit operations for contracting and registration. The normative text requires that public operators and financial institutions adopt biometric verification with *proof of life*, ensuring the authenticity of individuals in payroll-deduction credit transactions.

Although the decree identifies workers as the data subjects, it does not specify which biometric modality may be used (e.g., facial recognition, fingerprints, or others). The text explicitly cites the principle of authenticity and recommends multi-factor authentication techniques as security mechanisms. The PET recommendations are summarized in Table 3.

Table 3. PET recommendations for Decree No. 12.564/2025 (Biometric Verification in Payroll-Deducted Credit).

PET/Measure	Application	Utility	Legal Justification
Zero-Knowledge Proof (ZKP)	Applied in biometric verification, allowing the verifying entity to confirm that the biometric data matches a valid record without revealing the biometric itself	Eliminates the need to expose or transfer biometric data to the financial institution, ensuring stronger privacy protection. Supports secure biometric verification with proof of life, guaranteeing authenticity of the contracting party	Ensure authenticity of the contracting party (Art. 2); biometric verification with proof of life (Art. 3, II, a)

4.4. Decree No. 12.561, of July 24, 2025: Mandatory Biometric Registration for Social Security Benefits

This decree establishes the mandatory biometric registration for the granting, maintenance, and renewal of federal social security benefits. The regulation requires the processing of personal data from all citizens who are beneficiaries of social services, although it does not specify the exact categories of data to be used in biometric registration and verification.

The decree explicitly states the interoperability between biometric databases of the National Driver's License (CNH), the Federal Police's civil identification system, and the National Civil Identification managed by the Superior Electoral Court, until the creation

of a unified Biometric Registry. It also reinforces the need to ensure security, privacy, and protection of personal data in these processes. The recommendations are summarized in Table 4.

Table 4. PET recommendations for Decree No. 12.561/2025 (Mandatory Biometric Registration for Social Security Benefits).

PET/Measure	Application	Utility	Legal Justification
Homomorphic Encryption (HE)	Protection of biometric data processing during authenticity verification, even in shared environments	Enables secure validation without exposing raw biometric data, mitigating fraud and leakage risks	Art. 2, §3 (interoperability) and Art. 4 (biometric verification)
Secure Multi-Party Computation (SMPC)	Secure collaboration among public agencies for biometric validation without revealing the full datasets under their custody	Ensures protection of biometric data across different entities, preserving privacy in interoperability	Art. 2, §3 (interoperability) and Art. 4 (biometric verification)

4.5. Decree No. 12.560, of July 23, 2025: National Health Data Network and SUS Digital Platforms

This decree creates the National Health Data Network (RNDS) and regulates the SUS Digital Platforms, ensuring interoperability within the Unified Health System (SUS) across the entire national territory. The RNDS is designed to integrate health, administrative, financial, and registration data related to health services and actions.

The decree encompasses all categories of data subjects, including children, adolescents, the elderly, and other vulnerable groups. Although it does not list data categories explicitly, it mandates the processing of personal data revealing physical and mental health information (therefore classified as sensitive), in addition to financial and registration data, whether from the present, past, or future.

It explicitly cites the principles of information security, privacy, confidentiality, transparency, and the ethical and lawful use of data, in line with the LGPD. The PET recommendations derived from this analysis are summarized in Table 5.

4.6. Decree No. 12.555, of July 16, 2025: Cabotage Program (BR do Mar)

This decree regulates the rules, criteria, and procedures to be observed by public and private entities for the implementation, authorization, execution, and monitoring of the Cabotage Incentive Program (BR do Mar), established by Law No. 14.301/2022. It also regulates provisions of Law No. 9.432/1997 and Law No. 10.893/2004.

Table 5. PET recommendations for Decree No. 12.560/2025 (National Health Data Network and SUS Digital Platforms).

PET/Measure	Application	Utility	Legal Justification
Homomorphic Encryption (HE)	Interoperability of personal and sensitive health data across multiple entities, ensuring secure computation without exposing raw data	Supports secure extraction of statistics, medical queries, audits, and population studies, while reinforcing confidentiality in transit and processing	Art. 2 (proportionality); Art. 6 (confidentiality and information security)
Secure Multi-Party Computation (SMPC)	Collaboration among multiple entities in scenarios such as epidemic monitoring and registry integration, without any entity accessing full datasets from others	Preserves privacy of patients and health professionals, enabling inter-institutional analyses without undue exposure	Art. 3 (secure interoperability); Art. 6 (protection of data in federated access and broad sharing scenarios)
Differential Privacy (DP)	Publication of reports, dashboards, and public statistics (including for research) while minimizing re-identification risks	Indispensable to ensure broad public access to Brazilian health information while safeguarding individual privacy	Art. 6 (principles of privacy, confidentiality, and efficiency); Arts. 15–16 (dissemination and access to information)

The decree specifies the requirements for navigation companies and the conditions for vessel chartering. From its provisions, it can be inferred that personal data processing primarily involves crew members and maritime workers, including sensitive data related to health. It also provides for collaboration and data sharing between public and private sector entities.

These aspects create opportunities for adopting PETs to ensure privacy-preserving inter-institutional collaboration and to support transparency mechanisms. The recommendations are summarized in Table 6.

This case highlights that PETs are also relevant beyond traditionally sensitive domains such as health or social protection, extending to logistics and labor-intensive economic programs.

5. Discussion

The analysis of federal decrees published in 2024–2025 revealed that, although Brazilian digital government initiatives are progressively incorporating privacy and security principles, there remain significant challenges in operationalizing these obligations into concrete technical measures. The recommendations presented in the Results section demonstrate that Privacy-Enhancing Technologies (PETs) [Razi et al. 2025] provide actionable

Table 6. PET recommendations for Decree No. 12.555/2025 (Cabotage Program – BR do Mar).

PET/Measure	Application	Utility	Legal Justification
Secure Multi-Party Computation (SMPC)	Collaboration among multiple entities (e.g., Ministry of Ports and Airports, Ministry of Labor and Employment, ANTAQ) to jointly analyze crew and worker data without revealing full datasets	Preserves privacy in inter-institutional cooperation, enabling federated analyses while preventing undue exposure of sensitive information	Art. 5 (oversight of Brazilian crew admission); Art. 4 (data processing for program monitoring); Art. 28 (reporting of health events)
Differential Privacy (DP)	Publication of dashboards, reports, and statistics derived from BR do Mar data while minimizing risks of individual re-identification	Strengthens transparency, social accountability, and public oversight without compromising individual privacy	Art. 22 (monitoring of the BR do Mar Program)

pathways to address these challenges, particularly when sensitive data and vulnerable populations are involved. These recommendations should be understood as analytical guidance rather than prescriptive solutions, as their feasibility depends on organizational maturity and contextual constraints.

From a theoretical perspective, our findings align with the literature that emphasizes the persistent difficulties faced by Brazilian developers and organizations in translating the LGPD into practice [Peixoto et al. 2025, Rocha and Canedo 2025, Spósito et al. 2025b]. As highlighted by Ferrão et al. [Ferrão et al. 2024] and Camelo et al. [Neves Camêlo and Alves 2023], the absence of standardized tools, taxonomies, and design patterns hinders the consistent adoption of privacy by design [Andrade et al. 2022]. The decrees analyzed here illustrate this gap: while they incorporate LGPD principles (e.g., authenticity, transparency, confidentiality), they do not specify how such principles should be technically operationalized. Our mapping suggests that PETs can act as socio-technical bridges between legal mandates and information system implementations, reinforcing the socio-technical nature of privacy protection.

International frameworks such as ENISA's PETs Control Matrix [ENISA 2016], the TNO Decision Tree [TNO 2021], and the UK-DSIT Adoption Guide [Department for Science and Technology 2025] provide structured decision-making processes for PET adoption, balancing legal compliance, usability, and governance. Our results echo these initiatives, but with a Brazilian focus: PETs such as Secure Multi-Party Computation, Homomorphic Encryption, and Differential Privacy emerge as critical for inter-institutional data sharing, biometric authentication, and the dissemination of public statistics. Unlike these generic frameworks, our analysis grounds PET selection in

concrete regulatory mandates, explicitly linking legal provisions to technical mechanisms in public-sector contexts. These findings extend prior studies by contextualizing PET applicability to specific regulatory scenarios in the Brazilian public sector, such as the National Integrated Policy for Early Childhood, the National Health Data Network, and the BR do Mar Cabotage Program.

The discussion also highlights that PETs cannot be viewed as purely technological artifacts. As observed by [Spósito et al. 2025a] and [Saraiva et al. 2025], their effective adoption depends on organizational readiness, training of public servants, and robust governance structures. This was evident in decrees such as the National Information Security Policy, where recommendations centered not only on cryptographic tools but also on identity management, auditing, and capacity building. This reinforces the view that PETs act as governance instruments, supporting accountability, transparency, and citizen trust in digital services.

Moreover, the analysis points to the need for advancing research on the socio-technical integration of PETs, embedding privacy by design and PETs into the architecture and governance of digital public services. While academic contributions on privacy patterns, taxonomies, and requirements engineering frameworks are advancing [Spósito et al. 2025b, Andrade et al. 2022], their translation into government practice remains incipient. The decrees studied illustrate both the opportunity and the urgency of embedding privacy by design and PETs into the architecture of digital public services. Bridging this gap requires interdisciplinary collaboration across law, computer science, information systems, and public administration.

Finally, this study contributes to the broader IS research agenda by demonstrating how empirical analysis of regulatory instruments can be combined with technical knowledge from PETs to generate context-specific recommendations. By doing so, it responds to the call for research that addresses the "Grand Challenges of Information Systems in Brazil" (GranDSI-BR 2016–2026), particularly the challenges of digital governance, transparency, and privacy in an era increasingly shaped by artificial intelligence and data-intensive systems.

6. Threats to Validity

As with any qualitative study based on document analysis, this research is subject to certain limitations that must be acknowledged. To enhance transparency and methodological robustness of the study, we discuss threats to validity across four dimensions. Construct validity concerns whether the concepts analyzed were correctly identified and operationalized. The analysis was limited to decrees explicitly referencing the term "personal data". As a result, some normative texts with indirect implications for privacy and data protection may not have been included. Furthermore, the mapping of PETs to regulatory provisions was interpretative, based on the authors' synthesis of legal and technical sources. To mitigate this, the study relied on established frameworks in privacy engineering [Spósito et al. 2025b, Andrade et al. 2022, Spósito et al. 2025a, Saraiva et al. 2025] and on international PET adoption guides [ENISA 2016, TNO 2021, Department for Science and Technology 2025]. This scope was deliberately adopted to ensure analytical consistency and traceability.

Internal validity relates to the causal inferences drawn from the analysis. This

study did not seek to establish causal relationships but rather to explore opportunities for applying PETs in the context of Brazilian decrees. However, by focusing on textual analysis only, we did not account for political, organizational, or technological factors that may influence the implementation of these decrees in practice. The recommendations should therefore be interpreted as illustrative rather than prescriptive. External validity refers to the generalizability of findings. The decrees analyzed were restricted to the period between December 2024 and August 2025, which may not represent the entire regulatory landscape of Brazilian digital government. Moreover, the recommendations are tailored to the Brazilian context and may not be directly applicable to other jurisdictions, although the methodological approach linking regulations to PETs can be adapted internationally. Although the empirical scope is national, the analytical approach can be transferred to other regulatory contexts with similar data protection frameworks.

Reliability addresses the consistency and replicability of the study. The analysis followed a systematic process: (i) selection of decrees based on explicit mentions of personal data; (ii) extraction of relevant provisions; and (iii) mapping to PETs using theoretical and practical references. Nonetheless, because the mapping process required interpretative judgments, different research teams might arrive at partially different recommendations. To mitigate this risk, we documented the analysis procedure and provided detailed tables (Section 4) to support verification and replication.

In sum, while the study provides valuable insights into the applicability of PETs in Brazilian digital government, its results must be interpreted in light of the methodological boundaries. Future work should triangulate document analysis with interviews, case studies, or empirical evaluations of PET adoption to strengthen construct and external validity.

7. Conclusion

This study analyzed the role of Privacy-Enhancing Technologies (PETs) as strategic tools and approaches to ensure the protection of personal data and the privacy of citizens in the context of Brazilian digital government. The study showed that privacy and data protection, recognized as fundamental rights, must adapt to technological transformations and the growing flow of information in a data-driven society. The exponential increase in personal data processing has demanded proportional responses, and PETs have emerged as essential mechanisms to balance the legitimate use of personal data with the safeguarding of individual rights.

Our findings highlight that PET adoption extends beyond technical mechanisms to encompass organizational, legal, and cultural dimensions of data governance. Embedding privacy by design into the architecture of systems and services requires not only technical safeguards but also robust governance structures and institutional cultures oriented toward accountability and transparency. Although complex, PETs such as Homomorphic Encryption, Secure Multi-Party Computation, and Differential Privacy offer viable and proactive mechanisms to mitigate risks and support ethical and lawful data processing, particularly in critical domains such as health, early childhood, and social security.

The case analysis of federal executive decrees published in 2024–2025 underscored both the opportunities and challenges of PET adoption in the public sector. While the decrees reinforce LGPD principles authenticity, confidentiality, transparency, and

security they do not specify the technical pathways for operationalizing them. Our mapping demonstrated that PETs can bridge this gap by providing actionable solutions to enable secure interoperability, privacy preserving data sharing, and trustworthy dissemination of public information. These findings align with international frameworks [ENISA 2016, TNO 2021, Department for Science and Technology 2025] while contextualizing their application in the Brazilian regulatory environment. Our mapping demonstrated that PETs can bridge this gap by providing actionable, regulation-grounded recommendations.

Despite their promise, PET adoption in Brazilian digital government still faces significant barriers, including limited technical expertise, institutional resistance to adopting emerging technologies, and concerns about implementation costs and interoperability. As highlighted in related studies [Peixoto et al. 2025, Rocha and Canedo 2025, Spósito et al. 2025a, Saraiva et al. 2025], overcoming these challenges requires investment in capacity building, organizational readiness, and systematic governance practices. Addressing these gaps will be crucial for enabling PETs to move from academic proposals and international reports into sustained and large-scale adoption in the Brazilian public sector.

In conclusion, the effectiveness of privacy protection in digital government depends not only on advanced technologies but on a multidimensional approach that integrates institutional, legal, technical, and cultural aspects. Strengthening data governance, expanding the training of public servants, and systematically embedding PETs into digital services are decisive steps toward supporting the development of a modern, transparent, and trustworthy state one that respects and protects its citizens across all dimensions of digital interaction.

Acknowledgments

This study was financed in part by the Project No. TED 33/2023 “Pesquisa Aplicada em Privacidade e Segurança da Informação na Diretoria de Privacidade e Segurança da Informação da Secretaria de Governo Digital" – Diretoria de Privacidade e Segurança da Informação (DPSI)/Centro de Excelência em Privacidade e Segurança (CEPS)/ Secretaria de Governo Digital (SGD) do Ministério da Gestão e da Inovação (MGI) em Serviços Públicos do Governo Federal; and Conselho Nacional de Desenvolvimento Científico e Tecnológico CNPq (Grant Nº 300883/2025-0).

References

Andrade, V. C., Gomes, R. D., Reinehr, S. S., de Almendra Freitas, C. O., and Malucelli, A. (2022). Privacy by design and software engineering: a systematic literature review. In Canedo, E. D., Viana, D., Garcia, V. C., Bezerra, C. I. M., de Sousa Santos, I., Gadelha, B., Machado, I., Soares, S., Kulesza, U., de França, B., Conte, T., Maldonado, J. C., Reinehr, S. S., Malucelli, A., Albuquerque, A. B., Santos, G., Barcellos, M. P., dos Santos, R. P., Lima, C., Monteiro, D., Damian, A., and Rocha, L., editors, *Proceedings of the XXI Brazilian Symposium on Software Quality, SBQS 2022, Curitiba, Brazil, November 7-10, 2022*, pages 18:1–18:10. ACM.

Azevedo, L. F. D. and Canedo, E. D. (2025). A structured checklist approach to evaluating transparency and privacy in brazilian digital services. In Santos, G., Reinehr, S. S.,

de Farias Júnior, I., Gadelha, B., Barcellos, M., Freire, S., de França, B. B. N., Canedo, E. D., Oran, A. C., Matsubara, P., and Parizi, R., editors, *Proceedings of the 24th Brazilian Symposium on Software Quality, SBQS 2025, São José dos Campos, SP, Brazil, November 4-7, 2025*, pages 400–410. SBC.

Brasil (2018). Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). *Diário Oficial da República Federativa do Brasil*.

Braz, A. and Canedo, E. (2025). Mapping lgpd principles to ethical principles in the context of artificial intelligence. In *Anais do VI Workshop sobre as Implicações da Computação na Sociedade*, pages 1–13, Porto Alegre, RS, Brasil. SBC.

Calvi, A., Malgieri, G., and Kotzinos, D. (2024). The unfair side of privacy enhancing technologies: addressing the trade-offs between pets and fairness. In *The 2024 ACM Conference on Fairness, Accountability, and Transparency, FAccT 2024, Rio de Janeiro, Brazil, June 3-6, 2024*, pages 2047–2059. ACM.

Co-Operation, O. F. E. and Development (2023). Oecd guidelines on the protection of privacy and transborder flows of personal data. *OECD*, page 1–65.

da Gestão e da Inovação em Serviços Públicos, M. (2016). Estratégia de governança digital. *Governo Digital*.

Department for Science, I. and Technology (2025). Privacy enhancing technologies adoption guide. *Centre for Data Ethics and Innovation's (CDEI)*.

Dwork, C. and Roth, A. (2014). The algorithmic foundations of differential privacy. *Found. Trends Theor. Comput. Sci.*, 9(3-4):211–407.

ENISA (2016). Readiness analysis for the adoption and evolution of privacy enhancing technologies. *European Union Agency for Cybersecurity*.

Ferrão, S. É. R., Silva, G. R. S., Canedo, E. D., and Mendes, F. F. (2024). Towards a taxonomy of privacy requirements based on the LGPD and ISO/IEC 29100. *Inf. Softw. Technol.*, 168:107396.

Kamm, L., Bogdanov, D., Brito, E., and Ostrak, A. (2023). Blueprints for deploying privacy enhancing technologies in e-government. In Bieker, F., Conca, S. D., Gruschka, N., Jensen, M., and Schiering, I., editors, *Privacy and Identity Management. Sharing in a Digital World - 18th IFIP WG 9.2, 9.6/11.7, 11.6 International Summer School, Privacy and Identity 2023, Oslo, Norway, August 8-11, 2023, Revised Selected Papers*, volume 695 of *IFIP Advances in Information and Communication Technology*, pages 3–19. Springer.

Kurth, H. A. (2023). Privacy-enhancing and privacypreserving technologies: Understanding the role of pets and ppts in the digital age. *CIPL*, page 1–25.

Lemieux, V. L. and Werner, J. (2023). Protecting privacy in digital records: The potential of privacy-enhancing technologies. *ACM Journal on Computing and Cultural Heritage*, 16(4):83:1–83:18.

Lindell, Y. (2020). Secure multiparty computation. *Commun. ACM*, 64(1):86–96.

Mahmodi Parchini, M., Riazi, L., and Porebrahimi, A. (2025). Proposed model for data governance implementation with emphasis on privacy protection. *Sciences and Techniques of Information Management*.

Matos, A., Patrício, M., Nicolau, M. I., Canedo, E. D., Pereira, J. A., and Uchôa, A. G. (2025). Data privacy in software practice: Brazilian developers' perspectives. *J. Internet Serv. Appl.*, 16(1):299–319.

Neves Camêlo, M. and Alves, C. (2023). G-priv: A guide to support lgpd compliant specification of privacy requirements. *iSys - Brazilian Journal of Information Systems*, 16(1):2:1 – 2.

Nissim, K. and Wood, A. (2017). Differential privacy: A primer for a non-technical audience. *Workshop on New Advances in Disclosure Limitation (CDAC)*.

Parliament, T. E. and Council, T. (2018). General Data Protection Regulation (GDPR). *Intersoft Consulting*.

Pedrosa, G., Canedo, E., Pereira, W., and Figueiredo, R. (2025). Digital public service evaluation in brazil: Federal managers' perspectives and improvement opportunities. In *Anais do XIII Latin American Symposium on Digital Government*, pages 97–108, Porto Alegre, RS, Brasil. SBC.

Peixoto, M. M., Gorschek, T., Méndez, D., Silva, C., and Fucci, D. (2025). The perspective of agile software developers on data privacy. *J. Softw. Evol. Process.*, 37(2).

Porto, D., Prado, R., Marques, G., Serrano, A., Mendonça, F., and Canedo, E. (2025). Ethical requirements in the age of artificial intelligence: A systematic literature review. In *Anais do XXI Simpósio Brasileiro de Sistemas de Informação*, pages 663–672, Porto Alegre, RS, Brasil. SBC.

PÚBLICOS, M. D. G. E. D. I. E. S. (2024). Programa de privacidade e seguranÇa da informaÇÃo (ppsi), versão 1.1.4. *PRESIDÊNCIA DA REPÚBLICA*, 2:1–178.

Razi, Q., Piyush, R., Chakrabarti, A., Singh, A., Hassija, V., and Chalapathi, G. S. S. (2025). Enhancing data privacy: A comprehensive survey of privacy-enabling technologies. *IEEE Access*, 13:40354–40385.

Rocha, L. D. and Canedo, E. D. (2025). Optimizing compliance: Comparative study of data laws and privacy frameworks. *J. Internet Serv. Appl.*, 16(1):431–452.

Saniei, R. (2020). Challenges in the implementation of privacy enhancing semantic technologies (pests) supporting GDPR. In Rodríguez-Doncel, V., Palmirani, M., Araszkiewicz, M., Casanovas, P., Pagallo, U., and Sartor, G., editors, *AI Approaches to the Complexity of Legal Systems XI-XII - AICOL International Workshops 2018 and 2020: AICOL-XI@JURIX 2018, AICOL-XII@JURIX 2020, XAILA@JURIX 2020, Revised Selected Papers*, volume 13048 of *Lecture Notes in Computer Science*, pages 283–297. Springer.

Saraiva, J., Souza, C., and Soares, S. (2025). Mmai-lgpd: A maturity model for governance and data compliance in information systems institutions. In *Anais do XXI Simpósio Brasileiro de Sistemas de Informação (SBSI)*, pages 788–797, Porto Alegre, RS, Brasil. SBC.

Shahriar, S., Dara, R., and Akalu, R. (2025). A comprehensive review of current trends, challenges, and opportunities in text data privacy. *Comput. Secur.*, 151:104358.

Spósito, S. L., Alves, K., Nunes, R. R., Ferreira, L. R., and Canedo, E. D. (2025). Structuring privacy and information security competencies for public sector roles: A frame-

work for enhancing software quality and LGPD compliance. In Santos, G., Reinehr, S. S., de Farias Júnior, I., Gadelha, B., Barcellos, M., Freire, S., de França, B. B. N., Canedo, E. D., Oran, A. C., Matsubara, P., and Parizi, R., editors, *Proceedings of the 24th Brazilian Symposium on Software Quality, SBQS 2025, São José dos Campos, SP, Brazil, November 4-7, 2025*, pages 365–375. SBC.

Spósito, S., Moreira, F., and Canedo, E. (2025a). Designing a training journey for privacy and information security practitioners in the federal public administration. In *Anais do XXI Simpósio Brasileiro de Sistemas de Informação (SBSI)*, pages 95–104, Porto Alegre, RS, Brasil. SBC.

Spósito, S. L., Targino, J. F. G., Silva, G. R. S., Peotta, L., Porto, D. d. P., Mendonça, F. L. L., and Canedo, E. D. (2025b). A comprehensive review of techniques, methods, processes, frameworks, and tools for privacy requirements. *Journal of Internet Services and Applications*, 16(1):508–529.

TNO (2021). Pet decision tree. *Netherlands Organisation for Applied Scientific Research*.

Venson, E., da Costa Figueiredo, R. M., and Canedo, E. D. (2024). Leveraging a startup-based approach for digital transformation in the public sector: A case study of brazil's startup gov.br program. *Gov. Inf. Q.*, 41(3):101943.