A Structured Checklist Approach to Evaluating Transparency and Privacy in Brazilian Digital Services

Luciano Franceschi De Azevedo
Ministry of Entrepreneurship, Microenterprise and Small Businesses (MEMP)
Brasília–DF, Brazil
lfazevedo@hotmail.com

Edna Dias Canedo
University of Brasília (UnB)
Brasília–DF, Brazil
ednacanedo@unb.br

ABSTRACT

Context: The digitalization of public services in Brazil has improved access and efficiency, but has also raised concerns about transparency, privacy, and data protection. Despite the regulatory framework established by the Brazilian General Data Protection Law (LGPD), many services still lack clear communication and support for citizens regarding how their data is handled. **Objective:** This study aims to evaluate the trustworthiness of digital public services in Brazil, from the perspective of an ordinary citizen, by analyzing the alignment between declared privacy practices and actual data handling behaviors, as well as the accessibility of support provided to citizens in exercising their data protection rights. **Method:** We developed and applied a structured evaluation checklist based on three dimensions: (i) Declared Information Quality (QID), (ii) Factual Precision (PF), and (iii) Accessibility Support (AS). Five widely used federal services were selected and analyzed through manual inspection of public documentation, service behavior, and availability of support channels. Each item was scored based on predefined criteria, and qualitative observations were recorded to complement the analysis. **Results:** The overall average score across all services was 44.76%, with the best performance in factual precision (77.14%) and the worst in privacy support (20.00%). Only one service—"Conta Gov"—achieved a score above 50%. Transparency deficits were common, especially in the disclosure of sensitive data handling and the availability of dedicated support channels or Data Protection Officers (DPOs). **Conclusion:** The study reveals that while several services functionally comply with privacy expectations, most fail to communicate this effectively to users. The absence of accessible and explicit privacy declarations, combined with limited support mechanisms, undermines citizens' ability to exercise their rights and reduces trust in digital government services. Our findings highlight the need for standardized privacy documentation and specialized support channels, reinforcing the importance of transparency as a critical component of software quality in the public sector.

CCS CONCEPTS

• **Security and privacy → Human and societal aspects of security and privacy**; *Social aspects of security and privacy.*

KEYWORDS

Digital Public Services, Privacy, Data protection, Transparency, Citizens, Digital Transformation

1 INTRODUCTION

The digitalization of public services has become one of the main drivers of administrative transformation in Brazil, promoting broader access and increased efficiency in the delivery of essential services to the population [9, 14, 25]. With the growing adoption of digital platforms—especially in recent years—public administration has become more agile, while enabling direct and real-time interaction between citizens and the government [11]. However, despite the benefits of this digital expansion, it also brings forth critical challenges, particularly related to information security, personal data protection, and transparency in government operations [2, 10, 12].

The digitalization of public services in Brazil is underpinned by a legal framework aimed at safeguarding citizens' data and ensuring effective governance of digital platforms. A cornerstone of this framework is the Brazilian General Data Protection Law (LGPD)[6], enacted in 2020, which aligns with international best practices such as the European Union's General Data Protection Regulation (GDPR) [24]. The LGPD establishes obligations for the processing of personal data, defines data subjects' rights, and imposes penalties on public and private organizations that fail to comply. Therefore, adherence to this legislation is crucial to ensure that digital public services operate ethically and legally [4, 17].

Yet, as data collection and processing via platforms and apps increases, critical questions arise regarding citizens' privacy [5, 7, 22]. We argue that transparency plays a central role in building a trustworthy digital environment. As the main catalyst in this process, the public sector bears the responsibility of ensuring that the information it discloses aligns with actual service operations. Gaps, inaccuracies, or discrepancies in publicly available information can undermine public trust, potentially limiting citizens' willingness to adopt new digital services and accept emerging technologies [14, 26, 27].

Although many Brazilians recognize the advantages of digital public services—particularly in terms of convenience and agility—they have expressed concerns, especially regarding services related to social benefit control and taxation [13]. This resistance often stems from uncertainty about how their personal data will be used by the government [16]. We find that a significant portion of citizens approach these services with caution, fearing that their personal and behavioral data could be used to increase surveillance and control by public authorities. It is not uncommon to encounter narratives expressing these concerns. For instance: "We do not recommend using the "celular seguro" service because the government might track your real-time location and potentially use this information against you." " We do not recommend using the "online income tax declaration service", as the government might detect that you ran certain simulations and could use this information to monitor you more closely."

Without making any value judgments about the legitimacy of such fears, this study aims to objectively assess the trustworthiness of digital public services [1, 8, 28], focusing on their transparency and compliance with data protection principles. Such public skepticism is understandable, especially since many digital services aim to enhance governmental control and policy effectiveness by identifying fraud and analyzing behavioral patterns through data integration. In addition, with the exponential rise in cyber threats and citizens' growing awareness of digital risks [21, 23], it becomes increasingly important for public authorities to ensure the clarity and accuracy of information related to data collection and processing [19]. In this context, the study evaluates five widely used federal digital public services, aiming to answer the central research question: **RQ:*How trustworthy is a digital public service in terms of what it claims to do with citizens' data versus what it actually does?***

The study focuses on the alignment between declared and actual data practices—that is, "what the service says it does" versus "what it really does." We analyze the information disclosed to citizens by the responsible authorities regarding data collection and processing practices, including: The types of data collected; Retention periods; Data sharing with third parties; Availability and responsiveness of privacy support channels.

We also verify observable indicators of actual data collection and processing practices, and evaluate the clarity and accessibility of support channels related to privacy and data protection. Legal Framework and Evaluation Criteria The objectives of this study are grounded in Article 6 of the LGPD [6], which outlines the principles for personal data processing, including: Lawfulness and transparency: Data processing must be legitimate and explicitly communicated to data subjects (Article 6, I); Data minimization: Only the minimum necessary data should be collected and processed for the purposes declared (Article 6, II); Access and support: Citizens must have easy access to information about their data, which requires an accessible and efficient support process (Article 6, III); Clarity and precision: Information about data processing must be clear, explicit, and accurate (Article 6, VI).

We also examine whether services collect additional information—such as device identifiers, access to media, sensor data, temporary session information, and other metadata—and whether their storage and retention practices are consistent with the declared purposes. The transparency and clarity of publicly available information about the Data Protection Officer (DPO) [15]—a key figure in data privacy governance—are also analyzed. We assess whether services provide effective and accessible support channels that allow users to engage with the responsible public authorities regarding data protection concerns.

Another important aspect is the clear identification of the responsible agency. Surprisingly, many services fail to clearly disclose this information, which can hinder users' ability to access appropriate support channels—especially in cases where responsibilities are shared across agencies. Given the broad scope of themes related to digital public service quality, privacy, and security, this study does not address other technical aspects of data security or the robustness of privacy-enhancing technologies. To answer the research question, we propose the following analytical dimensions: 1) Quality of disclosed information – Does the responsible agency provide accessible, clear, and complete information about data collection and processing? 2) Accuracy of actual data processing – To what extent do actual data practices align with the declared ones? 3) Accessibility of privacy support channels: Do the channels exist, are they clearly disclosed, and are they accessible?"

2 BACKGROUND

The Brazilian government has acknowledged the need to strengthen privacy and information security within public administration through structured guidance. In this context, the *Information Security and Privacy Program* (PPSI) [20] serves as a practical framework to support federal public agencies in implementing the principles established by the General Data Protection Law (LGPD)[6]. The PPSI organizes a comprehensive set of controls into categories such as governance, security, and privacy. This study focuses on five privacy-related controls defined by the PPSI that directly impact the quality and legal compliance of digital public services:

- **Data Minimization:** Personal data collected by public services must be strictly limited to what is necessary to fulfill a specific and legitimate purpose. This control helps ensure proportionality and reduce privacy risks.
- **Purpose Specification:** Public organizations must define and document the specific purposes for data collection and communicate them to data subjects.
- **Justification of Collection:** Each data item must have a legal and functional basis, reinforcing accountability and supporting privacy by design.
- **Retention and Disposal:** Data must be kept only for as long as necessary and securely discarded thereafter.
- **Transparency:** Citizens must have clear and accessible information about how their data is collected, used, and shared.

These controls reflect the broader objective of the PPSI: to integrate privacy and security practices into both operational routines and strategic planning. When embedded into the software development lifecycle, such practices enhance not only legal compliance but also the quality, reliability, and credibility of digital public services.

Several recent studies have investigated related dimensions of quality in public digital services. The PS-DigQual model [3] proposed a multidimensional framework for evaluating service quality from the citizen's perspective, emphasizing accessibility, usability, transparency, and interoperability. However, the study focuses primarily on perception-based dimensions and does not assess actual compliance with data protection norms or the operationalization of privacy principles. Another study explored a startup-based approach to digital transformation in the public sector, highlighting the need for agility, experimentation, and user-centered development practices [25]. Although this approach aligns with modern service delivery principles, it leaves open questions regarding how legal compliance and data governance are maintained amid rapid iteration. Further, job perception analyses within digitally transformed public environments [14] indicate structural and cultural challenges that affect how digital services are developed and maintained. These include the fragmentation of roles and a lack of clarity about responsibilities related to privacy and service quality.

From a user perspective, an exploratory study with 143 respondents identified 14 key quality attributes grouped into four dimensions: Usability and Interaction, Technical Aspects, Efficient Delivery, and Service Feasibility [18]. Notably, users rated information quality, security, reliability, and effort as the most relevant factors influencing satisfaction. However, the study did not evaluate the extent to which services actually meet declared privacy obligations or how accessible the privacy-related information is to users.

Complementary studies also emphasize the gap between formal privacy regulations and their implementation in software development practices. A recent empirical study with Brazilian developers [16] found limited awareness and inconsistent integration of privacy practices, indicating a disconnect between legal requirements and day-to-day engineering. Likewise, a training journey for privacy and security practitioners in federal agencies [22] proposed a capacity-building roadmap, yet did not evaluate how this translates into improved service transparency or user trust. Despite this growing body of research, few studies have evaluated whether digital public services in Brazil declare and apply privacy practices in alignment with the LGPD, or whether users can easily find support to exercise their rights. There is also a lack of metrics and evaluation strategies that integrate privacy, transparency, and legal compliance into the broader discussion of software product quality in the public sector.

This study aims to fill this gap by proposing and applying a structured evaluation framework based on three critical dimensions: declared information quality, factual precision, and specialized support. By examining the presence, accessibility, and alignment of privacy-related declarations with actual practices, we contribute to the understanding of product quality in public digital services, reinforcing the role of transparency and data governance in trustworthy software.

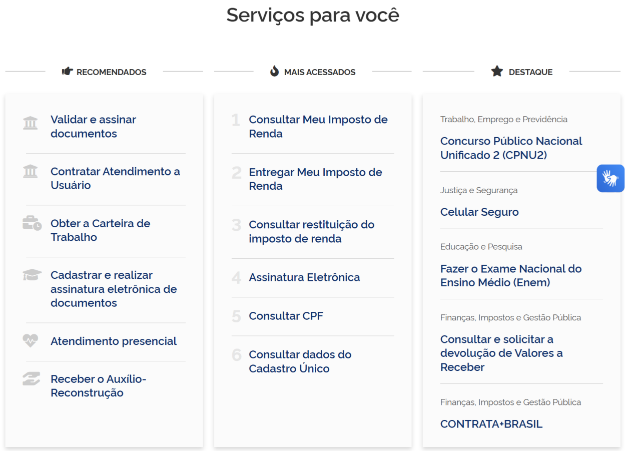
3 METHODOLOGY

This study aims to evaluate the quality of digital public services offered by the Brazilian federal government with respect to the collection, processing, and governance of personal data. The analysis focuses on three key dimensions: the clarity and completeness of the information disclosed about data practices, the alignment between declared and observed behaviors, and the availability of effective support channels for data privacy concerns.

To structure this evaluation, we designed a checklist-based instrument composed of 21 items, which reflect critical aspects of service quality in the context of personal data protection. The checklist is divided into three assessment categories:

- **Declared Information Quality (QID)** – Evaluates the clarity, accessibility, and completeness of the information provided by the service regarding the collection of personal and sensitive data, the purposes of data use, data sharing, retention policies, and international transfers.
- **Factual Precision (PF)** – Assesses whether the data practices observed in the service's actual operation are consistent with what is officially declared. To avoid penalizing services for missing or unverifiable declarations, this category adopts a three-point scale: full alignment, unverifiable or undeclared, and divergent from the declaration.
- **Support Quality (QS)** – Measures the presence and accessibility of key support structures, such as the identification of the responsible agency, the Data Protection Officer (DPO), and channels for citizens to exercise their data rights. These items are evaluated with a binary scale (yes/no) to minimize subjectivity.

Five digital public services were selected based on the "Most Accessed Services" ranking from the official gov.br portal (https://www.gov.br/pt-br), extracted in early July 2025. Figure 1 illustrates the selection criteria. The chosen services represent both current high-usage platforms and those with broad societal relevance, even if not trending at the time of analysis.



Serviços para você

RECOMENDADOS

Validar e assinar documentos

Contratar Atendimento a Usuário

Obter a Carteira de Trabalho

Cadastrar e realizar assinatura eletrônica de documentos

Atendimento presencial

Receber o Auxílio-Reconstrução

MAIS ACESSADOS

1 Consultar Meu Imposto de Renda

2 Entregar Meu Imposto de Renda

3 Consultar restituição do imposto de renda

4 Assinatura Eletrônica

5 Consultar CPF

6 Consultar dados do Cadastro Único

DESTAQUE

Trabalho, Emprego e Previdência

Concurso Público Nacional Unificado 2 (CPNU2)

Justiça e Segurança

Celular Seguro

Educação e Pesquisa

Fazer o Exame Nacional do Ensino Médio (Enem)

Finanças, Impostos e Gestão Pública

Consultar e solicitar a devolução de Valores a Receber

Finanças, Impostos e Gestão Pública

CONTRATA+BRASIL

Figure 1: Most accessed services on the gov.br portal, extracted on 02/07/2025.

Each service was evaluated by the authors through a structured review of its official declaration in the gov.br catalog, its associated documentation (such as terms of use and privacy policies), and its implementation on mobile platforms (Apple App Store and Google Play Store), when available. We prioritized information disclosed in the official catalog but considered other public sources when relevant. Discrepancies between information sources—such as outdated or inconsistent declarations—were taken into account, particularly in the evaluation of QID.

Each checklist item received a score according to predefined criteria, as detailed in Table 1. For each service, we calculated individual and aggregate scores by summing the item-level points and expressing them as a percentage of the maximum possible score (rounded to one decimal place). In addition to the quantitative assessment, we recorded qualitative observations to support further analysis and triangulation of findings.

This assessment model contributes to the software quality by providing a practical framework to evaluate digital public services under dimensions that directly impact product quality—namely transparency, compliance, and user trust—as expected in data-driven service ecosystems.

Table 1: Checklist of Evaluation Items Across the Three Categories

ID	Category	Question	Question Details	Scoring Criteria
1	QID	Clearly declares the collection of personal data?	The service explicitly declares, in a direct and accessible way, information about the collection of personal data.	2 – fully 1 – partially 0 – not declared
2	PF	Collects personal data as declared?	An initial analysis confirms whether the service effectively collects personal data as described.	2 – exactly 1 – no declaration 0 – collects differently
3	QID	Clearly declares the collection of sensitive personal data?	The service explicitly declares the collection of sensitive personal data in a clear and accessible manner.	2 – fully 1 – partially 0 – not declared
4	PF	Collects sensitive personal data as declared?	An initial analysis confirms whether the service collects sensitive data as declared.	2 – exactly 1 – no declaration 0 – collects differently
5	QID	Clearly declares the purpose for data collection?	The service states, in accessible terms, the purpose of the collected data.	2 – fully 1 – partially 0 – not declared
6	PF	Applies declared purpose in practice?	It is possible to confirm that the declared purposes are plausible and applied in practice.	2 – exactly 1 – no declaration / not verifiable 0 – differs from declaration
7	QID	Clearly declares the collection of device information?	The service states the collection of device data (e.g., IP, MAC address) used to access the service.	2 – fully 1 – partially 0 – not declared
8	PF	Collects device and access data as declared?	An initial analysis confirms the actual collection of device/access data as declared.	2 – exactly 1 – no declaration / not verifiable 0 – collects differently
9	QID	Clearly declares data sharing practices?	The service declares whether data is shared with other agencies or entities.	2 – fully 1 – partially 0 – not declared
10	PF	Shares data as declared?	An initial analysis confirms whether data sharing occurs as declared.	2 – exactly 1 – no declaration / not verifiable 0 – differs from declaration
11	QID	Clearly declares data retention period?	The service explicitly informs the data retention and disposal periods.	2 – fully 1 – partially 0 – not declared
12	PF	Applies declared retention rules in practice?	It is possible to confirm whether the declared retention periods are respected.	2 – exactly 1 – no declaration / not verifiable 0 – differs from declaration
13	QID	Clearly declares international data transfers?	The service states whether collected data is transferred internationally.	2 – fully 1 – partially 0 – not declared
14	PF	Applies international transfer rules as declared?	It is possible to confirm that international transfer practices match the declaration.	2 – exactly 1 – no declaration / not verifiable 0 – differs from declaration
15	AS	Declares the responsible agency?	The service clearly identifies the agency responsible for its operation.	2 – yes 0 – no
16	AS	Declares the Data Protection Officer (DPO)?	The service clearly provides the DPO contact details.	2 – yes 0 – no
17	AS	Declares the privacy support channel?	The service indicates how to access the privacy support channel.	2 – yes 0 – no
18	AS	Provides direct access to privacy support?	The service offers direct access to the privacy support channel via declaration or internal links.	2 – yes 0 – no
19	AS	DPO data is easily found on the agency's website?	DPO contact is visible on the homepage or main menu of the agency's website.	2 – yes 0 – no
20	AS	DPO data found via site search?	DPO contact appears among the top 10 results in the agency's website search.	2 – yes 0 – no
21	AS	Agency site provides a dedicated privacy support channel?	The agency's official site has a dedicated channel for privacy and data protection issues.	2 – yes 0 – no

4 ANALYSIS AND RESULTS

This section presents the results of the checklist-based evaluation applied to five federal digital public services, according to the methodology described in Section 3. We begin by acknowledging potential limitations in scoring accuracy due to the interpretative nature of some assessment criteria.

Items under the categories *Declared Information Quality (QID)* and *Factual Precision (PF)* involve three response levels and require the evaluators' judgment regarding completeness, clarity, and plausibility. As such, some degree of subjectivity is inherent, especially when assessing whether the declared information sufficiently meets the criteria or when approximating factual consistency in the absence of formal confirmation from the responsible agency. Therefore, scores presented here should be considered provisional and subject to future revision, given the dynamic nature of digital services and evolving privacy practices.

Similarly, items in the *Accessibility Support (AS)* category, despite using a binary scale (yes/no), depend on the evaluators' ability to locate the required information based on predefined criteria. This includes verifying whether privacy support contacts and DPO information are clearly and easily accessible through official websites or service pages.

In addition to numeric scores, qualitative observations recorded by the authors during the checklist application offer valuable insights. These comments are particularly relevant for justifying borderline cases and guiding service providers toward more transparent and citizen-friendly practices. Evaluations were conducted from a citizen-centered perspective, simulating the experience of an average user attempting to understand how their data is handled.

Service #01 – *"Criar conta gov"*

This service is a foundational component of Brazil's digital public services ecosystem, enabling citizens to create a unified login for accessing a wide range of services across government levels. It is provided and maintained by the Digital Government Secretariat (SGD)[1] of the Ministry of Management and Innovation in Public Services (MGI) [2].

Despite its central role, the service does not include a user feedback or evaluation mechanism on the gov.br portal. It is categorized under "Science and Technology" → "Promotion" → "Digital Inclusion." The official catalog entry is available at: https://www.gov.br/pt-br/servicos/criar-sua-conta-gov.br.

Table 2 summarizes the checklist scores for this service. The overall score of **54.7%** reveals a moderate level of trustworthiness regarding declared and actual data handling practices. However, the breakdown across the three quality dimensions shows notable discrepancies:

1. **Factual Precision (100%):** The service demonstrates full alignment between declared and observed practices. It explicitly states the collection of personal, sensitive, and device-level data, as well as the sharing of such data with third parties—including private entities. The clarity of these declarations, despite potential privacy implications, supports a strong score in this category.
2. **Declared Information Quality (50%):** The key weakness lies in the accessibility and usability of the information. Although required declarations are available, they are not found within the official *gov.br* service catalog. Instead, they appear in lengthy and highly technical documents (terms of use and privacy notice) embedded in the login page via non-downloadable and non-printable iframes. These issues hinder user comprehension and conflict with principles of transparency and citizen-centered service design.
3. **Accessibility Support (28.6%):** While the responsible agency and DPO are nominally declared, contact information is not easily accessible or discoverable via official websites. A practical test of the available chat support interface revealed that attendants were unable to provide answers to privacy-related questions. This suggests a functional gap between the declared purpose of the support channel and its actual capabilities.

Based on these findings, some observations can be made regarding the product quality of this digital service:

- **Service positioning:** The name "Criar conta gov" may not fully reflect the scope of the service, which also enables account recovery, identity validation, and user profile management.
- **Information accessibility:** Key privacy-related information is not available directly in the gov.br catalog entry. Instead, it is embedded in complex legal texts (terms of use and privacy notice) located on the login page. These documents are written in highly technical language and presented in a non-downloadable, non-printable frame, limiting user access and understanding.
- **Scoring implications:** Due to the limited accessibility of privacy information and its presentation format, several QID items received partial scores.
- **Declared practices vs. actual behavior:** The service broadly declares its use of personal and sensitive data, including sharing with private entities. Based on these explicit declarations and observed behavior, all PF items were scored as fully aligned.
- **Support channel test:** An attempt to contact the support channel indicated in the privacy policy ("Falar com atendente") revealed that attendants were not equipped to answer privacy-related questions. They clarified that the channel was intended only for technical account issues, contradicting the stated scope of support.
- **User feedback mechanisms:** Given the strategic importance of this service, it would be appropriate to include a user evaluation or feedback feature.

Service #02 – *"Realizar a Assinatura Eletrônica de Documentos"*

This service was selected due to its extensive use by the public and its critical importance in ensuring legal security and protecting citizens' privacy. It is particularly relevant to this study given its operational mechanics: the platform temporarily uploads the document to be signed to its infrastructure before returning the signed version to the user, which introduces significant privacy and security implications.

Similar to Service #01, this platform is provided and maintained by the Digital Government Secretariat of the Ministry of Management and Innovation in Public Services (MGI/SGD). It is categorized on the *gov.br* portal under "Science and Technology" → "Promotion" → "Digital Inclusion" and holds a high user rating of 4.7 out of 5, based on more than 670,000 reviews. The official service catalog is available at: https://www.gov.br/pt-br/servicos/assinatura-eletronica. Direct access to the platform is through: https://assinador.iti.br/.

Before presenting specific observations, it is worth highlighting that despite the service's functional relevance and high user ratings, the transparency regarding its data practices is notably insufficient. The checklist results reveal a consistent pattern of non-declaration across all privacy-related informational dimensions. This limits users' ability to make informed decisions and may compromise their trust. Below we present the main observations and recommendations regarding the service:

- **Absence of privacy declarations:** The service does not provide any explicit declaration—positive or negative—regarding the collection and processing of personal or sensitive data. This resulted in a score of 0% for the "Declared Information Quality" dimension.
- **Limited alignment:** Despite the absence of declarations, the evaluation inferred through use and system interaction that the service does process personal and device-related data. Thus, factual precision items received partial credit.
- **Separation from gov.br terms:** Although the login procedure relies on the *gov.br* identity platform, it is inappropriate to assume that the privacy policies and terms of use from

[1] https://www.gov.br/gestao/pt-br/composicao/secretaria-de-governo-digital
[2] https://www.gov.br/gestao/pt-br

Table 2: Checklist results – Service #01 “Criar conta gov”

ID	Category	Question (summary)	Score
1	QID	Declares collection of personal data?	1
2	PF	Collects personal data as declared?	2
3	QID	Declares collection of sensitive personal data?	1
4	PF	Collects sensitive personal data as declared?	2
5	QID	Declares purpose for data collection?	1
6	PF	Applies declared purposes?	2
7	QID	Declares device data collection?	1
8	PF	Collects device data as declared?	2
9	QID	Declares data sharing practices?	1
10	PF	Shares data as declared?	2
11	QID	Declares data retention period?	1
12	PF	Applies retention policies?	2
13	QID	Declares international data transfer?	1
14	PF	Applies international transfer rules?	2
15	AS	Declares responsible agency?	2
16	AS	Declares the DPO?	2
17	AS	Declares the privacy support channel?	0
18	AS	Provides direct access to privacy support?	0
19	AS	DPO contact easily found on agency site?	0
20	AS	DPO contact found via site search?	0
21	AS	Dedicated privacy support channel offered?	0
		Overall Score	**54.7%**
		Declared Information Quality (QID)	50.0%
		Factual Precision (PF)	100.0%
		Accessibility Support (AS)	28.6%

Table 3: Checklist results – Service #02 “Realizar a Assinatura Eletrônica de Documentos”

ID	Category	Question (summary)	Score
1	QIF	Clearly declares the collection of personal data?	0
2	PF	Collects personal data as declared?	1
3	QIF	Clearly declares the collection of sensitive personal data?	0
4	PF	Collects sensitive personal data as declared?	1
5	QIF	Clearly declares purposes for data collection?	0
6	PF	Applies purposes as declared?	1
7	QIF	Clearly declares collection of device/access information?	0
8	PF	Collects device/access data as declared?	1
9	QIF	Clearly declares data sharing practices?	0
10	PF	Shares data as declared?	1
11	QIF	Clearly declares data retention policy?	0
12	PF	Applies retention policy as declared?	1
13	QIF	Clearly declares international data transfer?	0
14	PF	Applies international transfer policy as declared?	1
15	AS	Declares responsible agency?	2
16	AS	Declares the DPO?	0
17	AS	Declares the privacy support channel?	0
18	AS	Provides direct access to privacy support?	0
19	AS	DPO contact easily found on agency site?	0
20	AS	DPO contact found via site search?	0
21	AS	Dedicated privacy support channel offered?	0
		Overall Score	**21.4%**
		Declared Information Quality (QID)	0.00%
		Factual Precision (PF)	50.0%
		Accessibility Support (AS)	14.2%

gov.br fully apply to this digital signature service. These distinctions are critical and should be explicitly clarified in the service’s documentation.

- **Lack of device data declarations:** The service does not mention the collection of device identifiers or metadata, which is concerning given its reliance on uploads and cryptographic operations.
- **High operational risk demands higher transparency:** Given the service’s mechanics—uploading and processing user documents—explicit declarations regarding technical behavior, storage duration, encryption, and data handling practices are essential. Without them, legal certainty and user trust are undermined.

These findings underscore the service’s low transparency and minimal user support, despite its essential role. Addressing these shortcomings is necessary not only for LGPD compliance but to improve perceived quality and accountability in digital service delivery.

Service #03 – *“Declarar meu Imposto de Renda - DIRPF”*

This service was selected due to its strategic relevance to Brazilian society. Filing an annual personal income tax return is a legal obligation with direct implications on taxation and potential penalties, often perceived with resistance and mistrust by users. Moreover, the system processes a wide range of sensitive data, including identification, financial, property, and dependent-related information, which makes it central to our privacy and transparency evaluation.

The online version of the tax return, analyzed in this study, represents a recent innovation compared to the traditional desktop application. It is provided by the Special Secretariat of the Federal Revenue of Brazil and is listed on the *gov.br* portal under the category "Finance, Taxes and Public Management → Taxes and Obligations → Income Tax and Tax Processing". The service has a rating of 4.6 out of 5 based on over 2.5 million reviews. Catalog link: https://www.gov.br/pt-br/servicos/declarar-meu-imposto-de-renda, Direct access: https://mir.receita.fazenda.gov.br/portalmir Before presenting the detailed observations, it is important to emphasize that the overall transparency of this service is above average in terms of LGPD-related declarations. However, there are inconsistencies between what is declared and what is actually practiced, especially regarding sensitive data processing and device data collection. Observations and Recommendations:

- **Sensitive data misstatement:** The declaration states that no sensitive personal data is collected, which appears inaccurate given the nature of information required in the income tax return—e.g., financial assets, dependent details (including disabilities), properties, and expenses. This discrepancy may mislead users and should be corrected.
- **Device data unmentioned:** There is no declaration regarding the collection of device or access metadata, despite partial evidence of such practices.
- **Institutional attribution issue:** The declaration mentions the Special Secretariat of the Federal Revenue of Brazil, but fails to clarify its affiliation with the Ministry of Finance, potentially confusing users. The link also redirects to the gov.br catalog rather than the institution's official website.
- **Absence of a dedicated privacy channel:** No dedicated support channel is provided for privacy-related inquiries. The general Fala.br platform is listed, but it aggregates multiple topics and does not allow direct communication with the DPO.
- **Positive mention of LGPD:** The service declaration includes a specific section referencing the LGPD, consolidating relevant information, which is considered a strong point.
- **Unclear retention policy:** The data retention statement is vague, using legalistic terms such as "at least while the right is not extinguished," which may hinder user understanding and trust.
- **Over-reliance on external references:** The linked privacy policy provides abundant legal references but lacks clarity on specific practices of this service, reducing its usefulness to end users.

Overall, the service demonstrates an effort toward transparency but still requires critical improvements to ensure alignment between declared practices and actual data handling, particularly with regard to clarity, completeness, and accessibility of privacy-related information.

Service #04 - *"Meu INSS"*

The "Meu INSS" service, provided by the National Social Security Institute (INSS), allows Brazilian citizens to access a wide range of social security-related services online, either via the portal https://meu.inss.gov.br or through the mobile application. Due to its massive public usage, the high volume and sensitivity of the personal data processed, and its structure composed of several internal micro-systems, this service was deemed highly relevant for this study.

As a newly updated version marked as "new" on the *gov.br* portal, the service does not yet feature user review data in the official catalog. Despite this, its operational role and privacy implications make it critical for assessing compliance and transparency with the General Data Protection Law (LGPD). Catalog link: https://www.gov.br/pt-br/temas/meu-inss. Direct access: https://meu.inss.gov.br/#/login. The following findings reflect both positive elements and critical areas for improvement regarding transparency, information consistency, and user support. As a comprehensive platform aggregating numerous micro-systems, "Meu INSS" must clearly communicate its privacy practices across all access points. Observations and Recommendations:

- **Lack of standardized privacy declarations:** The *gov.br* service catalog entry lacks basic LGPD-related information. Although a privacy policy is accessible within the logged-in environment, it should be directly linked from the public catalog page.
- **Sensitive data collection discrepancy:** The policy declares that sensitive data is not collected; however, due to the nature of INSS records (e.g., health-related benefits), this claim is misleading. In contrast, an official LGPD document from INSS acknowledges such data processing, highlighting an inconsistency that should be resolved.
- **Fragmented service structure:** The "Meu INSS" platform consolidates multiple services without clear modular separation, complicating individual analysis and transparency about specific data practices.
- **Privacy support channel is insufficient:** The only available contact for privacy issues is the general-purpose Fala.br platform. Additionally, although the LGPD page on the INSS website provides the DPO's name and email, it is unclear whether this serves as a dedicated privacy support channel.
- **Positive documentation initiative:** The same LGPD page links to a comprehensive PDF guide with detailed definitions and explanations of data processing practices. However, the guide's content partially contradicts the service's own privacy policy, signaling a need for harmonization.
- **Recommendation for consistency and centralization:** A broader standardization effort is needed to ensure coherence across all service-related privacy documents and access points. This includes harmonizing the catalog page, internal service interface, INSS's institutional website, and LGPD guidance materials.

Service #05 - *"Celular Seguro BR"*

The "Celular Seguro BR" initiative, developed by Brazil's Ministry of Justice and Public Security (MJSP), aims to combat smartphone theft and robbery. It provides a digital platform for citizens to report incidents and remotely block devices, banking applications, and other digital services. The service is accessible via web browser and mobile app, and its functionality involves access to sensitive data such as geolocation and device sensors.

The dual architecture, composed of a web-based interface and a native mobile application, makes this service particularly relevant

Table 4: Checklist results – Service #03 “Declarar meu Imposto de Renda - DIRPF”

ID	Category	Question (summary)	Score
1	QIF	Clearly declares the collection of personal data?	2
2	PF	Collects personal data as declared?	0
3	QIF	Clearly declares the collection of sensitive data?	2
4	PF	Collects sensitive data as declared?	0
5	QIF	Clearly declares the purpose of data collection?	2
6	PF	Applies purposes as declared?	2
7	QIF	Clearly declares collection of device/access data?	0
8	PF	Collects device/access data as declared?	1
9	QIF	Clearly declares data sharing practices?	0
10	PF	Shares data as declared?	1
11	QIF	Clearly declares data retention periods?	1
12	PF	Applies retention rules as declared?	2
13	QIF	Clearly declares international data transfer?	2
14	PF	Applies international transfer policy as declared?	2
15	AS	Declares responsible agency?	2
16	AS	Declares the DPO?	0
17	AS	Declares the privacy support channel?	0
18	AS	Provides direct access to privacy support?	0
19	AS	DPO contact easily found on agency site?	0
20	AS	DPO contact found via site search?	0
21	AS	Dedicated privacy support channel offered?	0
		Overall Score	**45.24%**
		Declared Information Quality (QID)	64.29%
		Factual Precision (PF)	57.14%
		Accessibility Support (AS)	14.29%

Table 5: Checklist results – Service #04 “Meu INSS”

ID	Category	Question (summary)	Score
1	QIF	Clearly declares the collection of personal data?	1
2	PF	Collects personal data as declared?	2
3	QIF	Clearly declares the collection of sensitive data?	0
4	PF	Collects sensitive data as declared?	2
5	QIF	Clearly declares the purpose of data collection?	1
6	PF	Applies purposes as declared?	2
7	QIF	Clearly declares collection of device/access data?	1
8	PF	Collects device/access data as declared?	2
9	QIF	Clearly declares data sharing practices?	1
10	PF	Shares data as declared?	2
11	QIF	Clearly declares data retention periods?	1
12	PF	Applies retention rules as declared?	2
13	QIF	Clearly declares international data transfer?	0
14	PF	Applies international transfer policy as declared?	1
15	AS	Declares responsible agency?	2
16	AS	Declares the DPO?	0
17	AS	Declares the privacy support channel?	0
18	AS	Provides direct access to privacy support?	0
19	AS	DPO contact easily found on agency site?	2
20	AS	DPO contact found via site search?	0
21	AS	Dedicated privacy support channel offered?	0
		Overall Score	**52.38%**
		Declared Information Quality (QID)	35.71%
		Factual Precision (PF)	92.86%
		Accessibility Support (AS)	28.57%

to privacy and security studies. Due to the integration with private financial institutions and government bodies, the complexity of its data processing and information sharing mechanisms requires special attention. Catalog link: https://www.gov.br/pt-br/servicos/comunicar-roubo-furto-de-aparelho-pelo-aplicativo-celular-seguro. Direct access: https://celularseguro.mj.gov.br/. The “Celular Seguro BR” service reveals a combination of promising operational transparency and important gaps in privacy communication. The following insights and recommendations are drawn from a detailed inspection:

- **Inconsistent naming and catalog structure:** The service appears under multiple titles such as “Celular Seguro” and “Comunicar roubo/furto de aparelho pelo aplicativo Celular Seguro” in the *gov.br* catalog. Additionally, the term “Celular Seguro” refers both to the service and the mobile app. This ambiguity may confuse users, especially those less familiar with digital platforms.
- **Access to privacy documentation:** While the mobile application presents terms of use and privacy policies, these are lengthy, presented in small font, and not available for download or offline review. After initial acceptance, the same limitations persist within the application.
- **High degree of factual adherence:** The service demonstrates strong alignment between declared and practiced data operations. This is particularly notable in the areas of retention, sensitive data handling, and international data transfer.
- **Low visibility of privacy governance:** Despite being a service that integrates with financial and telecommunications entities, no publicly accessible Data Protection Officer (DPO)

Table 6: Checklist Evaluation – Service #05: "Celular Seguro BR"

ID	Category	Evaluation Question	Score
1	QID	Clearly declares the collection of personal data?	1
2	PF	Collects personal data as declared?	2
3	QID	Clearly declares the collection of sensitive personal data?	1
4	PF	Collects sensitive personal data as declared?	2
5	QID	Clearly states the purpose for data collection?	1
6	PF	Applies declared purposes in practice?	2
7	QID	Clearly declares the collection of device information?	0
8	PF	Collects device and access information as declared?	1
9	QID	Clearly declares data sharing practices?	1
10	PF	Shares data as declared?	1
11	QID	Clearly declares data retention periods?	2
12	PF	Applies retention rules in practice?	2
13	QID	Clearly declares international data transfers?	1
14	PF	Applies international transfer rules in practice?	2
15	AS	Declares the responsible agency?	2
16	AS	Declares the Data Protection Officer (DPO)?	0
17	AS	Declares the privacy support channel?	0
18	AS	Provides direct access to privacy support?	0
19	AS	Is the DPO information easily found on the agency website?	0
20	AS	Is the DPO information easily found via site search?	0
21	AS	Does the agency website provide a dedicated privacy support channel?	0
		Overall Score	**50.00%**
		Declared Information Quality (QID)	50.00%
		Factual Precision (PF)	85.71%
		Accessibility Support (AS)	14.29%

contact information could be located on the MJSP website or via search functions.

- **Lack of a dedicated privacy support channel:** There is no evident specialized support mechanism for data protection requests. This absence may hinder data subjects in exercising their LGPD rights effectively.
- **Recommendation for harmonization and transparency:** Greater standardization is needed in how service names, policies, and support information are presented across the gov.br portal, mobile platforms, and the institutional website. Offering downloadable privacy terms and highlighting contact points for privacy issues would improve user trust.

5 DISCUSSION

The analysis of the five selected digital public services revealed a significant variation in their compliance with transparency and data protection principles, as assessed using the proposed checklist. Overall scores ranged from 21.43% to 54.76%, with most services scoring between 45% and 55%. The lowest-scoring service was **Service #02 – "Realizar a Assinatura Eletrônica de Documentos"**, which received only 21.43%. This under-performance is primarily due to the complete absence of any declaration regarding the collection, processing, or sharing of personal data. Given the technical architecture involving document uploads and downloads—which likely entails handling sensitive user information—the lack of clear disclosures severely undermines the trustworthiness of the service.

By contrast, the highest score was achieved by **Service #01 – "Criar conta gov"**, with 54.76%. This service stood out for its broad declarations of data processing practices, which aligned well with the evaluation criteria. However, there remains room for improvement in the *Declared Information Quality (QID)* dimension, particularly in making privacy information more accessible, understandable, and centralized within the gov.br catalog page.

The average score for the **QID** category was 40.00%, indicating a widespread need for improvement. Many services lack clear, user-friendly explanations about the data they collect and how it is processed. Frequently, such information is either fragmented, embedded in overly technical or legalistic documents, or entirely absent from official service descriptions.

The **Factual Precision (PF)** dimension achieved the highest average score (77.14%), suggesting that the actual behavior of the services often aligns with expected practices. Nonetheless, this figure should be interpreted with caution. Our assessment was based solely on observable behaviors and publicly available documentation, without access to internal systems or technical audits. As such, the evaluation reflects what can be confirmed from a user-facing perspective, rather than a complete verification of backend processes. The most significant gap emerged in the **Accessibility of Specialized Support (AS)** dimension, which averaged only 20.00%. All five services exhibited limitations in providing accessible, dedicated channels for handling privacy-related inquiries. Recurrent issues include the absence of clearly identified Data Protection Officers (DPOs), reliance on generic support platforms such as *Fala.BR*, and the lack of specific mechanisms for addressing user rights requests under the LGPD.

Since most evaluated services rely on Fala.BR as a general-purpose communication channel with citizens, we identify a concrete opportunity to enhance its capabilities. We recommend the creation of dedicated categories and mechanisms within Fala.BR specifically for privacy and data protection requests, enabling automatic routing of these requests to the responsible DPO. This approach would standardize support processes without requiring each agency to implement separate support structures. During the evaluation process, we also identified inconsistencies between the information declared on the service pages within the gov.br catalog and that found on institutional websites or other dedicated service pages. Although our analysis prioritized the content published in the gov.br catalog, we emphasize that convergence and consistency across all communication channels are essential to ensuring service credibility and user trust.

We also see a valuable opportunity for the gov.br catalog itself to be revised to include objective, accessible, and user-oriented privacy information. Suggested improvements include: explicit disclosure of the DPO responsible for each service; direct links to specialized support mechanisms; and the adoption of clear, printable, and downloadable summaries of privacy terms using plain language, ideally timestamped to document the information version accessed by the user. Furthermore, service declarations should be comprehensive—not only stating which data is collected (positive declarations), but also clearly indicating which data is not collected (negative declarations). This is particularly important for sensitive categories such as device data, geolocation, biometric identifiers, cookies, and sensor information.

To provide a visual synthesis of these findings, Figure 2 presents a comparative analysis of all five services across the three evaluation dimensions. The blue bars (QID) highlight notable disparities in how privacy information is disclosed. The green bars (PF) reflect strong factual alignment in most services, with "Conta Gov" and "Meu INSS" leading this category. Meanwhile, the red bars (AS) reveal a systemic weakness in privacy-related user support, with all services scoring below 30%. This visualization reinforces our core conclusion: while operational compliance is often achieved, the lack of transparency and poor accessibility to specialized support continue to compromise the perceived trustworthiness of these services.

In summary, although some services demonstrated consistency between declared and actual data processing practices, transparency deficits and insufficient user support remain widespread. To improve public trust and ensure full compliance with the LGPD, services must prioritize more accessible, centralized, and user-friendly privacy communications, along with robust support mechanisms for citizens seeking to exercise their data protection rights.

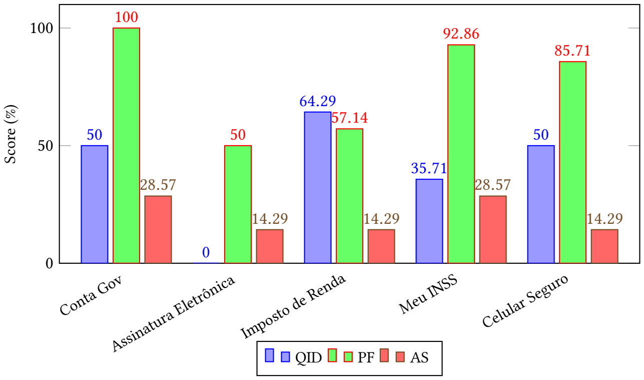


Figure 2: Comparison of scores by evaluation dimension (QID, PF, AS) across five Brazilian digital public services.

6 THREATS TO VALIDITY

As with any empirical investigation, this study is subject to some threats to validity that must be acknowledged. **Construct Validity:** The evaluation instrument was designed to assess compliance with privacy and data protection requirements based on publicly available information. However, the construct may not capture all dimensions of privacy governance, such as internal security policies, back-end data flows, or undocumented practices. Despite the use of a structured and piloted checklist, the inherent subjectivity in interpreting legal and declarative content may have influenced some scoring decisions. **Internal Validity:** The data collection and service inspections were conducted by two experienced researchers in privacy, digital services, and software quality. While this dual review minimizes individual bias and enhances the credibility of findings, the lack of automated tools or access to internal system logs limits the ability to fully verify the factual precision of some services.

External Validity: The sample includes five federal digital public services selected based on popularity and societal relevance. Although they represent a meaningful cross-section of the Brazilian digital government landscape, the results may not generalize to all public services or to services from other governmental levels (state or municipal). Future replications involving a broader set of services could increase the robustness and representativeness of findings. **Reliability:** Given the dynamic nature of digital public services and the continuous evolution of privacy policies and interfaces, it is possible that the information assessed may change over time. The evaluations reflect the status of the services at the time of analysis (July 2025). Regular updates or policy revisions might alter scores and require reanalysis in the future. Overall, the methodology employed—including a transparent checklist, clear scoring criteria, and dual independent assessments—supports the reliability and rigor of this exploratory study, while recognizing the need for continued refinement and validation.

7 CONCLUSION

This study proposed and applied a practical, checklist-based approach to evaluate the transparency and trustworthiness of digital public services in Brazil with respect to personal data processing. By examining five high-impact federal services, we assessed three key dimensions: the quality of information declared to users (QID), the alignment between declared and actual practices (PF), and the availability of specialized privacy support (AS).

The results reveal a moderate average level of compliance (44.76% overall), with the *Factual Precision* dimension scoring highest (77.14%) and *Support Accessibility* scoring lowest (20.00%). These findings suggest that while most services appear to operate in accordance with general privacy expectations, they lack transparency and adequate user support channels. In particular, deficiencies in clearly communicating data processing practices and identifying data protection officers limit the user's ability to understand and exercise their rights under the LGPD.

Services such as "Conta Gov" and "Meu INSS" demonstrated relatively stronger performance, while others, like "Assinatura Eletrônica", highlight the risks of omitting essential privacy declarations—especially when handling sensitive artifacts such as user documents. We recommend that public agencies invest in improving the accessibility and completeness of privacy disclosures within the official gov.br service catalog and across service entry points. Furthermore, the establishment of specialized, user-friendly support channels for privacy-related inquiries is critical to increasing public trust and legal compliance. Future work will involve expanding the service sample, refining the checklist based on stakeholder feedback, and exploring automated methods to support large-scale assessments. This research contributes toward the advancement of transparent, citizen-centered digital public services in alignment with the principles of data protection and software quality.

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.

REFERENCES

[1] Abdulrazaq Kayode AbdulKareem and Kazeem Adebayo Oladimeji. 2024. Cultivating the digital citizen: trust, digital literacy and e-government adoption. *Transforming Government: People, Process and Policy* 18, 2 (2024), 270–286.

[2] Basheer Al-haimi, Haliyana Khalid, Nor Hidayati Zakaria, and Tuti Haryati Jasimin. 2025. Digital transformation in the real estate industry: A systematic literature review of current technologies, benefits, and challenges. *Int. J. Inf. Manag. Data Insights* 5, 1 (2025), 100340. https://doi.org/10.1016/J.JJIMEI.2025.100340

[3] Juliano Nunes Alves, Luciana Flores Battistella, Eliete dos Reis Lehnhart, Kelmara Mendes Vieira, and Vinícius Costa da Silva Zonatto. 2025. Digital Public Service Quality (PS-DigQual): Proposal of a Multidimensional Framework. *Annual International Conference on Digital Government Research* 26 (Jun. 2025), 1–15. https://doi.org/10.59490/dgo.2025.1056

[4] Narek Andreasyan, Daniele Buson, José Mancera, Edy Portmann, and Luis Terán. 2025. Evaluation of Public Services Through the Lens of Digital Ethics. *Annual International Conference on Digital Government Research* 26 (Jun. 2025), 1–15. https://doi.org/10.59490/dgo.2025.1033

[5] Claire McKay Bowen. 2024. Government Data of the People, by the People, for the People: Navigating Citizen Privacy Concerns. *Journal of Economic Perspectives* 38, 2 (2024), 181–200.

[6] 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* 1 (2018), 1–23. http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm

[7] Molly Campbell, Ankur Barthwal, Sandhya Joshi, Austin Shouli, and Ajay Kumar Shrestha. 2025. Investigation of the privacy concerns in AI systems for young digital citizens: A comparative stakeholder analysis. In *2025 IEEE 15th Annual Computing and Communication Workshop and Conference (CCWC)*, Vol. 15. IEEE, 10.1109/CCWC62904.2025.10903925, 00030–00037.

[8] Marijn Janssen, Nripendra P Rana, Emma L Slade, and Yogesh K Dwivedi. 2021. Trustworthiness of digital government services: deriving a comprehensive theory through interpretive structural modelling. *Digital government and public management* 1 (2021), 15–39.

[9] Zoran Jordanoski and Morten Meyerhoff Nielsen. 2024. Comparative Study on the Digitalization of Specific Public Services Grouped by Life Events: The Case of Western Balkan and Eastern Partnership Countries. In *Proceedings of the 25th Annual International Conference on Digital Government Research, DGO 2024, Taipei, Taiwan, June 11-14, 2024*, Hsin-Chung Liao, David Duenas-Cid, Marie Anne Macadar, and Flavia Bernardini (Eds.). ACM, https://doi.org/10.1145/3657054.3657258, 453–462. https://doi.org/10.1145/3657054.3657258

[10] Jingrui Ju and Liuan Wang. 2025. The roles of trust and privacy calculus in citizen-centric services usage: evidence from the close contact query platform in China. *Behav. Inf. Technol.* 44, 3 (2025), 574–595. https://doi.org/10.1080/0144929X.2024.2330001

[11] Katrin Körner-Wyrtki, Christoph Buck, Anna Krombacher, and Maximilian Röglinger. 2024. Exploring success factors for developing citizen-centric digital public services - insights from a case study. *Electron. Gov. an Int. J.* 20, 5 (2024), 591–620. https://doi.org/10.1504/EG.2024.140777

[12] Xueping Liang and Yilin Xu. 2025. A novel framework to identify cybersecurity challenges and opportunities for organizational digital transformation in the cloud. *Comput. Secur.* 151 (2025), 104339. https://doi.org/10.1016/J.COSE.2025.104339

[13] Wander Cleber Maria Pereira da Silva, Edna Dias Canedo, George Marsicano Correa, Henrique Gomes de Moura, Paula Emilyn Deodato Franco, Giovanna Galvão Novaes Santana, and Rejane Maria da Costa Figueiredo. 2025. Fast Track for Collaborative Solutions: A Methodology for Public Service Design Workshops Supported by LLMs. *Annual International Conference on Digital Government Research* 26 (Jun. 2025), 1–15. https://doi.org/10.59490/dgo.2025.1061

[14] George Marsicano, Edna Dias Canedo, Glauco Vitor Pedrosa, Cristiane Soares Ramos, and Rejane M. da C. Figueiredo. 2024. Digital Transformation of Public Services in a Startup-Based Environment: Job Perceptions, Relationships, Potentialities and Restrictions. *J. Univers. Comput. Sci.* 30, 6 (2024), 720–757. https://doi.org/10.3897/JUCS.106979

[15] Maria Martins, Yuska Aguiar, and Juliana Saraiva. 2025. Assessment of Competences for LGPD DPO through ANPD Standard and Information Systems Curriculum. In *Anais do XXI Simpósio Brasileiro de Sistemas de Informação* (Recife/PE). SBC, Porto Alegre, RS, Brasil, 565–574. https://doi.org/10.5753/sbsi.2025.246585

[16] Aryely Matos, Mario Patrício, Maria Isabel Nicolau, Edna Dias Canedo, Juliana Alves Pereira, and Anderson Uchôa. 2025. Data Privacy in Software Practice: Brazilian Developers' Perspectives. *Journal of Internet Services and Applications* 16, 1 (Jun. 2025), 299–319. https://doi.org/10.5753/jisa.2025.5302

[17] Ghulam Mustafa, Waqas Rafiq, Naveed Jhamat, Zeeshan Arshad, and Farhana Aziz Rana. 2025. Blockchain-based governance models in e-government: a comprehensive framework for legal, technical, ethical and security considerations. *International Journal of Law and Management* 67, 1 (2025), 37–55.

[18] Glauco Vitor Pedrosa, Wander Cleber Maria Pereira da Silva, and Rejane Maria da Costa Figueiredo. 2025. EXPLORATORY STUDY OF QUALITY ATTRIBUTES IN BRAZILIAN DIGITAL PUBLIC SERVICES. *Environmental & Social Management Journal/Revista de Gestão Social e Ambiental* 19, 4 (2025), 1–20.

[19] Jidapa Preecha. 2025. Cybersecurity and Public Trust in Digital Governance: Focusing on Citizen Trust. In *Proceeding of International Conference on Social Science and Humanity*, Vol. 2. Antis International, https://doi.org/10.61796/icossh.v2i2.27, 26–37.

[20] MINISTÉRIO DA GESTÃO E DA INOVAÇÃO EM SERVIÇOS PÚBLICOS. 2024. PROGRAMA DE PRIVACIDADE E SEGURANÇA DA INFORMAÇÃO (PPSI), Versão 1.1.4. *PRESIDÊNCIA DA REPÚBLICA* 2 (2024), 1–178. https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/ppsi/guia_framework_psi.pdf

[21] Dimitrios Serpanos and Panayotis Antoniadis. 2025. Cyberphysical Systems in Control: Risks of Digital Transformation. *Computer* 58, 7 (2025), 161–164. https://doi.org/10.1109/MC.2025.3568303

[22] Stefano Spósito, Fernando Moreira, and Edna Canedo. 2025. 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* (Recife/PE). SBC, Porto Alegre, RS, Brasil, 95–104. https://doi.org/10.5753/sbsi.2025.246040

[23] Nida Türegün. 2025. Digital transformation and cybersecurity risks. *Int. J. Account. Inf. Syst.* 56 (2025), 100749. https://doi.org/10.1016/J.ACCINF.2025.100749

[24] European Union. 2018. General Data Protection Regulation (GDPR). *Intersoft Consulting, Accessed on October 24, 2019* 1, 1 (2018), 1–100. https://gdpr-info.eu/

[25] Elaine Venson, Rejane Maria da Costa Figueiredo, and Edna Dias Canedo. 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 (2024), 101943. https://doi.org/10.1016/J.GIQ.2024.101943

[26] Sose Raeinaldo Virnandes, Jun Shen, and Elena Vlahu-Gjorgievska. 2024. Building public trust through digital government transformation: A qualitative study of Indonesian civil service agency. *Procedia Computer Science* 234 (2024), 1183–1191.

[27] Sose Raeinaldo Virnandes, Jun Shen, and Elena Vlahu-Gjorgievska. 2025. Demystifying the Relationship between Digitalization of Government Services and Public Trust: A Scoping Review. *Digit. Gov.: Res. Pract.* 45 (Feb. 2025), 1–20. https://doi.org/10.1145/3716172 Just Accepted.

[28] Mingxi Zhou, Luning Liu, and Yuqiang Feng. 2025. Building citizen trust to enhance satisfaction in digital public services: the role of empathetic chatbot communication. *Behaviour & Information Technology* 1 (2025), 1–20.