RBPD
Revista Brasileira de Planejamento e Desenvolvimento
ISSN: 2317-2363

https://periodicos.utfpr.edu.br/rbpd

Technological migration and digital sovereignty in federative contexts: building a conceptual model

Bruno Gustavo Moreira de Brito
bruno.m.brito@caixa.gov.br
Instituto Federal do Acre. Rio Branco. Acre. Brasil.

Mario Sérgio Pedroza Lobão
mario.lobao@ifac.edu.br
Instituto Federal do Acre. Rio Branco. Acre. Brasil.

Sônia Marise Salles Carvalho
sonia.carvalho@unb.br
Universidade de Brasília. Brasília. Distrito Federal. Brasil.

Rodrigo Duarte Soliani
rodrigo.soliani@ifac.edu.br
Instituto Federal do Acre. Rio Branco. Acre. Brasil.

Renata Gomes de Abreu Freitas
renata.freitas@ifac.edu.br
Instituto Federal do Acre. Rio Branco. Acre. Brasil.

ABSTRACT

The growing dependence on technology providers in the public sector has intensified the debate on digital sovereignty and the need for national strategies of technological migration. This article examines international experiences in this field with the aim of proposing a conceptual model to foster digital autonomy in federal contexts such as Brazil. The study adopts a qualitative approach, grounded in a systematic literature review, documentary analysis, and multiple case studies of countries with high levels of digital maturity (Estonia, France, South Korea, and Canada). The comparative analysis revealed recurrent structural patterns, including the reuse of public software, the institutionalization of digital governance, the consolidation of interoperable infrastructures under state control, and the continuous training of civil servants. These elements, however, are shaped by specific political and administrative conditions that influence national strategies. Based on this evidence, a conceptual model was developed, structured around four interdependent dimensions (institutional, operational, normative, and sociotechnical), providing guidelines tailored to the Brazilian federative context. The findings contribute to strengthening public policies aimed at digital sovereignty, with particular emphasis on building lasting state capacities, enhancing federative coordination, and reducing dependence on external providers.

KEYWORDS: Technological Migration, Digital Sovereignty, Digital Government, Digital Transformation.

1 INTRODUCTION

Over the past two decades, the digitalization of public administration has ceased to be a distant promise and has become part of the daily routine of governments in different regions of the world. In many contexts, it has been conceived as a means to streamline processes and reduce costs; in others, as a response to the growing concern over dependence on foreign technology providers, which can limit state autonomy (LATUPEIRISSA et al., 2024). In this scenario, discussing technological migration goes beyond replacing proprietary software with open alternatives, it implies rethinking the role of the State in an environment of continuous and transnational connectivity (JANSEN et al., 2023).

The notion of digital sovereignty has gained prominence in this process of transition, driven by political disputes and strategic decisions concerning control over digital infrastructures. More than an emerging idea, it expresses a pursuit of technological autonomy, in other words, the preservation of data, systems, and essential competences under public control (POLIDO, 2024). Over time, this debate has expanded to include previously secondary dimensions, among them the development of sovereign artificial intelligences, designed to align technological innovation, social values, and national priorities (MÜGGE, 2024).

Technological migration, in this sense, is no longer a purely technical matter. It involves institutional revisions, governance reconfigurations, and new forms of mediation between the State and society (HAUG et al., 2024). International experiences show that there is no single path: the European Union tends to consolidate long-term strategies, while Asian countries opt for more immediate and adaptive responses (BOCEAN; VĂRZARU, 2023; CARVER, 2024). Despite this diversity, the concept of digital sovereignty continues to encompass multiple interpretations. It may refer to the State's regulatory authority, protection against external vulnerabilities (ROBERTS, 2024), or the formulation of cooperative models that integrate data openness, technological capacity-building, and networked governance (CIANCARINI et al., 2023). This variety of meanings reinforces that understanding the phenomenon requires an interdisciplinary perspective attentive to the historical and political particularities of each national context.

From a theoretical standpoint, there is no consensus. The modernization school associates digitalization with efficiency gains, transparency, and citizen participation (MILAKOVICH, 2021). Critical approaches, on the other hand, warn of the risks of technological power concentration and the erosion of national autonomy (VON SCHOMBERG, 2025). Institutional perspectives emphasize the importance of regulatory frameworks and organizational capacity, whereas sociotechnical readings highlight the interaction among technology, people, and culture (ALTHANI, 2025). In geopolitical terms, the European Union relies on regulation to preserve autonomy; the United States prioritizes market-driven innovation; and China strengthens state control over data and infrastructure (FRATINI et al., 2024; HULKÓ et al., 2025; YUN, 2025).

In the Brazilian case, although significant progress has been made in the digitalization of the public sector, there remains a lack of studies that systematically investigate the determinants of technological migration in federative arrangements (BARBIERI; SOTT, 2024; LATUPEIRISSA et al., 2024). Persistent barriers include dependence on foreign suppliers, budgetary constraints, and institutional asymmetries (LUI et al., 2025). It is worth noting that

the scarcity of theoretical models adapted to the national reality hinders the formulation of consistent strategies for digital autonomy. Another critical aspect is the predominance of global indicators poorly adjusted to local contexts, which underscores the need for context-specific diagnostics (IPEA, 2025).

Based on these references, this article examines international experiences of technological migration in the public sector, seeking to understand their motivations, strategies, challenges, and outcomes. From these findings, it develops a comparative analysis aimed at identifying governance patterns and drawing lessons useful for formulating policies that strengthen digital autonomy in Brazil, considering its institutional, economic, and federative particularities. Finally, it presents a conceptual model that articulates the main factors identified and outlines guidelines to orient sovereign technological migration processes in complex federative contexts.

The research was structured in two main stages. The first involved mapping and categorizing representative cases in developed countries, considering motivations, strategies, and obstacles across technical, organizational, and political dimensions. The second assessed the results in terms of digital sovereignty, administrative efficiency, and economic impacts, enabling the systematization of success factors with potential for adaptation to Brazil. The text is organized into five sections: introduction, methodology, analysis of results, guidelines for the national context, and final considerations.

2 METHODOLOGY

This research is characterized as applied, aimed at generating evidence to guide public policies for strengthening state digital autonomy. From the perspective of its objectives, it has an exploratory and descriptive nature and relies on a qualitative approach. The focus lies on the in-depth analysis of international experiences of technological migration in the public sector. Rather than pursuing statistical generalizations, the study seeks to understand complex phenomena in specific institutional contexts, with an emphasis on analytical inference (YIN, 2018).

To support the analytical process, three methodological strategies were employed: a systematic literature review (SLR), multiple case studies, and documentary analysis. The combination of these procedures sought to enhance the robustness of the findings and enable a dialogue between theoretical foundations and empirical evidence in the construction of the conceptual model.

2.1 SLR

The first stage consisted of conducting an SLR, following the procedure described by Carrera-Rivera et al. (2022), with the aim of gathering theoretical and empirical contributions relevant to the topic. The search covered the Web of Science, Scopus, SciELO, IEEE Xplore databases, and governmental repositories, with a temporal scope from 2020 to 2025. The search strategy employed Boolean operators and truncations, using descriptors such as “digital AND sovereignty AND government,” “technological migration AND government,” “digital transition AND

public sector," and "open source AND government AND digital transformation," among others.

Only studies that directly addressed government digital transformation, digital sovereignty, or technological migration experiences in the public sector were selected. The analysis encompassed scientific articles, technical reports from international organizations, and official documents that presented a clear and verifiable methodological foundation. Duplicates, incomplete materials, non-relevant languages, and sources outside the thematic scope or with excessively narrow coverage were excluded. These criteria were intended to ensure the relevance and comparability of the studies in relation to the central objectives of the research.

A total of 225 records were identified: Web of Science (26), Scopus (49), SciELO (57), IEEE Xplore (48), and governmental repositories (45). The initial screening excluded 88 works due to low thematic relevance (52), limited scope (24), language (12), or incomplete format (54). This left 137 studies, which were assessed based on titles and abstracts; 42 were then excluded for not being directly related to the study's objectives. In the end, 95 texts were read in full and 75 were incorporated into the references for presenting argumentative consistency, theoretical coherence, and methodological rigor. In addition to providing theoretical grounding, the SLR enabled the mapping of international experiences further explored in the documentary analysis.

2.2 Case study

The choice of a multiple case study approach, combined with documentary analysis, sought to reinforce the validity of the findings through source triangulation. This approach is recommended for contemporary phenomena where the boundaries between object and context are not clearly defined (KÄSS et al., 2024), as in the case of technological migration in government. The analytical replication logic inherent to this type of study allows each case to confirm or challenge inferences derived from others, contributing to the robustness of the results (ZANGIACOMI et al., 2020).

The selection of countries was based on their recent performance in the United Nations E-Government Development Index (EGDI) (UN, 2024), which measures digital maturity across three dimensions: online public services, telecommunications infrastructure, and digital human capital. Contexts with consolidated digital transformation strategies were prioritized to ensure the analysis of initiatives with institutional depth.

Two additional criteria guided the selection: (i) diversity of institutional models, to contrast different trajectories of digital sovereignty, and (ii) relevance of lessons for emerging countries with complex federative arrangements, such as Brazil. Thus, the sample comprised countries with recognized digital maturity but distinct governance structures, administrative centralization, and asset management approaches. This selection broadened the external validity of the research while highlighting the contextual limits of replication.

The final selection was based on qualitative criteria: the strategic relevance of the initiative for digital autonomy; national or large-scale implementation; alignment with the logic of technological migration; and availability of public

documentation. Following Yin's (2018) guidelines and recent studies on digital sovereignty (FRATINI et al., 2024), experimental cases without institutional continuity, subnational projects lacking national coordination, and insufficiently documented initiatives were excluded.

2.3 Data collection and analysis

Data collection was conducted using secondary sources, such as official documents, strategic plans, regulations, technical reports, and studies developed by international organizations, research centers, and public institutions. Priority was given to recent materials of proven relevance to the topic and recognized institutional legitimacy.

For the analytical phase, the content analysis technique described by Bardin (2016) was employed, organized into three stages: pre-analysis, material exploration, and interpretation. The initial reading, linked to the SLR results, enabled the identification of convergence axes among the cases examined. The data were systematized into four categories: (i) institutional motivations; (ii) implementation strategies; (iii) observed results; and (iv) challenges faced. This classification allowed for cross-case comparison, integrating technical, organizational, and political dimensions. Source triangulation contributed to strengthening internal validity, reducing potential biases, and increasing the reliability of the findings (VALENCIA, 2022).

2.4 Conceptual model construction

The conceptual model resulted from the systematization of recurring patterns identified across the analyzed cases. The aim was to propose a guide for national strategies of sovereign technological migration in federative arrangements. The process involved analytical inference and the consolidation of critical success factors, barriers, and documented practices.

The categories were reorganized into four interdependent dimensions—institutional, operational, normative, and sociotechnical, defined by the convergence between empirical findings and theoretical references from the SLR. The model is presented in graphical form, accompanied by guidelines that articulate governance levels and suggest pathways to strengthen digital sovereignty in Brazil.

It is worth noting that the research relied predominantly on secondary sources. Although triangulation contributed to increasing the consistency of the results, this approach may have limited access to operational aspects not documented in reports. During the manuscript preparation, the authors used the ChatGPT tool on a limited basis to assist in reviewing clarity and fluency. As Hosseini et al. (2024) emphasize, the use of artificial intelligence tools based on natural language processing in academic works requires transparency and critical review. All contributions from this stage were analyzed and adjusted, and the final version of the manuscript remains the sole responsibility of the authors.

3 RESULTS AND DISCUSSION

The EGDI 2024 (UN, 2024) remains one of the main references for assessing the digital maturity of governments on a global scale. The index is composed of three dimensions: online services, telecommunications infrastructure, and digital human capital. This framework makes it possible to observe not only technical performance but also the capacity of countries to incorporate digitalization as a state policy. Among the top-ranked nations, high levels of connectivity and digital services are consistently associated with solid institutional arrangements that ensure the continuity of public policies.

Across these experiences, certain patterns are recurrent: interoperability of digital infrastructures (OECD, 2025), continuous training of public servants (CHUNG et al., 2022), adoption of publicly controlled solutions (EC, 2023), and interministerial coordination that integrates strategies across different governmental levels (EC, 2024). These elements suggest that digital maturity cannot be reduced to technological innovation alone; it depends fundamentally on institutional articulation and policy continuity.

Countries that occupy leading positions in the digital agenda have followed distinct paths. In Denmark, the strategy has focused on building a digital government grounded in interoperability, connecting ministries, municipalities, and agencies through integrated platforms (DIGST, 2024). Estonia structured its policy around the national electronic identity (e-ID) and the X-Road platform, both associated with practices of software reuse and electronic voting (E-ESTONIA, 2020). These cases indicate that technical solutions achieve stability only when supported by long-term institutional arrangements.

In countries such as Singapore, the priorities follow a different logic: the adopted model is technocratic, supported by institutional autonomy and the intensive use of artificial intelligence in public services, underpinned by shared cloud infrastructure (GOVTECH, 2025). In South Korea, digitalization follows a decentralized logic, marked by the integration of administrative data and long-term strategic planning (MOIS, 2024). Finland, in turn, emphasizes transparency and automation, advancing toward so-called zero-touch services (FINNISH GOVERNMENT, 2022).

In the Anglophone world, the United Kingdom has advanced in the standardization of public Application Programming Interfaces (APIs) and consolidated its open data policy, reinforcing its leadership in transparency and interoperability (GOV.UK, 2024). France, on the other hand, invests in digital sovereignty through the reuse of public software and the Cloud au centre policy, which requires infrastructure certified by the SecNumCloud label for critical applications (EC, 2022a). Canada places particular emphasis on digital inclusion, with the Universal Broadband Fund aimed at expanding connectivity in rural, remote, and Indigenous communities (CANADA, 2025).

New Zealand provides a complementary example by adopting a decentralized digital identity system, accompanied by ethical guidelines for data use, supervised by the Data Ethics Advisory Group and supported by legal frameworks for privacy (DATA.GOVT.NZ, 2024). Germany, in turn, anchors its strategy in federative arrangements coordinated by the IT-Planungsrat, promotes the use of open-

source software through ZenDiS, and strengthens cybersecurity through certifications issued by the Federal Office for Information Security (BMI, 2024).

Table 1 presents the ten countries best ranked in the EGDI 2024, along with the best practices associated with their national strategies. An analysis of this set shows that, despite institutional differences, it is possible to identify patterns that contribute to the consolidation of digital maturity. These patterns will serve as reference points for the selection of cases discussed in the following section.

Table 1 – Top 10 Countries in the EGDI 2024 and Observed Best Practices

Country	EGDI 2024	Observed best practices
Denmark	0.9847	Full interoperability and integrated digital government across all public spheres.
Estonia	0.9727	Sovereign open-source infrastructure, national digital identity, and secure electronic voting.
Singapore	0.9691	Advanced use of artificial intelligence in public services and regional interoperability.
South Korea	0.9645	Universal digital education, centralized management of the state cloud, and widespread digitalization.
Finland	0.9632	Open governance focused on transparency, process automation, and citizen-centered services.
United Kingdom	0.9598	Open data platforms, mobile digital public services, and use of government APIs.
France	0.9564	Certified sovereign cloud and systematic reuse of open public code.
Canada	0.9543	Digital inclusion policies, accessibility, and digitalization of remote communities.
New Zealand	0.9517	Citizen-oriented public services with unified digital identity and ethical data management.
Germany	0.9486	Migration to open solutions, national security certification, and interoperable federative platforms.

Source: prepared by the authors (2025)

The comparison among the countries reveals that, although the adopted solutions follow different paths, certain pillars recur: interoperability, policy continuity, and control over critical infrastructures. These elements underpin the advancement of digital maturity and provide useful parameters for designing alternatives in federations such as Brazil. Thus, more than a simple inventory of experiences, the results highlight structural patterns that can guide, when adjusted to local conditions, technological migration strategies aimed at strengthening digital sovereignty.

3.1 Comparative analysis of national experiences

Building on the international trends presented earlier, the investigation proceeds with a multiple case study, conducted according to the logic of analytical replication proposed by Yin (2018). This strategy is particularly suitable for qualitative research that seeks to produce context-specific inferences, as it allows for the confrontation of contrasting experiences while simultaneously identifying shared patterns. Four countries were selected—enough to balance institutional diversity and analytical depth without losing the ability to observe, in detail, distinct technological migration strategies and extract structural elements applicable to the Brazilian federative context.

The choice of cases was not limited to their ranking in the EGDI 2024, although all belong to the group of the top ten countries. Additional criteria were considered, such as the availability of accessible public documentation, the diversity of institutional arrangements, and the strategic relevance to the study's objectives. Incorporating different political-administrative matrices (centralized, federative, technocratic, and liberal) broadened comparability among models and made it possible to highlight contextual factors with greater explanatory potential.

Not all countries with high index performance were included in the comparison. Denmark, although a global benchmark, developed its digital maturity based on a highly centralized model, not easily compatible with the Brazilian federative logic. In Singapore, vertical technocratic arrangements prevail, making adaptation to decentralized contexts difficult. Germany, despite its federative similarity, presented a shortage of English-language sources and a lack of consistent data regarding the reuse of public software.

Given these filters, the final sample focused on four countries: Estonia, France, South Korea, and Canada. Estonia has established itself as a global reference by integrating interoperability, electronic identity, and full digitalization of public services within a state architecture oriented toward digital sovereignty (E-ESTONIA, 2024). France combines a robust public infrastructure with regulatory frameworks that encourage technological reuse and maintain state control over digital assets (GOUVERNEMENT DE FRANCE, 2021). South Korea adopts a centralized strategy supported by intensive use of artificial intelligence and large-scale digital integration (CHEONG; CHO, 2024). Canada, in turn, offers a counterpoint: its federative experience is based on digital inclusion policies and coordination mechanisms among different levels of government (CANADA, 2021a).

This selection reveals diverse institutional trajectories and provides a foundation for understanding how each country structures its technological migration strategies and the results achieved. The analysis is organized into four dimensions: institutional motivations, implementation strategies, observed results, and persistent challenges.

3.1.1 Estonia

Estonia is often cited as one of the most striking examples of technological migration in the public sector and is internationally recognized as a benchmark in digital sovereignty (BUDNITSKY, 2022). After gaining independence in the 1990s, the country adopted digitalization as a central axis of its institutional reconstruction. This decision addressed both the need to overcome budgetary constraints and weaknesses inherited from the Soviet period, as well as the goal of repositioning itself geopolitically as an autonomous and interoperable nation (ESPINOSA; PINO, 2024).

The implementation of the X-Road platform marked a turning point in this trajectory by connecting more than one thousand public and private systems, supporting around 1,700 digital services, and enabling over 50 million monthly queries (EC, 2018). The decentralized communication among ministries, municipalities, health agencies, financial institutions, and universities preserves the autonomy of repositories while ensuring integration through encryption

protocols, authentication, digital signatures, and log recording. These mechanisms guarantee the integrity, transparency, and sovereignty of information (E-ESTONIA, 2024).

The unique digital identity (e-ID), used by more than 98% of the population, constitutes another cornerstone, enabling remote access to services, legally valid digital signatures, and participation in decision-making processes (E-ESTONIA, 2020). Since 2021, the country has formalized the adoption of open-source solutions by requiring that systems funded with public resources be made available under OSS licenses, in accordance with the Digital Agenda 2030 (ESTONIA, 2021). Public institutions are also encouraged to reuse interoperable components gathered in the Koodivaramu repository, known as Govstack modules (OPENFORUM EUROPE, 2025). This strategy is complemented by continuous investment in digital training. The Digital State Academy offers professional development programs for civil servants, while lifelong learning initiatives such as Look@World expand the digital skills of the general population (E-ESTONIA, 2023).

The results achieved by Estonia are remarkable: currently, 99% of public services are available online, contributing to lower operational costs and increasing public satisfaction to 83% (OECD, 2023). It is no coincidence that the Estonian model has been exported and adapted by various countries, consolidating itself as an example of digital sovereignty associated with efficiency and transparency.

Despite large-scale digitalization, the need to comply with European Union regulations such as the General Data Protection Regulation (GDPR) has created tensions between digital expansion and privacy protection. According to the European Interoperability Framework (EIF), Estonia performs below the European average in indicators of security and data protection, revealing weaknesses in the provision of interoperable services (EC, 2022b).

Cybersecurity remains a critical issue, as approximately 40% of electronic public services still operate on legacy software, although the national strategy aims to reduce this dependency to 20% by 2030. The rapid obsolescence of cryptographic algorithms reinforces the need for continuous updates to digital infrastructures and the development of quantum-resistant security solutions. In this context, a national center of competence in cryptography is being established, aimed at strengthening technical capabilities and evaluating quantum security solutions by 2027 (ESTONIA, 2024).

3.1.2 France

The French experience in technological migration is directly linked to the construction of a digital sovereignty strategy, guided by the protection of sensitive data, autonomy over critical infrastructures, and the reduction of dependence on foreign platforms (Blancato, 2024). In 2017, Decree No. 2017-1584 created the Direction Interministérielle du Numérique (DINUM), under the authority of the Prime Minister, tasked with coordinating the digital transformation of the central administration (FRANCE, 2017). Since then, DINUM has consolidated itself as the main governance body of France's digital agenda, working in coordination with the country's decision-making institutions.

Among the institutional motivations, digitalization has been interpreted as a mechanism for reaffirming state authority in the face of geopolitical risks

associated with the dominance of large technology corporations. As Fischer (2022) observes, the intensification of data protection litigation and the extraterritorial effects of commercial legislation have strengthened the perception of institutional vulnerability, encouraging the development of structured digital sovereignty policies.

In France, digital transformation has been organized along three main axes. The first is the Cloud de Confiance, which establishes technical, legal, and operational requirements for the use of cloud services by public bodies and ensures legal sovereignty over processed data. Only providers certified by SecNumCloud are authorized to operate in this environment, which prevents the enforcement of foreign legislation (EC, 2022a). The second axis is the public software reuse policy, centralized in the repository code.gouv.fr, which gathers solutions developed by state institutions and promotes cooperation among technical teams. The third concerns interoperability regulation, expanding integration between central and local administrations (EC, 2024).

The results of these initiatives have become evident on several fronts. In terms of transparency, the publication of public contracts and the work of the Observatoire Numérique maintained by DINUM are particularly significant, as the observatory is responsible for publishing indicators and evaluations of more than 250 digital services. In 2022, France achieved the highest score for the transparency principle in the EIF Scoreboard (EC, 2022a). From a legal standpoint, the Cloud de Confiance doctrine consolidated a national infrastructure dedicated to handling sensitive data under state control. Also in 2022, according to the OECD's Digital Government Index, the country scored 0.76 and ranked among the top three, with strong performance in open data, interoperability, and citizen-centered governance (OECD, 2025).

In the software domain, the reuse of solutions among ministries contributed to technological standardization and strengthened interministerial cooperation, in alignment with DINUM's OSS Action Plan (EC, 2023). The French experience has also extended beyond national borders, influencing regional initiatives such as Gaia-X, launched in 2019 in partnership with Germany, aimed at building a sovereign European cloud. In 2020, EuroCloud Europe introduced the European Sovereign Cloud Guidelines, which incorporated elements of the French model and expanded its influence on regulations and corporate practices (PANNIER, 2021).

Despite consistent progress, France has shown notable limitations. In the 2022 EIF Scoreboard, its performance was lower in specific recommendations, especially Recommendation 23, which evaluates the use of standard catalogs by ministries (EC, 2022a; OECD, 2025). Additionally, a shortage of specialized professionals in the public sector, exacerbated by competition with the private sector, has constrained large-scale implementation capacity (FRANCE, 2023). Even so, the country continues to advance in consolidating a model of digital governance grounded in sovereignty, technological reuse, and public infrastructure, with growing influence across the European landscape.

3.1.3 South Korea

In South Korea, the digital transformation of the public sector has been consolidated as a long-term national project, supported by a technocratic and centralized approach. In a coordinated manner, this strategy seeks to enhance economic competitiveness, modernize public administration, and ensure greater information security (CHUNG et al., 2022). The process combines continuous planning, consistent investment in infrastructure, and intensive use of emerging Technologies, such as AI, big data, and automation, resulting in a broadly integrated digital ecosystem (CHEONG; CHO, 2024).

The institutional motivations driving this model converge on three main objectives: improving administrative efficiency, strengthening digital resilience, and enhancing the government's capacity for anticipation in public policy formulation (CHEONG; CHO, 2024). These axes shape the Digital Government Master Plan 2021–2025, developed by the Ministry of the Interior and Safety (MOIS). The plan highlights priority areas such as AI-driven intelligent services, data-oriented public management, and the expansion of digital infrastructure (MOIS, 2021). Political coordination is overseen by the MOIS, while technical implementation is carried out by the National Information Society Agency (NIA, 2025).

Constant exposure to threats from North Korea and the recurrence of cyberattacks have made the regional geopolitical context a key factor in shaping strategic decisions, leading the country to treat digitalization and technological sovereignty as dimensions of national security (CSIS, 2024). In this environment, the government has adopted an offensive digital defense posture (defend forward), aimed at protecting critical assets and institutional resilience. Among the initiatives, the G4C (Government for Citizens) system stands out, as it connects more than 800 databases from different agencies and provides approximately 5,000 services, including the online issuance of 2,800 certificates (MOIS, 2024). The plan also includes digital certificates, the MyData system, and authentication solutions based on blockchain and the Internet of Things, applied to process automation and proactive public services (CSIS, 2024).

One of the highlights is K Cloud, a national cloud platform for the public sector developed using domestically produced artificial intelligence chips. The initiative strengthens state control over hardware, software, and services, while establishing strict security standards (MSIT, 2025). In another front, the Smart Government Academy has invested in the training of civil servants and in disseminating innovative public management practices (CHUNG et al., 2022).

According to the United Nations (UN, 2024), South Korea ranks among the countries with the highest levels of digital maturity in the public sector, showing satisfaction rates above 98% for public services, evidence of the remarkable results achieved. Automation in government procurement has generated estimated annual savings of USD 8 billion. In the OECD Digital Government Index 2023, the country leads in dimensions such as data-driven government and the provision of digital services as platforms (OECD, 2024). Beyond domestic achievements, South Korea has become an exporter of digital government expertise. The NIA coordinates projects in 46 countries involving artificial intelligence and digital inclusion, while the National Human Resources Development Institute (NHI) has

trained more than 5,000 civil servants from 125 countries since 1984 (NIA, 2024; MPM, 2024).

Although South Korea has made consistent progress, structural challenges persist. Centralization limits the autonomy of local governments, and the accelerated adoption of sensitive Technologies, such as facial recognition for public security and AI-based crime prediction systems, still lacks specific regulation, even after the approval of the AI Basic Act (LEE et al., 2025). Added to this is the influence of chaebols, family-run conglomerates whose economic and political weight shapes strategic sectors and, to some extent, determines the pace of innovation. This concentration raises concerns about the plurality of digital governance and limits the diversification of the innovation ecosystem (KIM et al., 2021). Despite these tensions, South Korea's trajectory demonstrates not only the strength of its institutional arrangements and technical capacity but also its ongoing effort to balance efficiency and digital sovereignty within an evolving regulatory environment.

3.1.4 Canada

The Canadian experience with technological migration stands out for reconciling the federal logic with an inclusive orientation based on the principles of accessibility, openness, and collaboration (MCMAHON, 2020). Unlike the more centralized models of South Korea and Estonia, digital transformation in Canada follows a decentralized format, in which national guidelines establish general parameters, and implementation occurs in a coordinated manner among the federal government, provinces, territories, and local communities.

The institutional motivations behind this agenda revolve around three main axes: improving administrative efficiency, ensuring equity in access to services, and recognizing territorial diversity as an essential component of governance (PBO, 2023). The COVID-19 pandemic reinforced this orientation by highlighting the need to extend the digital state to historically excluded populations and remote regions (CANADA, 2020a). Political coordination is the responsibility of the Treasury Board of Canada Secretariat (TBS), through the Office of the Chief Information Officer (OCIO). The Canadian Digital Service (CDS), created in 2017 and inspired by the U.S. 18F initiative, supports ministries and agencies in developing user-centered digital services (PBO, 2023).

Federal digital guidelines in Canada are shaped by open-source practices, system reuse, and user-centered design. These principles were consolidated in the Digital Standards policy, which emphasizes empathy, experimentation, interoperability, and transparency (CANADA, 2021a). In line with the Open First strategy, the presence of open standards in public software procurement has been expanded. Intergovernmental cooperation is facilitated by instruments such as the Pan-Canadian Trust Framework (PCTF), focused on the interoperability of digital identities, and the Public Sector CIO Council, a forum that brings together leaders from provinces, territories, and the federal government to coordinate data-sharing and technology initiatives (CANADA, 2024).

In Canada, the digital transformation agenda has already produced measurable results on multiple fronts. Notable examples include the expansion of access to digital services for Indigenous peoples, immigrants, and residents of

remote regions, as ensured by the Accessible Canada Act (CANADA, 2022). Another important result is the improved alignment among federal, provincial, and territorial services, which has reduced overlap and advanced standardization, driven by the Policy on Service and Digital and the CIO Council (CANADA, 2021b). As a result of these efforts, the country has consolidated itself as a reference in inclusive digital governance, ranks highly in OECD indexes, and participates actively in multilateral forums such as Digital Nations (OECD, 2025).

Coordination among levels of government remains a challenge, given the constitutional autonomy of provinces and territories (NRCAN, 2024). The uneven pace of technological adoption deepens regional disparities, and the lack of common metrics makes it difficult to assess results in an integrated way (CAPI, 2025). Added to this is the absence of a state-owned infrastructure, such as a sovereign cloud, which maintains dependency on private suppliers in sensitive areas (CANADA, 2020b). Even so, the Canadian trajectory shows that federal arrangements can evolve inclusively when supported by the principles of accessibility, cooperation, and interoperability.

Table 2 – Comparative summary of national experiences in governmental technological migration

Country	Institutional motivations	Strategies adopted	Observed results	Challenges faced
Estonia	Post-independence institutional reconstruction; overcoming administrative restrictions	X-Road platform; unique digital identity; reuse of public software; advanced interoperability; large-scale digital training	99% of public services digitized; cost reduction; increased social trust; international benchmark	Data privacy; European regulation (GDPR); cybersecurity weaknesses
France	Reducing dependence on big tech; legal protection of sensitive data	Cloud de Confiance; public software repository (code.gouv.fr); interoperability guidelines; regulatory governance	National digital infrastructure under state control; contractual transparency; influence on European initiatives	Institutional fragmentation; shortage of technical professionals; regulatory complexity
South Korea	State resilience; strategic use of AI and big data	G4C system; national public cloud; massive data integration; AI-based services; continuous training of civil servants	High citizen satisfaction; operational efficiency; institutionalization of data-driven government; export of digital expertise	Rigid centralization; ethical dilemmas in AI use; excessive influence of private conglomerates
Canada	Digital inclusion; federative coordination; responsive modernization	Open-source code and intergovernmental reuse; open standards; user-centered design; collaborative bodies; accessibility as a principle	Expanded access in remote areas; inclusion of vulnerable populations; rationalization of federative solutions	Asymmetries in adoption among provinces; absence of a unified national infrastructure; lack of standardized indicators

Source: prepared by the authors (2025).

The comparison shows that, despite institutional and cultural differences among the countries analyzed, certain core elements recur consistently. Three aspects are particularly relevant: (i) the consolidation of digital governance as a long-term public policy; (ii) the development of technological infrastructures under state control; and (iii) the strengthening of internal capacities through the

continuous training of public servants. In all cases, technological migration appears integrated into national projects aimed at modernizing the State and reducing vulnerabilities associated with dependence on external suppliers.

Across the four countries, institutional differences prove decisive, even though some convergences can be observed. Estonia and South Korea operate under centralized models that favor system standardization and integration but limit organizational autonomy. France and Canada, in turn, adopt decentralized arrangements supported by regulation, public software reuse, and intergovernmental coordination mechanisms. Motivations also vary: while Estonia and France link their strategies to the strengthening of digital sovereignty, South Korea and Canada prioritize administrative efficiency, social inclusion, and the State's responsiveness.

At the strategic level, similar practices reappear in distinct contexts, such as interoperability, public software reuse, sovereign clouds, and open data policies. These elements, institutionalized to varying degrees, constitute a shared repertoire of digital modernization. Among the main challenges are the shortage of qualified professionals, program fragmentation, and ethical dilemmas related to the use of emerging technologies (SOLIANI et al., 2025).

In summary, the evidence indicates that technological migration goes beyond infrastructure deployment or rule-making: it requires an institutional architecture capable of coordinating multiple actors and sustaining continuous innovation processes. Following this analysis, the next section focuses on Brazil, examining how the proposed conceptual model can be critically applied to the specific federal, institutional, and socioeconomic context of the country.

3.2 Brazil as a reference for model application

Although Brazil is not part of the main set of cases analyzed, it is considered in this study as a target country for applying the proposed conceptual model. The intention is to relate the international findings to the institutional, normative, and operational conditions that shape the digital transformation of the national public sector. In recent years, the country has made significant progress in providing digital services and, in the 2024 EGDI, reached the 29th global position, with a score of 0.90 in the online services dimension (UN, 2024). These results, however, are concentrated mainly at the federal level, particularly on the Gov.br Platform, with less intensity at the state and municipal levels.

The consolidation of an integrated national strategy still faces challenges arising from limited federal coordination and the fragmentation of digital initiatives (OECD, 2020). Although Decree No. 12.069/2024 established the National Digital Government Strategy and the GOV.BR Network, with the goal of strengthening cooperation among the Union, states, and municipalities, institutional asymmetries persist, compromising the coherence of public policies. Strengthening intergovernmental bodies with defined functions, technical capacity, and independent budgets is essential to ensure the continuity and convergence of actions across the national territory (BRAZIL, 2024). Permanent technical and political forums with multisectoral participation can contribute to articulating the different levels of government and enhancing the legitimacy of public decisions.

Among the most relevant normative advances are the Brazilian Strategy for Digital Transformation (MCTIC, 2018) and Law No. 14.129/2021 (BRAZIL, 2021), known as the Digital Government Law, which introduced principles such as interoperability, transparency, citizen-centered focus, and data-driven governance. The challenge, however, lies in consolidating a federative body capable of inducing, standardizing, and monitoring in an integrated way the actions undertaken by different governmental entities. The OECD (2020) recommends the institutionalization of permanent coordination mechanisms, with dedicated budgets and alignment between digital policies and regional development strategies. Without this institutional redesign, there is a risk of discontinuity and widening of territorial inequalities in access to public innovation.

The evidence gathered suggests the feasibility of a conceptual model adapted to Brazilian specificities. Built upon a critical reading of international experiences, the proposed model seeks to guide technological migration policies that strengthen digital sovereignty within a complex federative context such as Brazil's.

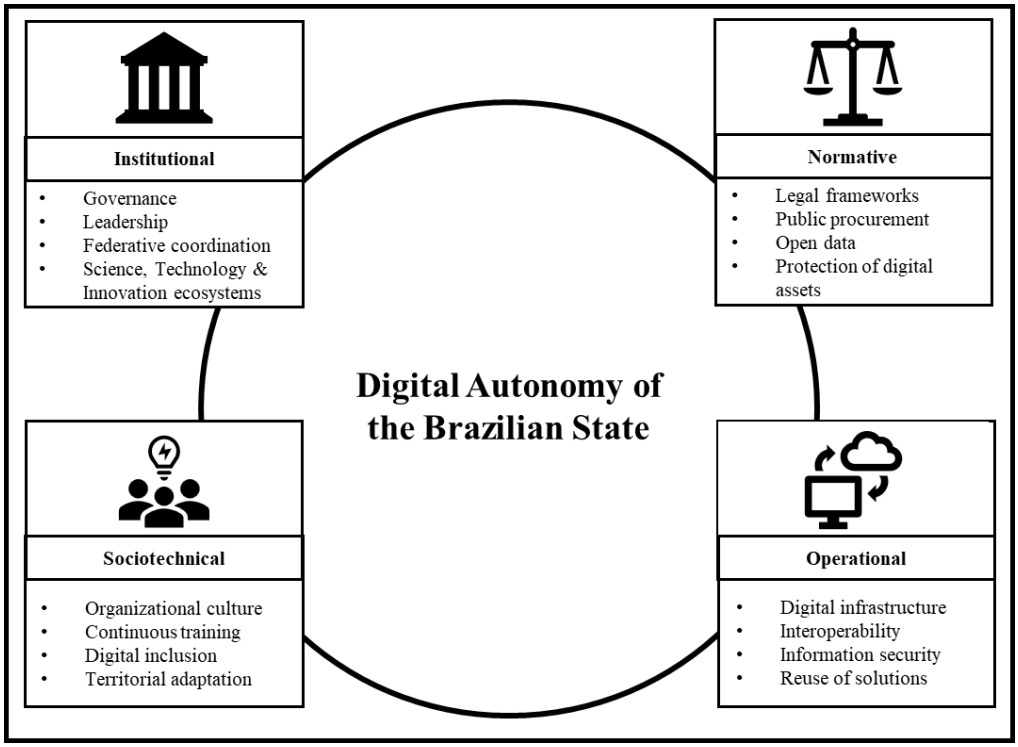
3.3 Conceptual model proposal for sovereign technological migration

Based on the empirical evidence gathered, this study proposes a conceptual model designed to guide sovereign technological migration processes in federative contexts. The international comparison revealed recurring practices, consolidated patterns, and specific contextual conditions that shape the performance of national strategies. In the Brazilian case, these elements provide a foundation for developing guidelines compatible with its institutional, technical, and federative conditions.

The model was conceived as an analytical instrument to support the formulation of public policies aimed at strengthening the State's digital autonomy. From this perspective, technological migration goes beyond simply replacing proprietary systems with open alternatives: it involves reorganizing institutions, revising operational processes, defining regulatory frameworks, and developing human competencies. It is a gradual process, sustained by consistent planning and coordination among multiple actors.

Based on the empirical categories identified in the comparative analysis, the findings were reorganized into four interdependent dimensions: institutional, operational, normative, and sociotechnical. These dimensions integrate the factors observed in international experiences and structure the proposed conceptual model. Figure 1 presents a graphical synthesis of these interrelations.

Figure 1 – Conceptual model for sovereign technological migration in federative contexts



Source: prepared by the authors (2025).

At the institutional level, technological migration depends on organizational arrangements and governance mechanisms capable of consolidating it as a State policy. Factors such as technical capacity, federative coordination, and decision-making legitimacy are key determinants (OECD, 2020). For these elements to gain consistency, it is necessary to define political and technical leadership, integrate different administrative entities, and connect digital policies with science, technology, and innovation ecosystems. Only under these conditions can isolated initiatives gain continuity.

The international experience illustrates this process: in Canada, collaborative bodies ensure coherence even in a context of subnational autonomy (CANADA, 2021a); in France, structures such as DINUM centralize coordination and establish national standards (EC, 2022a). In Brazil, a context marked by fragmented decision-making and institutional asymmetries, it becomes essential to strengthen intergovernmental bodies with their own budgets and to create permanent forums with multisectoral representation.

From an operational perspective, the challenge lies in translating guidelines into practice. This involves public management of digital infrastructure, open interoperability standards, data protection, digital asset management, and software reuse. International experiences demonstrate that success depends on the State's capacity to design and maintain its own systems, automate processes securely, and invest in staff training (MOIS, 2021; CHEONG; CHO, 2024; E-ESTONIA, 2024).

In Brazil, where systemic fragmentation and low coordination persist, three priority fronts emerge: developing interoperable platforms that integrate administrative data across all levels of government; implementing state-controlled

cloud environments to ensure technological autonomy; and institutionalizing reuse mechanisms supported by legal security, financial sustainability, and administrative rationality. Initiatives such as Estonia's X-Road and South Korea's public clouds demonstrate the feasibility of this approach.

The normative dimension encompasses the set of legal and regulatory instruments that support technological migration and ensure alignment with the principles of digital sovereignty (BRAZIL, 2021). This includes public procurement rules, open data policies, protection of sensitive information, and incentives for auditable solutions in trusted environments. Comparative experiences show that regulatory clarity strengthens institutional security.

France, for instance, consolidated the code.gouv.fr repository as the official platform for software reuse, supported by regulations on sovereign clouds, open licensing, and interoperability. In Canada, mandatory standards for accessibility and interoperability were established in its digital transformation policy, prioritizing open and auditable solutions. In Brazil, however, the decentralized procurement of proprietary systems and the absence of specific guidelines hinder coordination, reinforcing the need for national regulations that institutionalize reuse, prioritize open software, protect sensitive data, and ensure algorithmic transparency in public administration.

Finally, the sociotechnical dimension encompasses the human, organizational, and cultural factors that determine both the acceptance and sustainability of digital strategies. Unlike the operational dimension, which focuses on technical execution, this one emphasizes the ability of individuals and institutions to integrate innovations into their daily routines. Organizational culture, staff qualification, digital inclusion of the population, and territorial adaptation of solutions are central elements (CANADA, 2022; CHUNG et al., 2022).

The analyzed national experiences reveal distinct paths. Canada has invested in mandatory digital inclusion, reaching Indigenous and immigrant populations, while South Korea has focused on the large-scale training of public servants, fostering the State's capacity to absorb innovations. In Brazil, overcoming sociocultural barriers, access inequalities, and disparities in training is essential. Accordingly, the model proposes continuous education programs, the promotion of an innovative institutional culture, and territorially adapted strategies that respect federative diversity.

An integrated reading of these four dimensions shows that technological migration cannot be reduced to a set of isolated projects. It is a process that demands political, technical, regulatory, and cultural coordination, involving multiple actors in a continuous effort toward innovation. The model should be understood less as a prescriptive roadmap and more as an analytical tool to support strategic decision-making in unequal federative contexts. By systematizing critical factors observed in international experiences and adapting them to the Brazilian case, this study seeks to provide robust inputs for public policies aimed at strengthening the digital sovereignty of the State.

3.4 National strategies for technological migration in Brazil

Based on the analytical dimensions of the conceptual model constructed from international experiences, recommendations were developed and adapted to the Brazilian context. The proposal seeks to guide public policies for sovereign technological migration, taking into account the federal pact, the disparities among subnational entities, and the existing legal frameworks.

These recommendations are organized into four strategic axes corresponding to the institutional, operational, normative, and sociotechnical dimensions, each aimed at strengthening the State's long-term capabilities. Table 3 presents a summary of these axes, their conceptual linkage, and main objectives.

Table 3 – Strategic axes for sovereign technological migration in Brazil

Strategic axis	Associated dimension	Central objective
Federative governance of digital transformation	Institutional	Establish multisectoral coordination and federative alignment
Public and interoperable digital infrastructure	Operational	Consolidate technological structures under state control
Normative frameworks for digital sovereignty	Normative	Establish legal and technical support for open solutions
Technical and cultural capacities	Sociotechnical	Strengthen human competencies and ensure social adherence

Source: prepared by the authors (2025).

The federative governance axis, aligned with the institutional dimension, proposes the creation of permanent coordination structures with balanced participation of the federal government, states, and municipalities (CANADA, 2021b; PBO, 2023). These bodies would be responsible for deliberating on national digital strategies, ensuring political alignment, administrative stability, and federative cooperation. It is also recommended to promote public consortia aimed at developing joint solutions, reusing existing systems, and optimizing investments (CANADA, 2020a; EC, 2023). Integration with universities, research centers, and funding agencies adds technical and scientific depth, an essential factor for strengthening state planning (MARITAN et al., 2024).

The public and interoperable digital infrastructure axis, corresponding to the operational dimension, emphasizes the need to consolidate technological bases under state management, ensuring security and autonomy in handling sensitive data. Priority actions include the development of public cloud platforms managed by government agencies and the establishment of national interoperability standards (MOIS, 2021; E-ESTONIA, 2024; NIA, 2025). It is further recommended to create official repositories of reusable solutions and to institutionalize technology reuse policies, thereby reducing costs and dependency on private suppliers.

The regulatory framework axis, aligned with the normative dimension, aims to consolidate a regulatory environment consistent with the principles of digital sovereignty. In this regard, it is essential to define technical and legal criteria for the procurement of digital solutions, prioritizing open, auditable, and publicly funded software (CANADA, 2021a; EC, 2022a; FRANCE, 2023). It is also recommended to expand source code sharing, make applications available in

public repositories, strengthen algorithmic governance, and enhance cybersecurity policies. Updating existing legislation, such as the Digital Government Law (Brazil, 2021) and the General Law on the Protection of Personal Data (BRAZIL, 2018), both inspired by international best practices, can provide greater regulatory solidity, reduce institutional vulnerabilities, and foster convergence between technical and legal governance.

The technical and cultural capacities axis, linked to the sociotechnical dimension, highlights that digital transformation requires not only adequate infrastructure but also institutions and professionals prepared to operate it. From this perspective, continuous training of public sector teams plays a central role and reinforces the importance of expanding programs for developing digital competencies focused on interoperability, data management, information security, accessibility, and the ethical use of emerging technologies (CANADA, 2022; CHUNG et al., 2022; NIA, 2024). This effort should be complemented by the creation of specific career plans for technology professionals, accompanied by incentives to reduce turnover and attract new talent to the public sector. Another important front involves establishing national metrics of digital maturity, applied periodically to guide consistent diagnostics and support continuous cycles of institutional improvement (CANADA, 2021b; OECD, 2024).

When considered together, these four axes form an integrated agenda capable of enhancing the Brazilian State's capacity to conduct its technological migration processes in a sovereign manner. By aligning institutional, operational, normative, and sociotechnical dimensions, these strategies translate international evidence into practical guidelines adapted to the national context, helping to consolidate a public project of digital transformation grounded in state-owned infrastructure, democratic governance, legal security, and the continuous development of public competencies.

4 FINAL CONSIDERATIONS

This article examined international experiences of technological migration in the public sector with the aim of proposing a conceptual model oriented toward building digital sovereignty in federative contexts such as Brazil's. Digital transformation was understood not as the simple adoption of tools but as a process that requires the reorganization of state capacities, supported by institutional coordination, publicly managed infrastructure, clear regulatory frameworks, and continuous civil service training.

In the cases of Estonia, France, South Korea, and Canada, recurring elements were identified—such as the strengthening of digital governance, the development of interoperable infrastructures, the reuse of public solutions, and permanent capacity building—although these are embedded in distinct administrative and cultural contexts. The combination of these factors varies according to each country's degree of political centralization, regulatory traditions, and strategic objectives. Together, these experiences offer valuable references for shaping public policies in complex federations such as Brazil.

The main theoretical contribution of the study lies in the proposition of a model organized into four interdependent dimensions, capable of integrating critical success factors and adapting them to national conditions. From a practical

standpoint, the article translated this model into applicable guidelines for Brazil, focusing on federative governance, public digital infrastructure, regulatory frameworks, and the development of technical and cultural capacities.

The research was based on secondary documentary sources which, although analyzed with methodological rigor and triangulation, did not allow direct access to internal practices or the perceptions of the actors involved. The qualitative approach, appropriate for examining governance arrangements, limited the observation of operational and managerial dynamics. Another limitation stems from the empirical focus on developed countries, a choice justified by their institutional maturity and data availability, but one that requires caution when transposing results to the Brazilian context, whose interpretation demands a critical and situated reading.

Future research may broaden the model's practical application in national initiatives for technological migration. The combination of qualitative and quantitative methods, such as interviews, longitudinal analyses, and comparative case studies, would help to understand the evolution of strategies, their effects on public services, and their impact on institutional capacity. Systematic monitoring of ongoing experiences could also generate evidence on sustainability and adaptability, fostering continuous learning cycles.

By gathering international evidence, articulating distinct theoretical frameworks, and proposing a model adapted to Brazilian conditions, this article seeks to contribute to the strengthening of digital sovereignty. It is expected that the results will provide inputs for the formulation of more autonomous and secure public policies, consistent with the demands of a State operating in an environment increasingly structured by data and digital infrastructures.

Migração tecnológica e soberania digital em contextos federativos: construção de um modelo conceitual

RESUMO

A crescente dependência de fornecedores tecnológicos no setor público tem intensificado o debate em torno da soberania digital e da necessidade de estratégias nacionais de migração tecnológica. Este artigo analisa experiências internacionais nesse campo com o propósito de propor um modelo conceitual voltado à promoção da autonomia digital em contextos federativos, como o brasileiro. O estudo adota uma abordagem qualitativa, fundamentada em revisão sistemática da literatura, análise documental e estudo de casos múltiplos em países de elevada maturidade digital (Estônia, França, Coreia do Sul e Canadá). A análise comparativa revelou padrões estruturantes recorrentes, como o reuso de software público, a institucionalização da governança digital, a consolidação de infraestruturas interoperáveis sob controle estatal e a capacitação contínua de servidores. Esses elementos, contudo, articulam-se a condicionantes político-administrativos específicos que moldam as estratégias em cada país. Com base nessas evidências, foi desenvolvido um modelo conceitual estruturado em quatro dimensões interdependentes (institucional, operacional, normativa e sociotécnica), oferecendo diretrizes adaptadas à realidade federativa brasileira. Os resultados contribuem para o fortalecimento de políticas públicas voltadas à soberania digital, com ênfase na construção de capacidades estatais duradouras, na coordenação federativa e na redução da dependência de fornecedores externos.

PALAVRAS-CHAVE: Migração Tecnológica, Soberania Digital, Governo Digital, Transformação Digital.

REFERENCES

ALTHANI, B. Migration challenges of legacy software to the cloud: a socio-technical perspective. Cogent Business & Management, v. 12, n. 1, 2025.

BARBIERI, L. M.; SOTT, M. K. Critical success factors in the implementation of cloud ERP in SMEs: A case study in Brazilian organizations. REGEPE Entrepreneurship and Small Business Journal, v. 14, e2624, 2024.

BARDIN, L. Análise de conteúdo. São Paulo: Edições 70, 2016.

BLANCATO, F. G. The cloud sovereignty nexus: How the European Union seeks to reverse strategic dependencies in its digital ecosystem. Policy & Internet, v. 16, n. 1, p. 12–32, 2024.

BOCEAN, C. G.; VĂRZARU, A. A. EU countries' digital transformation, economic performance, and sustainability analysis. Humanities & Social Sciences Communications, v. 10, n. 1, 2023.

BRASIL. Decreto nº 12.069, de 21 de junho de 2024. Dispõe sobre a Estratégia Nacional de Governo Digital e a Rede Nacional de Governo Digital – Rede Gov.br e institui a Estratégia Nacional de Governo Digital para o período de 2024 a 2027. Diário Oficial da União, Brasília, DF, 2024.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Diário Oficial da União, Brasília, DF, 2018.

BRASIL. Lei nº 14.129, de 29 de março de 2021. Dispõe sobre princípios, regras e instrumentos para o Governo Digital e para o aumento da eficiência pública. Diário Oficial da União, Brasília, DF, 2021.

BUDNITSKY, S. A relational approach to digital sovereignty: e-Estonia between Russia and the West. International Journal of Communication, v. 16, p. 1918–1939, 2022.

BUNDESMINISTERIUM DES INNERN – BMI. IT-Planungsrat. Berlin: Federal Ministry of the Interior, 2024.

CANADA. Audit of Information Management – Readiness to Implement the Policy on Service and Digital. Ottawa: Government of Canada, 2021b.

CANADA. COVID-19 Digital Government Accomplishments. Ottawa: Government of Canada, 2020a.

CANADA. Digital Standards. Ottawa: Government of Canada, 2021a.

CANADA. Government of Canada White Paper: Data Sovereignty and Public Cloud. Ottawa: Government of Canada, 2020b.

CANADA. Governments of Canada and British Columbia connecting more than 7,700 households to high-speed Internet and bringing mobile connectivity to remote areas. Ottawa: Government of Canada, 2025.

CANADA. Guideline on Service and Digital. Ottawa: Government of Canada, 2024.

CANADA. Summary of the Accessible Canada Act. Ottawa: Government of Canada, 2022.

CAPI. Barriers to adoption: digital agriculture in Ontario's food production landscape. Ottawa: The Canadian Agri-Food Policy Institute, 2025.

CARRERA-RIVERA, A.; OCHOA, W.; LARRINAGA, F.; LASA, G. How-to conduct a systematic literature review: a quick guide for computer science research. MethodsX, v. 9, n. 101895, 2022.

CARVER, J. Developing digital "peripheries" for strategic advantage: capacity building assistance and strategic competition in Africa. Contemporary Security Policy, p. 1–42, 2024.

CHEONG, I.; CHO, J. Digital government in the Republic of Korea: evaluation and challenges. In: Empowering Online Public Service in Asia: The Digital Frontier. Jakarta: ERIA, 2024. p. 177–197.

CHUNG, C. S.; CHOI, H.; CHO, Y. Analysis of digital governance transition in South Korea: focusing on the leadership of the president for government innovation. Journal of Open Innovation Technology Market and Complexity, v. 8, n. 1, p. 2, 2022.

CIANCARINI, P.; GIANCARLO, R.; GRIMAUDO, G. Digital transformation in the public administrations: a guided tour for computer scientists. arXiv, 2023.

CSIS. South Korea's 2024 Cyber Strategy: A primer. Washington, DC: Center for Strategic and International Studies, 2024.

DATA.GOVT.NZ. Guidance from Data Ethics Advisory Group. Wellington: Digital Public Service, 2024.

DIGST. Denmark tops UN E-Government Survey. Copenhagen: Agency for Digital Government, 2024.

EC. Digital public administration factsheet 2022: France. Brussels: European Commission, 2022a.

EC. Digital public administration factsheets 2022 – Estonia. Brussels: Directorate-General for Informatics, European Commission, 2022b.

EC. Governance – France. Brussels: Interoperable Europe, European Commission, 2024.

EC. Open Source Software Country Intelligence Report: France 2023. Brussels: European Commission, 2023.

EC. X-Road – cross-border co-development of national data exchange platform. Brussels: European Commission, 2018.

E-ESTONIA. e-Identity. Tallinn: Estonian Business and Innovation Agency, 2020.

E-ESTONIA. IT-skills are not only for programmers; they're for me, you, and your grandma. Tallinn: Estonian Business and Innovation Agency, 2023.

E-ESTONIA. X-Road – interoperability services. Tallinn: Estonian Business and Innovation Agency, 2024.

ESPINOSA, V. I.; PINO, A. E-government as a development strategy: the case of Estonia. International Journal of Public Administration, p. 1–14, 2024.

ESTONIA. Cybersecurity Strategy 2024–2030 'Cyber-Conscious Estonia'. Tallinn: Ministry of Economic Affairs and Communications, 2024.

ESTONIA. Estonia's Digital Agenda 2030. Tallinn: Ministry of Economic Affairs and Communications, 2021.

FINNISH GOVERNMENT. Government report: Finland's Digital Compass. Helsinki: Finnish Government, 2022.

FISCHER, S. C. France: a European pioneer in the geopolitics of technology. CSS Analyses in Security Policy, n. 302, 2022.

FRANCE. Décret n° 2017-1584 relatif à la Direction interministérielle de la transformation publique et à la Direction interministérielle du numérique et du système d'information et de communication de l'État. Paris: Journal Officiel de la République Française, 2017.

FRANCE. Les ressources humaines de l'État dans le numérique. Paris: Inspection Générale des Finances, République Française, 2023.

FRATINI, S.; HINE, E.; NOVELLI, C.; ROBERTS, H.; FLORIDI, L. Digital sovereignty: a descriptive analysis and a critical evaluation of existing models. Digital Society: Ethics, Socio-Legal and Governance of Digital Technology, v. 3, n. 3, 2024.

GOUVERNEMENT DE FRANCE. Doctrine « Cloud au centre » sur l'usage de l'informatique en nuage au sein de l'État (n° 6282-SG). Paris: Gouvernement de France, 2021.

GOV.UK. API technical and data standards. London: Government Digital Service, 2024.

GOVTECH. Government on Commercial Cloud. Singapore: Government Technology Agency, 2025.

HAUG, N.; DAN, S.; MERGEL, I. Digitally-induced change in the public sector: a systematic review and research agenda. Public Management Review, v. 26, n. 7, p. 1963–1987, 2024.

HOSSEINI, M.; RASMUSSEN, L. M.; RESNIK, D. B. Using AI to write scholarly publications. Accountability in Research, v. 31, n. 7, p. 715–723, 2024.

HULKÓ, G.; KÁLMÁN, J.; LAPSÁNSZKY, A. The politics of digital sovereignty and the European Union's legislation: navigating crises. Frontiers in Political Science, v. 7, 2025.

IPEA. Estado digital: análise crítica sobre indicadores de transformação digital e sua aplicação no setor público. Brasília, DF: Instituto de Pesquisa Econômica Aplicada, 2025.

JANSEN, B.; KADENKO, N.; BROEDERS, D.; VAN EETEN, M.; BORGOLTE, K.; FIEBIG, T. Pushing boundaries: an empirical view on the digital sovereignty of six governments in the midst of geopolitical tensions. Government Information Quarterly, v. 40, n. 4, p. 101862, 2023.

KÄSS, S.; BROSIG, C.; WESTNER, M.; STRAHRINGER, S. Short and sweet: multiple mini case studies as a form of rigorous case study research. Information Systems and E-Business Management, 2024.

KIM, W.; KIM, W.; PARK, K. S. A survey of research on the corporate governance of Korean firms. Brussels: European Corporate Governance Institute (ECGI), 2021.

LATUPEIRISSA, J. J. P.; DEWI, N. L. Y.; PRAYANA, I. K. R.; SRIKANDI, M. B.; RAMADIANSYAH, S. A.; PRAMANA, I. B. G. A. Y. Transforming public service delivery: a comprehensive review of digitization initiatives. Sustainability, v. 16, n. 7, p. 2818, 2024.

LEE, H.; KIM, E.; PARK, D. H. Insights from the Incheon Airport case in South Korea: balancing public safety and individual rights with global scalability analysis. Humanities and Social Sciences Communications, v. 12, p. 1104, 2025.

LUI, L.; DE AGUIAR, R. B.; DOS SANTOS TEN CATE, L. N.; DE MELO BARBOSA, S. What drives local governments' digital transformation in Brazil? Conference on Digital Government Research, v. 1, 2025.

MARITAN, F. B.; SOLIANI, R. D.; FERREIRA JUNIOR, G. C.; SATRAPA, H. F. M.; FLORENTINO, M. M. G. Regional development through innovation: a proposal for a technological hub framework. Revista de Gestão e Secretariado, v. 15, n. 10, e4255, 2024.

MCMAHON, R. Co-developing digital inclusion policy and programming with Indigenous partners: interventions from Canada. Internet Policy Review, v. 9, n. 2, 2020.

MCTI. E-Digital: Estratégia Brasileira para a Transformação Digital. Brasília, DF: Ministério da Ciência, Tecnologia, Inovações e Comunicações, 2018.

MILAKOVICH, M. E. Digital governance: applying advanced technologies to improve public service. London: Routledge, 2021.

MOIS. Digital Government Innovation. Seoul: Ministry of the Interior and Safety, Republic of Korea, 2021.

MOIS. Korea's e-government best practices. Seoul: Ministry of the Interior and Safety, Republic of Korea, 2024.

MPM. Training for foreign government officials. Sejong-si: Ministry of Personnel Management, Republic of Korea, 2024.

MSIT. MSIT launches KRW 400 billion K-Cloud R&D project based on domestic AI semiconductors. Seoul: Ministry of Science and ICT, Republic of Korea, 2025.

MÜGGE, D. EU AI sovereignty: for whom, to what end, and to whose benefit? Journal of European Public Policy, v. 31, n. 8, p. 2200–2225, 2024.

NIA. IT cooperation project. Seoul: National Information Society Agency, Republic of Korea, 2024.

NIA. Working together by sharing digital government experiences and best practices. Seoul: National Information Society Agency, Republic of Korea, 2025.

NRCAN. What we heard: findings from federal/provincial/territorial (FPT) qualitative interviews on the current state of Canada's spatial data infrastructure. Ottawa: Natural Resources Canada, 2024.

OECD. 2023 OECD digital government index. Paris: OECD Publishing, 2024.

OECD. Going digital in Brazil. Paris: OECD Publishing, 2020. (OECD Reviews of Digital Transformation).

OECD. Government at a glance 2023: country notes. Paris: OECD Publishing, 2023.

OECD. Government at a glance 2025. Paris: OECD Publishing, 2025.

OPENFORUM EUROPE. Open source software country intelligence report – Estonia. Brussels: Interoperable Europe, European Commission, 2025.

PANNIER, A. The changing landscape of European cloud computing: Gaia-X, the French national strategy, and EU plans. Briefings de l'Ifri. Paris: French Institute of International Relations (Ifri), 2021.

PBO. Overview of the government's digital service transformation. Ottawa: Parliamentary Budget Officer, 2023.

POLIDO, F. B. P. Estado, soberania digital e tecnologias emergentes: interações entre direito internacional, segurança cibernética e inteligência artificial. Revista de Ciências do Estado, v. 9, n. 1, p. 1–30, 2024.

ROBERTS, H. Digital sovereignty and artificial intelligence: a normative approach. Ethics and Information Technology, 26(4), 2024.

SOLIANI, R. D.; OLIVEIRA, D. A.; PONTES, J. C. N.; DRUMOND, T. D. R. Professional training in Industry 4.0: a competency-based educational model. Gestão & Produção, 32(e2225), 2025.

UN. E-Government survey 2024. New York: Department of Economic and Social Affairs, United Nations, 2024.

VALENCIA, M. M. A. Principles, scope, and limitations of the methodological triangulation. Investigacion y Educacion En Enfermeria, 40(2), 2022.

VON SCHOMBERG, R. On technological and innovation sovereignty: a response to Carl Mitcham's call for a political theory of technology. Nanoethics, v. 19, n. 1, 2025.

YIN, R. K. Case study research and applications. 5. ed. Thousand Oaks: SAGE Publications, 2018.

YUN, H. China's data sovereignty and security: implications for global digital borders and governance. Chinese Political Science Review, v. 10, n. 2, p. 178–203, 2025.

ZANGIACOMI, A.; PESSOT, E.; FORNASIERO, R.; BERTETTI, M.; SACCO, M. Moving towards digitalization: a multiple case study in manufacturing. Production Planning & Control, v. 31, n. 2–3, p. 143–157, 2020.

Recebido: 02 nov. 2025.
Aprovado: 08 dez. 2025.
DOI: 10.3895/rbpd.v15n1.21152
Como citar: BRITO, B. G. M.; LOBÃO, M. S. P.; CARVALHO, S. M. S.; SOLIANI, R. D.; FREITAS, R. G. A. Technological migration and digital sovereignty in federative contexts: building a conceptual model. **R. Bras. Planej. Desenv.** Curitiba, v. 15, n. 01, p. 222-250, jan./abr. 2026. Disponível em: <https://periodicos.utfpr.edu.br/rbpd>. Acesso em: XXX.
Correspondência:
Rodrigo Duarte Soliani
Av. Brasil, 920 - Xavier Maia, Rio Branco - AC